Міжнародний союз електрозв'язку

Державний університет телекомунікацій

Студентська рада Державного університету телекомунікацій

Наукове товариство студентів та аспірантів

Державного університету телекомунікацій

«СВІТ ТЕЛЕКОМУНІКАЦІЇ ТА ІНФОРМАТИЗАЦІЇ»

Збірник матеріалів

VI Міжнародної науково-технічної конференції студентства та молоді

17 травня 2018 р.

КИЇВ

«СВІТ ТЕЛЕКОМУНІКАЦІЇ ТА ІНФОРМАТИЗАЦІЇ»: матеріали Міжнародної науково-технічної конференції студентства Державного університету телекомунікацій – Київ: ДУТ, 2018 – 352 с.

Збірник містить матеріали Міжнародної науково-технічної конференції студентства Державного університету телекомунікацій «СВІТ ТЕЛЕКОМУНІКАЦІЇ ТА ІНФОРМАТИЗАЦІЇ». Пропонує статті та тези студентів й аспірантів, що висвітлюють перспективи розвитку інформаційних та телекомунікаційних технологій в Україні та світі.

Упорядники:

Бондаренко Євгеній Олександрович, голова Студентської ради Державного університету телекомунікацій.

Соснова Дана Назарівна, голова Студентської ради факультету телекомунікацій

Щетініна Анастасія Артурівна, голова Студентської ради факультету інформаційних технологій.

Перепелиця Ліна Сергіївна, голова Студентської ради Навчально-наукового інституту захисту інформації.

Лазоренко Анастасія Вячеславівна, голова Студентської ради Навчально-наукового менеджменту та підприємництва.

ЗМІСТ

СЕКЦІЯ №1. ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ

СЕКЦІЯ №2. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

СЕКЦІЯ №3. БЕЗПЕКА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

СЕКЦІЯ №4. СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

СЕКЦІЯ №1. ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖ

Соснова Дана Назарівна
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

СТАНДАРТ 4G/LTE В УКРАЇНІ

Не встигли ми, як слід насолодитися 3G інтернетом, який був запущений зовсім недавно - в 2015 році операторами Київстар, Водафон і Лайфселл (а раніше -ТріМобом), як з'ясовується, що вже і 4G на підході. Нічого собі, прогрес! Вигукне обиватель, не сильно стежить за передовими технологіями. Насправді наша країна, як це не сумно, пасе задніх цього прогресу, так як практично у всіх розвинених, частково в недорозвинених країнах інтернет 4G вже повноцінно використовується. Україна поки тільки вчепилася в хвіст тікаючого потяга сучасних технологій в передачі даних. Тому, давайте подивимося, які перспективи нас чекають на найближче майбутнє в стандарті 4G ...

Що таке 4G

4G - це стандарт, а точніше, покоління мобільного зв'язку, що використовує технології, які дозволяють передавати дані зі швидкістю понад 100 Мбіт / сек. Технологія 4G LTE в світі вважається вже практично пройденим етапом і це, як не дивно, для України добре. Тому, що всі деталі цього стандарту зв'язку вже налагоджені, проблеми відомі і усунені, а ми отримуємо готовий продукт, який необхідно просто запустити технічно. Якщо впровадження 4G піде такими ж темпами, як і 3G, то протягом року-двох-трьох ми цілком наздоженемо більшість країн світу, в крайньому випадку, в великих містах України.

Якщо вони, до цього часу, не перейдуть на 5G ... З огляду на те, що в серпні 2017 року наш д уряд, нарешті, відкрив для стандарту LTE діапазон частот 1800 МГц, можна очікувати, що українські оператори візьмуться за справу. Позитивна сторона в тому, що ця частота не вимагає установки нового обладнання - антен, приймально-передавальної частини, а тільки її модернізацію, що значно дешевше обійдеться кінцевому споживачеві, тобто, нам з вами. У найближчих планах - відкрити також частоту 2600 МГц для технології LTE, але вона вже буде використовуватися для місцевості з щільною міською забудовою. І обійдеться оператору вже дорожче, так як потребує монтажу основного обладнання практично заново.

Про частоти і спектри

На сьогоднішній день в Україні національні оператори працюють в наступних умовних частотних діапазонах:
800 Мгц - оператор CDMA Інтертелеком, PeopleNet (часткове покриття)
900 МГц - оператори GSM Водафон, Київстар, Лайфселл
1800 МГц - оператора GSM Водафон, Київстар, Лайфселл
2100 МГц - оператора UMTS / WCDMA ТриМоб

На всіх цих частотах можна побудувати мережу LTE 4G. Питання тільки у вартості витрат, які можуть істотно різнитися при виборі різних варіантів. Від частоти залежить зона покриття, яку може забезпечити базова станція (вишка). Залежність в даному випадку зворотна - чим вище частота, тим менше радіус покриття бази. А ось по пропускній

здатності навпаки - чим вище частота, тим більше людей одночасно можуть розмовляти або користуватися інтернетом. Тому виділення частоти 1800 МГц можна назвати найбільш оптимальним рішенням на сьогоднішній момент. Це і не вимагає великих вкладень в нове обладнання, витрати на монтаж і дозволяє закрити великий простір навколо базової станції, як в умовах міста, так і за містом. Хоча оператори будуть покривати в першу чергу найбільш «платоспроможні» ділянки мережі для більш швидкої окупності своїх вкладень. А це міська забудова. Переважно центральна частина міста, де є бурхлива ділова активність. Але є й інша проблема. З спектром частот: для повноцінної роботи стандарту LTE необхідно виділити кожному оператору суцільну смугу частот в діапазоні 1800 МГц. Тут у операторів, можна сказати, відносний бардак, так як частоти виділялися шматками. Тільки Київстар має більш-менш «красиву» смугу.

Щоб отримати від нової технології те, що вона може дати - малий час відгуку, швидкість, яку можна порівняти з провідним інтернетом, велику пропускну здатність, необхідно, щоб виділена ширина частотного спектра для одного оператора була мінімум 10 Мгц.

А краще - 20.

Технічно таку складну операцію з обміну частот планується провести через державний орган з романтичною назвою НКРЗІ (Національна комісія з регулювання у сфері зв'язку та інформатизації), до якого оператори здадуть безкоштовно свої частоти, а потім у неї ж викуплять їх заново. Може навіть, зі знижкою. В результаті у операторів буде новий красивий спектр (смуга) частот. Поки все це вирішується, у нас є час насолоджуватися мобільною мережею 3G в містах (не у всіх) і в найближчому їх передмісті. Тепер можна коротко ознайомитися з поколінням (а саме так перекладається буква G - generation - покоління) 4G з приписку LTE, щоб розуміти, що нас з вами, можливо, чекає в 2018 і 2019 роках. Сама абревіатура LTE - це скорочена назва Long-Term Evolution - «довгий або тривалий розвиток». Те, що ми називаємо 4G - це десятий реліз (версія) - LTE Advanced, яка була запущена на комерційній основі в далекому 2009 році в Швеції. Після цього почалося масове впровадження мереж LTE по всьому світу. Ось список основних і далеко не всіх країн, які використовують цю технологію на сьогоднішній день. Австралія, Австрія, Ангола, Арабські Емірати, Вірменія, Білорусь, Бельгія, Бразилія, Великобританія, Угорщина, Німеччина, Грузія, Гонконг, Данія, Індія, Казахстан, Канада, Киргизія, Колумбія, Латвія, Литва, Молдова, Норвегія, Намібія, Польща , Пуерто-Ріко, Росія, Саудівська Аравія, Сінгапур, США, Таджикистан, Туркменістан, Узбекистан, Філіппіни, Чехія, Швейцарія, Швеція, Естонія, Південна Корея, Японія…В недалекому майбутньому в цьому списку може з'явиться і наша країна ..

Відмінність мереж 4G LTE від мереж 3G

Головна відмінність - це звичайно на порядок збільшена швидкість передачі даних, тобто швидкість інтернету.

Також зменшується і час відгуку, так званий ping, який дає повноцінну можливість, наприклад, грати в мережеві ігри на рівні проводового інтернету, проводити інтерактивні конференції. Це все досягається, крім усього іншого, за рахунок більш короткого шляху, який повинен був пройти сигнал від абонента до абонента.

У новій технології з ланцюжка абонент-оператор-абонент виключені контролери, які були, по суті, «слабкою ланкою», який гальмує весь потік. Якщо говорити конкретно про швидкостях доступу в мережу, то у 3G максимально можлива швидкість на сьогодні в Україні - до 42 Мбіт / сек. Саме «до», так як таку швидкість можна побачити тільки в лабораторних умовах, коли один абонент знаходиться біля базової станції, а у всіх інших смартфони та планшети забрали, щоб вони не завантажували базу. Реальна швидкість у 3G операторів з Великої трійки (плюс ТриМоб) - від 2 до 6 Мбіт / сек. Це не так вже й мало, враховуючи, що ще пару років тому все задовольнялися швидкістю до 150 кбіт / сек і були майже щасливі, якщо з'єднання не обривалася. У технології 4G LTE можна говорити про

теоретичні 100 Мбіт / сек для мобільних пристроїв. Реально швидкість, звичайно, буде трохи нижче, але вона не повинна опускатися менше 20 Мбіт / сек. Така швидкість дозволяє, наприклад, дивитися відео в якості HD без гальмувань.

Друга важлива перевага нової технології в тому, що при одночасному великому скупченні користувачів (на стадіонах, концертах, масових гулянь) мережа продовжує обслуговувати абонентів без збоїв і не «лягає». Зараз це частенько буває з 3G, коли доступними залишаються тільки голосові дзвінки, а інтернет пропадає геть.

Які телефони підтримують технологію LTE

Все це добре, але щоб користуватися такою гарною швидкістю, треба мати пристрій з підтримкою цієї технології. Далеко не всі смартфони працюють в новому стандарті. Швидше за все, знадобиться і заміна SIM карти для роботи в мережі LTE. Щоб перевірити, чи підходить ваш смартфон або SIM карта для роботи в новому стандарті, необхідно:

У оператора Київстар:

Ввести команду * 245 * 4 # + Виклик для перевірки сім карти

Або * 245 * 5 # + Виклик для перевірки телефону

У оператора Водафон-Україна:

Набрати на клавіатурі * 222 # + Виклик для перевірки сім карти

За оцінками операторів, абонплата для нової послуги повинна бути не менше 100-150 грн. в місяць, щоб вона почала окупатися, а в подальшому давати прибуток. І хоча зараз вони заявляють, що щомісячний платіж буде в межах вашого поточного тарифу, але, швидше за все, вартість послуги буде підвищуватися - надто вже великі витрати на запуск мережі 4G. Тільки за ліцензію (практично за повітря) оператори виклали близько 8 мільярдів гривень. Але ж є ще обладнання, монтаж, настройка ... Зрозуміло, що далеко не всі категорії населення зможуть потягнути таку оплату. При розвиненої мережі 3G в місті, багато хто залишиться на старому стандарті. А до населених пунктів за містом LTE дійде ще не скоро. Так що, чекаємо і сподіваємося на краще ...

Останні новини

Здається, відбувається якийсь рух в потрібному напрямку. 23 січня 2018 року тендерна комісія розглянула «підтверджуючі документи по надходженню в НКРЗІ тендерної гарантії за відповідними лотами від претендентів на участь у тендері». При цьому вона з'ясувала, що «всі претенденти виконали відповідні умови». Перекладаючи з бюрократичного - процес пішов. У тендері беруть участь всі три GSM оператора. Торги будуть проведені в кінці січня 2018 року, на яких і визначать, кому і які шматки дістануться в частотному діапазоні 2600 МГц. Тобто, спочатку будуть накриватися цим зв'язком центральні частини великих населених пунктів, де у абонентів є в цьому потреба і фінансові можливості. Ну, а потім, коли небудь, може бути і всіх інших. А 31 січня 2018 року були проведені торги і викуплені частоти в частотному діапазоні 2600 МГц. У торгах брали участь всі три національні оператори, які отримали за свої (або наші) гроші смугу частот шириною 80Мгц (2510-2545 МГц, 2565-2570 МГц, 2630-2665 МГц, 2685-2690 МГц). З них Лайфселл і Київстар викупили по 30МГц, а Водафон - смугу, шириною в 20МГц. В цілому оператори витратили 2,4 мільярда гривень, що дає надію про швидкий запуск зв'язку в стандарті 4G у великих містах України. В березні місяці плануються торги по частоті 1800МГц, яка більш пристосована для дрібних населених пунктів. 22 лютого 2018 року Київстар поділився своїми планами щодо розгортання мережі 4G (2600 Мгц) на українських просторах. Запуск цього стандарту планується на квітень 2018 року. Покриватися в першу чергу будуть великі міста - обласні центри. Правда, далеко не всі. У першочерговому списку, який представив оператор (судячи по карті), це будуть:

- Київ
- Харків
- Дніпро

- Одеса
- Ужгород
- Вінниця
- Хмельницький
- Івано-Франківськ
- Тернопіль
- Львів

Також будуть покриті ряд прикордонних пунктів практично по всьому периметру країни і ряд невеликих курортних міст в Одеській і Запорізькій областях. (Затока, Кароліна-Бугаз, Кирилівка, Краковець, Поляниця, Рада-Руська, Старовойтове, Устилуг, Чоп, Шегині, Ясіня). Оператор Водафон-Україна обіцяє запустити надшвидкий інтернет «У Києві, Одесі, Харкові, Дніпрі, Львові та інших обласних центрах. Потім - в інших населених пунктах країни. » 6 березня 2018 року відбувся обіцяний аукціон з викупу частот в «народному» діапазоні 1800МГц. На цьому завершується епопея з купівлею-продажем частот, і всі три українські оператори можуть вже повноцінно зануритися в розгортання мережі 4G. І навесні-влітку цього 2018 роки нам обіцяють покрити вищеназвані міста і містечка високошвидкісним інтернетом. 30 березня 2018 роки два оператора lifecell і Vodafone Україна оголосили про запуск довгоочікуваної мережі 4G. Поки тільки в діапазоні 2600Мгц (LTE band 7). Лайфселл пішов навіть далі і назвав мережу 4,5G.

З покриттям цього оператора можна ознайомитися на його сайті. А Водафон просто скромно проанонсував цю подію в Facebook на своїй сторінці. Основні міста, в яких 4G з'явився або з'явиться в найближчому майбутньому у цього оператора: Київ, Ірпінь, Бровари, Бориспіль, Вишневе, Чабани, Дніпро, Харків, Куп'янськ, Запоріжжя, Енергодар, Львів, Полтава, Суми, Івано-Франківськ, Чернівці, Луцьк, Кропивницький, Одеса, Херсон. 6 квітня 2018 року і оператор Київстар запустив свою раніше обіцяну мережу 4G в діапазоні 2600Мгц. Перші базові станції загальною кількістю понад 500 були встановлені у великих містах: Дніпро, Одеса, Львів, Харків, Тернопіль, Вінниця, Ужгород, Хмельницький. Також покриті деякі курорти і місця перетину державного кордону: Затока, Кароліно-Бугаз, Кирилівка, Ясіня, Поляниця, Чоп, Рава-Руська, Старовойтове, Краковець, Устилуг, Шегині.

Влітку цього ж року оператор Київстар обіцяє запустити мережу в діапазоні 1800МГц, що істотно розширить покриття високошвидкісної, поки ще дивовижної для України мережі.

Процес пішов…

Література:

1. http://trushenk.com/standart-4g-lte-v-ukraine.html

Мацкевич Владислав Вікторович
Державний університет телекомунікацій
Факультет телекомунікацій
м.Київ

СОТОВАЯ СВЯЗЬ

Сотовая связь, сеть подвижной связи — один из видов мобильной радиосвязи, в основе которого лежит сотовая сеть. Ключевая особенность заключается в том, что общая зона покрытия делится на ячейки (соты), определяющиеся зонами покрытия отдельных базовых станций (БС). Соты частично перекрываются и вместе образуют сеть. На идеальной (ровной и без застройки) поверхности зона покрытия одной БС представляет собой круг, поэтому составленная из них сеть имеет вид шестиугольных ячеек (сот). Сеть составляют разнесённые в пространстве приемопередатчики, работающие в одном и том же частотном диапазоне, и коммутирующее оборудование, позволяющее определять текущее

местоположение подвижных абонентов и обеспечивать непрерывность связи при перемещении абонента из зоны действия одного приёмопередатчика в зону действия другого.

История:

Первое использование подвижной телефонной радиосвязи в США относится к 1921 г.: полиция Детройта использовала одностороннюю диспетчерскую связь в диапазоне 2 МГц для передачи информации от центрального передатчика к приёмникам, установленным на машинах. Федеральная комиссия связи США выделила для телефонной радиосвязи 4 канала в диапазоне 30—40 МГц, и в 1940 г. телефонной радиосвязью пользовались уже около 10 тысяч полицейских машин. В СССР в 1957 г. московский инженер Л. И. Куприянович создал опытный образец носимого автоматического дуплексного мобильного радиотелефона ЛК-1 и базовую станцию к нему. Мобильный радиотелефон весил около трех килограммов и имел радиус действия 20—30 км. В 1958 году Куприянович создаёт усовершенствованные модели аппарата весом 0,5 кг и размером с папиросную коробку. В конце 50-х гг в Воронежском НИИ Связи разработали первую в мире систему полностью автоматической мобильной связи “Алтай”, введённая в опытную эксплуатацию в 1963 г. Система «Алтай» первоначально работала на частоте 150 МГц. В 1970 г. система «Алтай» работала в 30 городах СССР и для неё был выделен диапазон 330 МГц. Принцип связи был таков: город обслуживала одна базовая станция. Оборудование устанавливалось, как правило, на одном из самых высоких зданий в городе. В зависимости от высоты, рельефа и этажности застройки, устойчивый сигнал в городе мог быть в радиусе до 50 — 60 км, а кое-где и до 100 км вокруг базовой станции. В этом радиусе и можно было звонить, причём как с «Алтая» на «Алтай», так и на городские номера АТС, и даже по межгороду и за рубеж.

Сотовые системы:

Архитектура той системы, которая сегодня известна как система сотовой связи, была изложена только в техническом докладе компании Bell System, представленном в Федеральную комиссию связи США в декабре 1971 года. С этого времени начинается развитие собственно сотовой связи.

Первая автоматическая коммерческая система сотовой связи была введена в эксплуатацию в Чикаго в октябре 1983 г. компанией American Telephone and Telegraph. В Канаде сотовая связь используется с 1978 г., в Японии — с 1979 г., в североевропейских странах (Дания, Норвегия, Швеция, Финляндия) — с 1981 г., в Испании и Англии — с 1982 г. По состоянию на июль 1997 г. сотовая связь работала более чем в 140 странах всех континентов, обслуживая более 150 млн абонентов.

Услуги сотовой связи:

1- Голосовой звонок
2- Автоответчик в сотовой связи
3- Роуминг
4- Доступ в интернет
5- Прием и передача сообщений
6- Определение местоположения
7- Видеозвонки

Принцип действия сотовой связи:

Основные составляющие сотовой сети — это сотовые телефоны и базовые станции, которые обычно располагают на крышах зданий и вышках. Будучи включённым, сотовый телефон прослушивает эфир, находя сигнал базовой станции. После этого телефон посылает станции свой уникальный идентификационный код. Телефон и станция поддерживают постоянный радиоконтакт, периодически обмениваясь пакетами. Связь телефона со станцией может идти по аналоговому протоколу (AMPS, NAMPS, NMT-450)

или по цифровому (DAMPS, CDMA, GSM, UMTS). Если телефон выходит из поля действия базовой станции (или качество радиосигнала сервисной соты ухудшается), он налаживает связь с другой (англ. *handover*).

Сотовые сети разных операторов соединены друг с другом, а также со стационарной телефонной сетью. Это позволяет абонентам одного оператора делать звонки абонентам другого оператора, с мобильных телефонов на стационарные и со стационарных на мобильные.

Операторы могут заключать между собой договоры роуминга. Благодаря таким договорам абонент, находясь вне зоны покрытия своей сети, может совершать и принимать звонки через сеть другого оператора.

Литература:

1.https://ru.wikipedia.org/wiki/

2.http://www.corporacia.ru/pages/page/show/816.htm

3.https://sergeydolya.livejournal.com/203437.html

Карагманова Юлия Константинова
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
Свердлюк Богдан Ігорович
Державний університет телекомунікацій
Факультет телекомунікацій
г. Киев

ASTERISK МАЙБУТНЄ ТЕЛЕФОНІЇ

Телекомунікації - це, одна з небагатьох сфер на які не повпливав рух Open Source. Основні виробники телефонного обладнання досі створюють дорогі і несумісні системи. Про зручність і гнучкість - забудьте. Виробники не хочуть забезпечувати вам зручність вибору.

Однак з появою персональних комп'ютерів і з ініціативи хакерів, телефонний зв'язок отримав нове життя.

Переваги IP телефонії над традиційною:

- *Системи зв'язку масштабуються*

Перевага IP телефонії полягає в тому, що вона дозволяє оперативно змінювати базу віртуальної АТС: наприклад включати або виключати з неї абонентів. Більшість функціональних можливостей реалізується через «хмарні» технології.

- *IP-телефонія вигідна*

Як правило, при переході на IP телефонію витрати на зв'язок сильно скорочуються вже в перший місяць.

- *IP-телефонія знімає обмеження на відстані*
- *легкість управління даними*

Переваги SIP телефонії дозволяють легко її підключити, причому для цього не потрібно прокладати додаткові лінії. Крім того, дешевизна SIP телефонії забезпечується ще й завдяки особливостям каналу.

Трохи історії

Це проект з відкритим вихідним кодом компанії Digium. Asterisk має всі можливості класичної АТС, підтримує безліч VoIP протоколів і надає функції голосової пошти, конференцій, інтерактивного голосового меню (IVR), центру обробки викликів (постановка дзвінків в чергу і розподіл їх по агентам використовуючи різні алгоритми), запис CDR та інші функції.

Для створення власної функціональності можна скористатися власною мовою Asterisk для написання діалплану, написавши модуль на мові C, або скориставшись AGI, який є гнучким і універсальним інтерфейсом для інтеграції з зовнішніми системами обробки даних.

Asterisk поширюється за умовами подвійний ліцензії, завдяки якій одночасно з основним кодом, поширюваним по відкритій ліцензії GNU, можливе створення закритих модулів, що містять ліцензований код. Наприклад модуль для підтримки кодека G.729.

Операційні системи

Додаток працює на операційних системах GNU / Linux, FreeBSD і Solaris і призначений для створення рішень комп'ютерної телефонії.

Протоколи

Asterisk забезпечує достатню кількість протоколів для підтримки з'єднань між традиційними системами телефонії та віртуальними мережами включаючи H.323, Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), and Skinny Client Control Protocol (SCCP).

Можливості Asterisk

Asterisk може використовуватися в якості IP або гібридної АТС, комутуючи виклики, керуючи маршрутами. Також може поєднувати традиційну телефонну мережу (PSTN) зі світом IP телефонії. Модульна структура Asterisk дозволяє підтримувати широкий спектр протоколів комунікації і кодеків. Якщо ви маєте потребу в інтерактивному голосовому меню, конференц викликах, або автовідповідачі, Asterisk це зробить для вас. Може бути використаний для організації центру обробки викликів. Розробники програмного забезпечення для контакт-центрів і центрів обробки викликів будують свої рішення на базі Asterisk. Asterisk також вдихнув нове життя у вже існуючі рішення контакт-центрів додаючи можливості віддалених IP агентів, додаткову розширену маршрутизацію, прогнозований і груповий виклики, і безліч інших.

Провайдери послуг Інтернет локального рівня (район / місто) і навіть глобальні провайдери відкрили для себе привабливість побудови голосових комунікацій за допомогою вільно розповсюджуваних програм з відкритим кодом. Вони можуть вбудовувати Asterisk в свій спектр послуг на рівні сервера додатків, систем голосової пошти, карткових платформ для передплачених телефонних карток. Всі такого роду рішення дають бажані результати - гнучкість і надійність, значно знижуючи стартові витрати і витрати в ході експлуатації.

Інтеграція з CRM системами дозволить збирати статистику по кожному клієнту, обробляти виклики, керувати рекламними номерами, використовувати call tracker та багато інших цікавих можливостей.

Деякі поняття:

Asterisk Dialplan

Найбільш важливим для розуміння Asterisk є план набору (dialplan). Всі виклики, такі як, черга, конференція, меню автосекретаря або виклик телефону, визначаються логікою і концепцією діалплану

Extensions

У традиційних АТС *extensions* пов'язаний з інтерфейсом (портом). В Asterisk *extensions* визначається як перелік додатків (applications) та їх аргументів, які виконуються в певному порядку, Порядок виконання визначається пріоритетами (priority). Коли *extensions* набраний пріоритети виконуються до роз'єднання виклику, або перенаправлення на інший *extensions*.

Маршрутизація по CallerID

В залежності від номеру того хто телефонує, Asterisk може виконувати різні сценарії.

З чого почати вивчення Asterisk?

У більшості це починається з нестаріючої класики: “Asterisk - майбутнє телефонії”. Там ви можете знайти посилання на інші джерела. Також рекомендую відвідати офіційний сайт: asterisk.org

Література:

1. *asterisk.org*
2. *asterisk-pbx.ru*
3. *voxlink.ru*

Бочко Марк Андреевич
Государственный университет телекоммуникаций
Факультет телекоммуникаций
г. Киев

СВЯЗАННЫЕ РАДИОТЕЛЕСКОПЫ С ТЕЛЕКОММУНИКАЦИОННЫМ ВОЛОКНОМ

Надежды высоки для Square Kilometer Array (SKA), смелого плана по созданию крупнейшего в мире радиотелескопа, объединив тысячи широко распространенных индивидуальных радиоастрономических тарелок в Австралии и Южной Африке. Выполнение плана оперативным, однако, требует стабильного стандарта опорной частоты разделяет широко дисперсных телескопы, чтобы позволить сигналы от объектов, которые будут совмещены во время и в сочетании когерентно.

В настоящее время группа ученых из Австралии продемонстрировала подход к надежной передаче такой ссылки частоты на сотни километров установленного стандартного телекоммуникационного волокна - даже когда волокно одновременно передает прямой телеком-движение.

Идея SKA основывается на технике интерферометрии с very-long-baseline interferometry (VLBI). В VLBI многочисленные географически отделенные радиоастрономические объекты одновременно обучают своим областям на одном и том же участке неба. Затем коррелированные по времени сигналы интерферометрически комбинируются, чтобы обеспечить угловое разрешение, намного превосходящее по сравнению с одиночной, гораздо меньшей индивидуальной радио-тарелкой. Например, SKA предоставит «виртуальную тарелку» общей площадью сбора около миллиона квадратных метров, что позволит ему подключаться к радиосигналам с чувствительностью, в 50 раз превышающей чувствительность космического телескопа Хаббла в оптическом домене.

Чтобы система работала, радиосигнал от каждого телескопа преобразуется с понижением частоты и сэмплируется с использованием местного осциллятора с частотой, характерной для высокоточных атомных часов, для контроля времени. До этого радиотелескопы были оснащены собственными атомными часами, чтобы обеспечить стабильную опорную частоту.

Но для этого многочасового подхода в настройке VLBI существуют большие недостатки. Одна из них заключается в экономии расходов на атомные часы на данном объекте телескопа, стоимость которых составляет 200 000 долларов США. Другим недостатком является то, что система в целом зависит от всех часов, имеющих превосходную долгосрочную стабильность; дрейф или потери согласованности между часами на отдельных объектах могут ухудшить интерферометрический сигнал.

Используя стабильную частотную ссылку, предоставленную водородным мазером ***(Ма́зер*** (англ. *maser*) — квантовый генератор,
излучающий когерентные электромагнитные волны сантиметрового диапазона) на одном объекте для калибровки обоих телескопов, исследователи смогли установить, что относительная стабильность частоты превысила скорость, полученную с отдельными

водородными мазерами на двух объектах. Действительно, команда обнаружила, что стабильность частоты, передаваемая по волокну, была «значительно лучше», чем ошибка, вызванная атмосферными возмущениями между двумя телескопами.

Исследователи полагают, что система, которая не требует изменений в остальной волоконной сети и может быть реализована сравнительно легко, может оказаться значительно более рентабельным для большого проекта VLBI, такого как SKA, чем поддерживать атомные часы на каждом объекте , Подход, по словам соавтора OSA Кеннета Болдуина из Австралийского национального университета, соавтора исследования, «позволяет атомным часам, стоимость которых стоит около двухсот тысяч долларов, должна быть заменена системой, которая стоит всего несколько десятков тысяч долларов. »

Группа также полагает, что за пределами VLBI система может найти применение при передаче стандартов частоты «для других применений, таких как точная калибровка молекулярного спектроскопического зондирования на основе окружающей среды, промышленного и лабораторного».

Исследовательский консорциум, включенный в эту работу, включал Австралийскую академическую и исследовательскую сеть (AARNet), Австралийский национальный университет, Организацию научных и промышленных исследований Содружества (CSIRO), Национальный институт измерения, Университет Маккуори и Университет Аделаиды.

Литература:

1. *https://www.osa-opn.org/home/newsroom/2018/february/binding_radio_telescopes_with_telecom_fiber/*
2. *https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D0%B7%D0%B5%D1%80*

Краснолицкий Владимир Витальевич
Государсвенный университет телекоммуникаций
Факультет телекоммуникаций
г.Киев

СПУТНИКОВЫЕ АНТЕНЫ

Спутниковая антенна (антенна спутниковой связи) — антенна, используемая для приёма и передачи радиосигналов между наземными станциями и искусственными спутниками Земли, в более узком значении — антенна, используемая при организации связи с ретрансляцией через спутники. В спутниковой связи используются различные типы антенн, самый известный — зеркальные параболические антенны ,массово применяемые для приёма спутникового ТВ-вещания и в спутниковой связи. В зависимости от назначения системы спутниковой связи могут применяться и другие типы антенн.

Офсетные антенны, или антенны со смещённым облучателем, получаются путем вырезки из параболического зеркала. Диаграмма направленности такой антенны смещена относительно оси её зеркала на угол, называемый углом офсета (или углом смещения).

Основное преимущество офсетных антенн в том, что облучатель и элементы его крепления не перекрывают собой направление на спутник и не затеняют зеркало антенны, что позволяет увеличить коэффициент использования поверхности. Дополнительное преимущество — такая антенна при наведении на спутник устаналивается более «вертикально», что уменьшает влияние на неё атмосферных осадков (налипание снега, льда).

По офсетной схеме построены большинство антенн небольшого размера (до 2.5 метров), используемых в приёме спутникового ТВ и спутниковой связи, поскольку на таких размерах возможность полного использования зеркала антенны, без затенения его облучателем, дает заметный выигрыш в усилении.

Офсетная конструкция имеет и ряд недостатков. Офсетные антенны имеют худший уровень поляризационной развязки, что может приводить к увеличению уровня помех от сигналов соседней поляризации на том же спутнике. При работе с круговой поляризацией диаграмма направленности офсетной антенны отличается для левой и правой поляризаций, причем эффект тем заметнее, чем больше размер зеркала. Офсетные зеркала большого размера сложнее в изготовлении и сборке, чем осесимметричные.

При малых углах вертикального наведения наклон офсетной антенны к вертикали становится отрицательным — зеркало «смотрит в землю», хотя нацелено на спутник, находящийся выше горизонта. При этом конструкция опорно-поворотного устройства может ограничивать минимальный угол наведения. Минимальный угол видимости спутника над горизонтом для различных офсетных антенн составляет от 0 до 10 градусов
Слабонаправленные антенны используются для связи через низкоорбитальные и геостационарные спутники в спутниковых телефонах, спутниковом радио, приёме сигналов систем спутниковой навигации и других приложениях, где нет возможности непрерывно ориентировать антенну. Такие антенны имеют широкую диаграмму направленности, что приводит к приёму большого количества шумов (высокой шумовой температуре антенны) и малому отношению сигнал/шум для полезного сигнала на входе приёмника, а следовательно и к низкой пропускной способности системы в целом.

Антенны бегущей волны и близкие к ним (спиральные, волновой канал, логопериодические и т. д.), применяются в диапазонах метровых и дециметровых волн для приёма телеметрии и связи со спутниками на низких орбитах, обмена информацией с метеорологическими спутниками, в любительской радиосвязи через спутники, для некоторых специальных видов спутниковой связи.

Зеркальные антенны — наиболее распространенный класс спутниковых антенн. Применяются в различных диапазонах, от дециметровых волн до Ka-диапазона, и на различных типах станций — от систем индивидуального ТВ-приёма до центров космической связи. Могут иметь размер от десятков сантиметров до десятков метров. Усиление зеркальной антенны зависит от отношения её апертуры к длине волны, точности изготовления зеркала (чем выше частоты, на которых работает антенна, тем большая точность требуется), коэффициента использования поверхности, зависящего от выбранной конструкции антенны и характеристик её облучателя, точности установки частей антенны (зеркала, облучателя, контррефлектора, если есть) относительно друг друга[8].Один и тот же рефлектор (зеркало) может использоваться в различных диапазонах частот при установке на него различных облучателей и выполнения требований по точности изготовления зеркала для самого высокочастотного (коротковолнового) из используемых диапазонов. Чем в более высокочастотном диапазоне используется антенна, тем у́же её диаграмма направленности и выше усиление при одном и том же размере зеркала.
Кроме рефлектора и облучателя в состав антенны входит опорно-поворотное устройство, с помощью которого производится наведение антенны на спутник.
Фазированные антенные решетки используются для создания компактных антенн различных диапазонов.

На основе ФАР строятся в основном спутниковые антенны с малой апертурой. Такие антенны имеют ряд ограничений. Они могут работать только в одном узком диапазоне частот (например, работа во всем диапазоне от 10.7 до 12.75 ГГц с одной антенной на базе ФАР невозможна), сложны в разработке и изготовлении и имеют более высокую цену. В то же время на базе ФАР возможно создавать компактные спутниковые терминалы, они используются в составе носимых и подвижных станций диапазонов Ku и Ka, портативных терминалов Inmarsat BGAN (L-диапазон), носимых спутниковых станций специального назначения.

Также на базе ФАР выпускаются плоские компактные антенны для домашнего приёма спутникового ТВ, которые требуют для установки гораздо меньше места, чем

классические «тарелки» сравнимой апертуры. Это позволяет размещать их не только на улице, но и в помещении (на окне, балконе, лоджии и т. п.) при условии, что место установки обеспечивает видимость спутника.

Литература:

1. *https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D1%83%D1%82%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2%D0%B0%D1%8F_%D0%B0%D0%BD%D1%82%D0%B5%D0%BD%D0%BD%D0%B0*

Кувшинова Марія Андріївна
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

МУЛЬТИСЕРВИСНЫЕ СЕТИ

С ростом количества предоставляемых услуг и расширением географии своего присутствия все больше предприятий и организаций приходит к выводу о необходимости увеличения объема передаваемых данных внутри собственной корпоративной сети. Создание мультисервисной (голос, видео, данные) территориально распределенной инфраструктуры позволяет использовать весь потенциал современных информационных технологий, что дает возможность наладить эффективное функционирование компании и оптимизировать внутренние бизнес-процессы предприятия.

Решения для предприятий и организаций

Территориально-распределенные сети связи

Основной задачей построения территориально-распределенной сети является объединение географически разнесенных подразделений корпорации в единое инфокоммуникационное пространство с целью оптимизации ее бизнес-процессов.

Важным свойством современной корпоративной территориальной сети является ее мультисервисность, т.е. интеграция в единой среде таких услуг, как передача данных, телефония, видеоконференцсвязь, технологическая связь и т.д.

Основными аргументами в пользу создания мультисервисных сетей являются:

- повышение эффективности использования каналов связи
- сокращение эксплуатационных затрат за счет использования единой инфраструктуры
- гибкие возможности по внедрению новых сервисов

Ключевым вопросом при построении корпоративной территориальной сети является выбор магистральных каналов связи. Здесь возможны несколько вариантов:

- использование выделенных линий связи
- использование услуг связи, арендуемых у операторов
- использование ресурсов сети Интернет

В последнее время все большую популярность приобретает использование арендуемой у оператора услуги MPLS/VPN, которая предоставляет наиболее гибкий и экономичный способ объединения узлов сети. Основными достоинствами данной технологии с точки зрения абонентов являются:

- гибкие возможности по созданию наложенных топологий – от «звезды» до «каждый с каждым»
- реализация механизмов качества обслуживания делает возможным внедрение услуг телефонии, видеоконференцсвязи и т.д.
- масштабируемость – возможность подключения новых узлов без изменения существующей конфигурации

- безопасность – виртуальные частные сети полностью изолированы друг от друга

Локальные и кампусные вычислительные сети

Современная ЛВС представляет собой совокупность интеллектуальной сетевой инфраструктуры на базе протокола IP и различных сервисов (телефония, видеоконференцсвязь, технологические системы, пользовательские приложения и т.д.), использующих эту универсальную инфраструктуру для своей работы.

Локальная сеть, как правило, объединяет абонентов в пределах одного здания. Когда необходимо объединить несколько площадок (зданий) (чаще всего с использованием оптических каналов связи), такая ЛВС становится кампусной.

Согласно классическому подходу, архитектура ЛВС включает 3 ярко выраженных уровня иерархии: уровень ядра сети, уровень распределения и уровень доступа. При этом, если сеть не выходит за пределы одного здания, функции уровня ядра и уровня распределения обычно объединяются, что приводит к двухуровневому дизайну. Кампусная сеть, объединяющая несколько зданий, включает, как правило, все три уровня иерархии.

Такая иерархическая архитектура позволяет реализовать следующие основные принципы построения современной ЛВС:

- масштабируемость – возможность расширения функциональности и увеличения количества подключаемых абонентов
- надежность – минимизация времени простоя системы за счет резервирования основных компонентов и оптимизации структуры
- мультисервисность – возможность передачи по сети разнородного трафика (голос, данные, видео, трафик интерактивных приложений и т.д.) с требуемым качеством обслуживания
- безопасность – защита бизнес-процессов и ресурсов компании от посягательств злоумышленников, воздействия вредоносных программ и ошибочных действий пользователей

Решения для операторов связи

Современным подходом к построению мультисервисных операторских сетей связи является декомпозиция сети на уровни с четким отделением уровня универсальной транспортной среды от уровня услуг. Базовым протоколом транспортной магистрали де-факто стал IP. Получив подобную независимость друг от друга, уровни в дальнейшем могут развиваться самостоятельно. Такое разделение легло в основу концепции, получившей название NGN (NextGenerationNetwork).

Физическое разделение уровня транспорта и уровня услуг делает возможной схему, при которой эти уровни находятся под юрисдикцией разных операторов. Это, в свою очередь, изменяет структуру построения их бизнес-моделей. Появляются разные типы операторов: одни занимаются исключительно транзитом трафика, другие представляют собой сервис-провайдеров или поставщиков конечных услуг для абонентов, используя каналы первых лишь в качестве «битовой трубы». Год от года доходность «битовой трубы» снижается. Новые сервисы, напротив, высокодоходны, и должны хорошо продаваться, давая возможность операторам заработать на новых услугах. Это весомый аргумент для традиционных операторов в пользу перехода к NGN.

Литература:

1.. http://www.informsviaz.co.ua/inform_tech/multiservice.html

Соколов Валерий Витальевич

Государственный Университет Телекоммуникаций
Факультет Телекоммуникаций
г. Киев

ИСПОЛЬЗОВАНИЕ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ДЛЯ ЗАЩИТЫ И ПОИСКА АВТОМОБИЛЕЙ

В настоящее время во всем мире намечается значительный рост интереса к системам, обеспечивающим автоматизацию контроля за перемещением автотранспорта. В последнее время широкое распространение во всем мире получили системы и комплексы технических средств определения местоположения подвижных объектов. Эти системы используются на воде, суше и воздухе для слежения за объектами, определения их местоположения, корректировки маршрута и т.д. Они различаются по методам определения координат объектов, способам передачи информации между подвижными объектами и диспетчерскими пунктами, логикой построения и т.д. Однако во всех этих системах логично выполняется условие-возможность для потребителя самостоятельно определять её основные параметры:

-зону работы системы;

-тип транспорта, который требуется контролировать;

-частоту обновления информации о подвижном объекте;

-перечень задач, решаемых в системе.

В настоящее время наиболее актуальными являются задачи автоматизированного местоопределения подвижных объектов в составе комплексного обеспечения безопасности.

Современные системы автоматического определения местонахождения транспортных средств-AVL, выполняющие эти задачи, автоматически определяют координаты транспортного средства в группе ему подобных по мере его перемещения в пределах определенной территории.

Система AVL обычно состоит из подсистемы управления определения местоположения, подсистемы передачи данных и подсистемы управления и обработки данных.

Классификация и характеристика систем автоматического определения местоположения

По территории охвата системы определения местоположения транспортных средств условно логично подразделить на следующие зоны покрытия:

-глобальную, которая охватывает земной шар, материки или территории нескольких государств;

-региональную, ограниченную, как правило, границами населенного пункта, области, региона;

-локальную, которая рассчитанная на малый радиус действия, что характерно в основном для систем дистанционного сопровождения и поиска угнанных автомобилей.

Глобальная зона покрытия обычно требуется для контроля подвижных объектов, находящихся от диспетчерских пунктов на несколько тысяч километров. Поэтому наиболее приемлемое решение для реализации систем подобного масштаба - использование спутниковых каналов связи.

Их можно разделить на системы:

-на базе геостационарных спутников;

-на базе низко и среднеорбитальных спутников.

Основная масса систем контроля основана на использовании геостационарных спутников.

В этих системах время доставки информации составляем 5-15 минут в зависимости от организации диспетчерского пункта. Период обновления информации обычно 1 час.

В комплект подвижного объекта обычно входит:

-спутниковая станция;

-GPS антенна;
-бортовой компьютер;
-набор датчиков.

Габариты мобильного передатчика таковы, что он без проблем устанавливается даже на автомобиль. Бортовой компьютер обеспечивает автоматическую передачу навигационной информации на диспетчерский пункт по запрограммированной временной сетке или при возникновении нештатной ситуации. Точность местоположения составляет около 50 метров.

Классификация методов и AVL-систем показаны в данной таблице.

Методы определения местоположения можно разбить на три основных категории:

-методы приближения;
-методы навигационного счисления ;
-методы определения местоположения по радиочастоте.

Литература:
1.Автомобильные охранные системы. Справочное пособие. (Андрианов В.И., Соколов А.В.)
2. http://www.shevchenkove.org.ua

Фурсович Іван Юрійович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м.Київ

NIMSES

Сьогодні у світі існують багато різноманітних соціальних мереж, таких як facebook, twitter, skype, viber, telegram, instagram та інші. Людство зараз не можна уявити без сайтів, де можна викласти якийсь пост, підписатись на друзів чи знаменитостей, поспілкуватись… варіантів є безліч. Ми проводимо в інтернеті як мінімум 10% свого дня, ми просто тратимо час, не отримуючи нічого в замін. Але є соціальна мережа, точніше екосистема, яку розробили українські програмісти, де кожна хвилина не проходить даремно, не залежно від того, онлайн ти, чи офлайн - це nimses.

Nimses – єдина світова система, яка фіксує та зберігає прожитий час людського життя та дозволяє ним управляти. Після реєстрації в Nimses кожна хвилина життя людини перетворюється в один nim (нім), унікальний цифровий запис, що не зникає. Загальна кількість німів вироблених та отриманих однією людиною, накопичується в індивідуальному балансі, в nimb (німбі). Людина може керувати своїми німами, використовуючи безкоштовний геолокаційний додаток Nimses.

Час – це незворотній перебіг з минулого в майбутнє через сьогодення. Для окремої людини та для людства в цілому це означає неминучий лінійний рух в сторону якоїсь кінцевої точки. Іншими словами, час стрімко йде, його не повернути та не зупинити. Крім того, життя, як таке, можливе тільки в часі.

Час друкується на всіх формах живої матерії, при цьому не маючи свого тіла. Час накладає відбиток на всіх формах живої матерії не маючи свого тіла. Час нематеріальний.Nimses – концепція, яка наділяє час тілом, дозволяє його накопичувати та споживати.

Компанія Nimses Inc. зареєстрована в штаті Делавер, США, у 2016 році. З технічної точки зору, Nimses — це алгоритм, що дозволяє відцифровувати хвилини життя кожного зареєстрованого користувача. Після реєстрації кожен користувач отримує унікальний рахунок, створений в Nimses.

Кожна хвилина життя людини стає постійним цифровим записом - nim (німом), яка не зникне з Інтернету ніколи. Немає жодної хвилини життя зареєстрованого користувача, яка б не була відображена в системі Nimses у вигляді німу.

Кожну хвилину, в тому числі під час сну, відпустки, хвороби або кругосвітньої подорожі, користувач отримує один нім. Індивідуальний баланс німів відображений в німбі конкретної людини. Це загальна сума німів, вироблених однією людиною, а також отриманих ним від інших зареєстрованих користувачів. За 1440 прожитих за день хвилин, тобто за добу, німб користувача збільшується на 1440 німов. Це безумовний гарантований базовий добовий "прибуток" кожної людини. Неможливо створення двох німів для однієї і тієї ж хвилини часу, одного і того ж користувача.

Всі Німи, що зняходяться на рахунку конкретного користувача (вироблені ним самостійно або отримані від інших користувачів), є його власністю і не можуть бути вилучені - ні системою, ні іншими користувачами. Це свого роду «патент на час». Отримувач німів має право розпоряджатися ними на свій розсуд.

Я вважаю, навіть якщо проект nimses закриють, створиться багато нових аналогічних екосистем, за якими буде майбутнє.

Література:

https://nimses.com/uk_ua/

Дудка Олександр Борисович
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

FIFTH GENERATION OF MOBILE NETWORKS

First of all let's learn what is 5G. It is best understood in terms of its predecessors — 2G, 3G, and 4G. With the debut of 2G in the early '90s, wireless phone technology expanded from a voice-based technology to one that supported text messaging. 3G carried data in addition to text messages and phone calls, and 4G LTE (Long-term Evolution) enhanced those capabilities with greater speeds and greater reliability.

5G brings about more improvements, but it's also comprised of a suite of new technologies. Not every vendor agrees on what should be included in the final specifications, but the most popular contenders are small cells; millimeter waves; massive Multiple-input Multiple-output (MIMO); beamforming; and full duplex.

If preliminary tests are any indication, 5G will be fast. Really fast. The ITU's latest draft specification calls for a minimum of 20Gbps downlink and 10Gbps uplink per mobile base station. In wireless scenarios, that capacity will be split between all users on a cell tower. There are many benefits of 5G. Because it is a new kind of network: a platform for innovations that will not only enhances today's mobile broadband services, but will also expand mobile networks to support a vast diversity of devices and services and connect new industries with improved performance, efficiency, and cost. 5G will redefine a broad range of industries with connected services from retail to education, transportation to entertainment, and everything in between. We see 5G as technology as transformative as the automobile and electricity.

There are several differences between 4G vs 5G:

- 5G is a unified platform that is more capable than 4G
- 5G uses spectrum better than 4G
- 5G is faster than 4G
- 5G has more capacity than 4G
- 5G has lower latency than 4G

People from over the word are waiting for 5G. And we know that it should be available in 2019.

Literature:

1. *https://www.gemalto.com/mobile/inspired/5G*
2. *https://uk.wikipedia.org/wiki/5G*

3. https://www.tomsguide.com/us/5g-release-date,review-5063.html

Нагорная Елизавета Дмитриевна
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
г. Киев

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

В настоящее время современный человек не может представить свою жизнь без телевизора, радио, сотового телефона, а главное без компьютера. В современном мире персональный компьютер играет главную роль во всех сферах деятельности, во всех странах мира. Конечно, можно отметить, что еще несколько десятилетий назад, никто не пользовался ПК и при этом не имели никаких удобств, но мир не стоит на месте и необходимо идти «в ногу со временем». Информационные технологии — широкий класс дисциплин и областей деятельности, относящихся к технологиям управления и обработки данных, в том числе, с применением вычислительной техники.

Информационная технология - совокупность методов, производственных и программно-технологических средств, объединенных в технологическую цепочку, обеспечивающую сбор, хранение, обработку, вывод и распространение информации. Информационные технологии предназначены для снижения трудоемкости процессов использования информационных ресурсов.

Анализируя общее понимание информационных технологий, то можно выделить, что ИТ охватывает все области передачи, хранения, восприятия информации. Но в большем случаи ИТ ассоциируются с компьютерными технологиями, так как возникновения компьютеров вывело информационные технологии на новый уровень развития.

Существуют определенные этапы развития информационных технологий:

1. 1 этап (с начала 60 – 70- е г.г.) – основным направлением являлась автоматизация рутинных действий человека, обработка данных в вычислительных центрах в режиме коллективного использования, в условиях ограниченных возможностей аппаратных средств, характеризуется проблемой обработки больших объемов информации.
2. 2 этап (70-е года) – появления персональных компьютеров, распространение ЭВМ серии IBM/360, ориентация на индивидуального пользователя, использование централизованных обработок данных, так и децентрализованного, который базируется на решении локальных задач и работе с локальными базами данных на рабочем месте пользователя.
3. 3 этап (80-е года) – компьютером начинаю пользоваться непрофессионалы, создание информационных технологий, направленных на решение задач, одна из которых максимально удовлетворить потребность пользователя и создания соответствующего интерфейса работы в компьютерной среде.
4. 4 этап (90-е года) - создание современной технологии между организационных связей и информационных систем, организация защиты и безопасности информации, организация доступа к стратегической информации, выработка соглашений и установление стандартов, протоколов для компьютерной связи.

Информационная технология должна обеспечивать разделения всего процесса обработки информации на этапы, действия. При этом этапы, действия должны позволить эффективно осуществлять целенаправленное управление информационными процессами, то есть быть стандартизированы и унифицированы.

Классификация Информационных Технологий

Информационные технологии в различных сферах жизни имеют свою определенную классификацию.

По типу интерактивности информационные технологии делятся:

- с избирательной интерактивностью (технологии, которые обеспечивают хранение информации в структурированном виде, то есть пользователь работает с уже существующими данными. Пример: банки и базы данных, видео - , теле – текст, Интернет и др.)
- с полной интерактивностью (технологии, которые обеспечивают прямой доступ к информации, хранящиеся в информационных сетях или каких – либо носителях. Дает возможность передавать, изменять и дополнять информацию).

Использовать, применять информационные технологии можно в различных областях: образование, культура, наука, производство, военное дело и др.

Для примера компьютерных и бескомпьютерных технологий рассмотрим область образования. К компьютерным информационным технологиям, которые предоставляют учебную информации относятся технологии, которые используют компьютерные обучающие программы, мультимедиа технологии, технологии дистанционного обучения.

К числу бескомпьютерных информационных технологий предъявления учебной информации различаются бумажные, отпотехнические, электроннотехнические технологии. Между ними есть отличие: средство предоставление информации и то, что онм деляться на бумажные, оптические и электронные. Бумажные средства обучения это учебники, учебные и учебно – методические пособия. Оптические это кинопроекторы, диапроекторы, графопроекторы. К электронным средствам обучения относятся телевизоры и проигрыватели лазерных дисков.

Современные средства компьютерной техники также можно классифицировать:

- персональные компьютеры (развитие современных информационных технологий связано как рах с широким распространением с начала 1980-х г.г. персональных компьютеров, в которых сочетается относительная дешевизна и широкие для непрофессионального пользователя функциональные возможности. ПК это наиболее многочисленные класс вычислительной техники).
- Корпоративные компьютеры (вычислительные системы, которые обеспечивают совместную деятельность большого количества интеллектуальных работников в какой либо организации. Сфера использования корпоративных компьютеров – деятельность в крупных финансовых и производственных организациях, организация обслуживания большого количества пользователей: бронирование и продажа билетов, биржевые и банковские системы)).
- Суперкомпьютеры (вычислительные системы, использующиеся в военной и космической отрасли, в фундаментальных научных исследованиях, в глобальном прогнозирование погоды).
- Мультимедиа (технология, которая позволяет использовать текст, графику, видео и мультипликацию в интерактивном режиме).
- Виртуальная реальность (технология неконтактного информационного взаимодействия, которые создается с помощью мультимедийной среды иллюзию присутствия в реальном времени в стереоскопическом представленном «экранном мире». В виртуальном мире поддерживается иллюзия местна нахождения с помощью определенных предметов: вместо дисплея - очки телемониторы (воспроизводят непрерывно изменяющийся мир), управление – «информационные перчатки» (определяют направление перемещения пользователя относительно виртуальных объектов), устройство создания и передачи звуковых сигналов.

- Технология Интернет (WWW (от англ. World Wide Web - всемирная паутина)), предоставляют пользователям возможность выбора источника информации на серверах сети).

Современные Информационные Технологии

В настоящее время практически все организациям необходимо информационное обслуживание, переработка большого количества информации. Одним из главных техническим средством по передаче, восприятие, обработки информации является компьютер. Роль компьютера усилие интеллектуальных возможностей человека и общества в целом, служит для связи и передачи информации.

Основные характеристики новой информационной технологии

Методология	Основной признак	Результат
Принципиально новые средства обработки информации Целостные технологические системы Целенаправленные создание, передача, хранение и отображение информации	"Встраивание" в технологию управления Интеграция функций специалистов и менеджеров Учет закономерностей социальной среды	Новая технология коммуникаций Новая технология обработки информации Новая технология принятия управленческих решений

Начало 21 века отождествляется с появлением информационного общества. Компьютер в информационном обществе является составляющей частью.

Информационное общество — теоретическая концепция постиндустриального общества; историческая фаза возможного развития цивилизации, в которой главными продуктами производства становятся информация и знания. Отличительные черты: увеличение роли информации, знаний и информационных технологий в жизни общества; возрастание числа людей, занятых информационными технологиями, коммуникациями и производством информационных продуктов и услуг в валовом внутреннем продукте; нарастающая информатизация общества с использованием телефонии, радио, телевидения, сети Интернет, а также традиционных и электронных СМИ; создание глобального информационного пространства, обеспечивающего:

1 - эффективное информационное взаимодействие людей;

2 - их доступ к мировым информационным ресурсам;

3 - удовлетворение их потребностей в информационных продуктах и услугах.[7]

Информационному обществу компьютерные и телекоммуникационные технологии являются потребность в существенном увеличении производительного труда в информационном секторе общественного производства.

Благодаря широкому распространению компьютеров и созданию Интернета люди могут общаться между собой чрез ПК.

Для большинства, Интернет- это распространенная и привычная глобальная сеть, которая уже используется как обыденные способ в получение, передачи информации. С помощью Интернета, компьютер становиться настоящим средством связи. Каждый, кто имеет доступ к WWW, может получить всю необходимую ему информацию, а также передать ее по всему миру. World Wide Web (WWW) на Интернете – это самый демократичный носитель информации: с его помощью любой может сказать и услышать сказанное без промежуточной интерпретации, искажения и цензуры, руководствуясь

определенными рамками приличия. Интернет обеспечивает уникальную свободу самовыражения личности и информации. Сейчас именно Интернет делает работу, бизнес более эффективным, чем раньше, так как люди имеют широкий доступ к получению любой информации, о чем раньше нельзя было сказать.

Нельзя не отметить тот факт, что информационные технологии имеют такую особенность устаревать и заменяться новыми: большой ЭВМ в вычислительном центре заменился на персональный компьютер на рабочем месте пользователя, телеграф на телефон, телекс на факс и электронную почту.

Конечно, за всем «не угонишься», но для организаций необходимо не отставать от своих конкурентов, поэтому со временем совершенствовать информационные продукты. Если в процессе внедрения новой информационной технологии этому фактору не уделять должного внимания, возможно, что к моменту завершения перевода фирмы на новую информационную технологию она уже устареет и придется принимать меры к ее модернизации.

Заключение

Формирование и совершенствование информационных технологий является одним из главных факторов в обществе. Распространение ИТ преобразует жизнь людей, облегчает работу, дает больше свободного времени, приносит развитие в экономической, культурной, образовательной и других сферах.

Развитие информационно-телекоммуникационной инфраструктуры в масштабах страны – это необходимое условие для того, чтобы предприятия могли выйти на зарубежные виртуальные рынки, взять на вооружение самые передовые технологии электронного бизнеса, а создание общенациональных банков данных позволит сделать их привлекательнее для потенциальных клиентов, партнеров и инвесторов.

Информационная насыщенность не только изменила мир, но и создала новые проблемы, которые не были предусмотрены.

Современное общество наполнено и пронизано потоками информации, которые нуждаются в обработке. Поэтому без информационных технологий, равно как без энергетических, транспортных и химических технологий, оно нормально функционировать не может.

Bondarenko Yevhenii
State University of Telecommunications
Faculty of Telecommunications
Kyiv
Koltsova Anastasiia
National Mining University
Faculty of Information Technologies
Dnipro

FEATURES AND ADVANTAGES OF THE FREE GAME NETWORK 5G

What is 5G? This is the future standard of mobile networks, which will bring them to a fundamentally different level. It is believed that the fifth generation of mobile communications will appear by 2020. Obviously, in the future, many more devices will be connected to the network, most of which will work on a "always online" basis. In this case, a very important parameter will be low power consumption. Of course, in networks of the fifth generation, average speeds should be at least twice as high as in the networks of the fourth generation. According to the developers, the existing global telecommunication infrastructure in the form of LTE over time will reach its technological maximum. This will be facilitated by the rapid development of various devices with access to the Internet. At the moment, mobile networks provide the speed of data transfer to the client side up to 1 Gbit / s. However, there are difficulties with a clear link to specific bands of the

spectrum of frequencies and their aggregation. There are issues with signal delays. All these issues must be resolved by the 5G standard.

Wider use of OFDM modulation will significantly increase the speed of data transmission. For example, primary tests already show a level of 3.6-3.7 Gb / s. The forward-looking interface will also be able to effectively multiple future 5G services with widespread use of QoS, that is, providing different levels of data transfer speed, mobility, delay time, and fault-tolerance. The fundamental innovation of 5G is the use of the widest spectrum of frequencies from 1 GHz and down to the millimeter range of 20-60 GHz with the possibility of their unification. The spectrum below 1 GHz is scheduled to be used to service the Internet of Things (IoT). The low frequency will allow for reliable reception over long distances, which at the moment limits LTE application in the IoT area. Increased number of admissible density of nodes together with support for IPv6 will allow the introduction of a huge number of new devices.

The fifth-generation standard, according to Qualcomm's vision, provides multiple connections, including through relay from one device to another (d2d), so-called multi-threaded routing (multihop), which will extend the coverage. In fact, each device can become a small access point for other devices. First, this will reduce the power of the transmitter of each individual device (first of all it concerns devices with autonomous power supply). Secondly, the operating time of the devices will significantly increase from one battery charge or one replacement of the battery.

The bandwidth available on 5G networks is currently rated at 20 Gbps. At the same time, developers intend to reduce the delay of the signal to 1 ms or less. It is especially useful to reduce delays in the area of smart cars. The situation on the road now changes with lightning speed and the response time of the communication system is much more important than the extra gigabits per second. All together, this will allow the use of wireless devices in scenarios previously available only to leading technologies of data transmission - for example, in systems of virtual reality.

A specialty is also the branch of remote medicine, before which 5G will open new unique opportunities. And the matter here is not only in Internet consultations and the transfer of physiological data to a doctor. The industry has taken a huge step forward. Already not a science fiction remote surgical operation, during which the doctor will be able to operate the patient while with him in different places. For such equipment, critical data rates are critical for fast and fast network response.

So far, the introduction of new networks in commercial operation is not, but manufacturers are already actively developing developments in this direction, and many hardware and software developers have managed to conduct the first field trials of their solutions for the 5G.

Literature:

1. Jonathan Rodriguez, Fundamentals of 5G Mobile Networks. - Wiley, 2015.

2. Networks 5G: What is it? [Electronic resource] https://habrahabr.ru/post/243525/

3. Would you wait from the network of generations? [Electronic resource] http://www.computerra.ru/89955/chego-zhdat-ot-setey-pyatogo-pokoleniya.html

Свердлюк Роман Ігорович

Государственный университет телекоммуникаций

Факультет Телекоммуникаций

г. Киев

FREESWITCH

FreeSWITCH — открытая телефонная платформа, распространяемая в исходных кодах, созданная для удовлетворения потребности в управляемых голосом или текстом

системах, масштабируемых от софтфона до софтсвича. FreeSWITCH может быть использован в качестве коммутатора, АТС, медиа шлюза или медиа сервера для приложений IVR, использующих простые или XML скрипты для управления алгоритмом обработки звонка. FreeSWITCH поддерживает разные протоколы, такие как SIP, H.323, IAX2 и Google Talk, что позволяет взаимодействовать с sipX, OpenPBX, Bayonne, Yate, или Asterisk.

FreeSWITCH поддерживает много продвинутых возможностей SIP, таких как присутствие/BLF/SLA, TCP TLS и sRTP. Он может использоваться как прозрачный прокси-сервер с проксированием медиапотоков или без такового, работать с T.38 (проксирование и преобразование T.38 в T.30 и обратно) и другие протоколы.

FreeSWITCH поддерживает узко- и широкополосные кодеки, что делает его идеальным мостом старых устройств в будущее. Голосовые каналы и конференции могут работать на частотах 8, 16, 32 и 48 kHz и позволяют объединять каналы с разными частотами.

Некоторые кодеки поддерживаются только в режиме pass-through. Это означает, что сжатые данные передаются насквозь между абонентами без какой-либо обработки. Так как данные не кодируются и не декодируются, это позволяет реализовать поддержку некоторых кодеков, которая не может быть реализована из-за патентных/лицензионных ограничений. Однако, в этом случае данные не могут быть перекодированы, то есть в режиме pass-through оба абонента должны использовать один кодек, а также не поддерживаются некоторые функции записи и воспроизведение (такие как IVR).

Кроме того есть поддержка аппаратной перекодировки, например карт производства Sangoma. В этом случае кодеки реализованы аппаратно, что позволяет уменьшить нагрузку на процессор. Некоторые из этих кодеков полностью лицензированы, что дает альтернативу к режиму pass-through.

Литература:

1. *en.wikipedia.org/wiki/FreeSWITCH*
2. *freeswitch.org*
3.

Говорухін Станіслав Олексійович
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

BIGGEST TELECOM TRENDS, THAT WILL AFFECT INDUSTRY BY 2020

Telecommunications these days are huge — we interact and use different technologies on a daily basis. But, since we're learning telecommunications and make researches, it's crucial for us to stay informed and know the biggest and most important trends. In coming up with this list of predictions for telecommunications, I instead wanted to focus upon external factors that will drive the industry. Here are six major trends that will drive the most change in telecommunications by 2020.

1. Content companies will acquire telecoms

Connectivity is capturing an ever-smaller proportion of the information value chain, while content, service, and product deliverers capture ever-more. By 2020, it is likely that one or more major telecom companies will be acquired by a content company. Being connected continues to become cheaper and cheaper, adhering rather slavishly to Moore's Law of diminishing costs. The cost of providing such a service keeps falling, and competition means that the price keeps getting smaller and smaller in a strong, negative feedback loop.

2. Internet of Things will become an actual thing

The next major trend that will impact telecommunications is the explosion of connected devices. This internet of things, or Thingification, will add billions if not trillions of new connected data sources globally by 2020.

The upswing of all of these devices will be an astronomical growth in data volumes; we will quickly push through exabyte volumes and enter the world of zettabytes per year.

3. Wireless will outscale and outspace hardline

Global growth of mobile connectivity is far outpacing hardline connectivity. This makes sense, as most growth is occurring in the developing world and amongst poorer populations. Such consumers may not even own a home, let alone a FiOS connection. For these people, mobile is cheaper, more convenient, and more useful, even when landline connectivity is an option.

4. Market saturation is coming

As they retire, boomers will enter retirement communities and assisted living facilities which are fully digitized in order to be as efficient as possible. Older Americans will be forced into using these technologies by the world around them and will likely consume vastly more bandwidth than they, or their carriers, ever imagined. As this occurs, the last remaining percentages of market penetration will be achieved, and the market will be thoroughly saturated.

5. Worrying about security on a brand new level

As custodians of the networks, carriers play a pivotal role in fighting the new threats that are emerging. Customers will begin to expect, then demand, more proactive protection from the entire internet value chain, and carriers will be expected to support these expectations with a range of technical and operational innovations. The desire for greater security may be a boon for carriers, if they embrace the need.

6. Internet access for everyone, everywhere

I'm predicting that Skynet 2.0 is about to reappear. These space-, balloon-, or drone-based systems will provide high-quality broadband access to anywhere and everywhere in the world, they'll do it affordably, and they'll likely start arriving around 2020. And this time, they'll be wildly successful.

Література:

1. https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/telecommunications-industry-outlook.html
2. https://www.youtube.com/watch?v=7JC2BiRchfE

Михайловский Александр Ильич
Государственный университет телекоммуникаций
Факультет телекоммуникаций
г. Киев

ПЕРСПЕКТИВЫ РАЗВИТИЯ БЕСПРОВОДНЫХ СЕТЕЙ РЕГИОНАЛЬНОГО УРОВНЯ

IEEE 802.22 WRAN — стандарт беспроводных региональных сетей, описывающий двухуровневую архитектуру (уровень PHY и уровень MAC) с многоточечным (Point-to-Multipoint) соединением. Сеть предназначена как для работы с профессиональными фиксированными базовыми станциями, так и с портативными (либо фиксированными) пользовательскими терминалами (модемами). Обмен данными по стандарту производится на «свободных» частотах ОВЧ/УВЧ (VHF/UHF) телевизионного вещания. По утверждению разработчиков, сеть в основном предназначена для использования в малонаселённых пунктах, а также сельской местности, где вероятнее всего будет достаточное количество свободных каналов в рабочей полосе частот стандарта.

Уникальные особенности данного стандарта:

- относительно низкий уровень производственных и ионосферных шумов;
- разумные габариты антенн для эффективного приема и передачи сигнала;

- хорошие характеристики распространения сигнала в условиях прямой видимости;
- идеальная возможность для обеспечения больших зон покрытия, особенно в пригороде и сельской местности.

Основные характеристики стандарта:

- ***Назначение*:** широкополосный беспроводной доступ к Интернету для сельской местности.
- ***Ядро*:** технология когнитивной радиопередачи, предназначенная для безлицензионного использования частот телевизионного диапазона.
- ***Целевая аудитория*:** промышленность, правительство и управляющие органы, академические организации, провайдеры.
- ***Проекты:*** IEEE 802.22.1, IEEE 802.22.2
- ***Портативность:*** можно использовать в движении до 114 км/ч
- ***Топология сети:*** многоточечная (Point-to-Multipoint)
- ***Радиус зоны покрытия:*** 10-100 км (для фиксированной базовой станции и модема)
- ***Максимальная скорость:*** до 22 Мбит/с
- ***Мощность излучения:*** 4 Вт (под мощностью излучения понимается эффективная изотропно излучаемая мощность, EIRP)
- ***Антенны:*** на базовой станции используется ненаправленная (либо секторная) приемопередающая антенна, а на стороне абонента направленная антенна с 14 дБ подавлением заднего лепестка; помимо этого, есть ненаправленная антенна для сканирования частотного диапазона (когнитивная радиосвязь).
- ***Геопозиционирование*:** GPS или наземное (необходимо для функционирования системы).

Использование когнитивных технологий в IEEE 802.22.

Концепция когнитивного радио впервые была представлена в 1999 и с тех пор получила значительное развитие. Одним их направлением развития когнитивных технологий является область динамического доступа к спектру, в котором сеть когнитивного радио динамически определяет и использует часть спектра, которая не используется другими системами. Эти неиспользуемые участки спектра получили название «белые пятна». «Белые пятна» могут состоять из неиспользованных частот или временных интервалов в данном месте. В IEEE 802.22 под «белыми пятнами» обычно понимаются неиспользуемые каналы телевидения на данной территории, то есть частотные промежутки между зонами покрытия.

Когнитивная радиосистема — самоорганизующаяся радиосистема с динамическим доступом к радиочастотному спектру, которая способна познавать свою эксплуатационную и географическую среду, адаптировать к ней свои функциональные параметры и протоколы и/или изменять свою эксплуатационную среду за счет накопленных в процессе функционирования знаний и приобретенных навыков, с учетом установленных регуляторных политик и своего функционального состояния.

Существует несколько методов, которые могут быть использованы когнитивной радиосетью для анализа спектра окружающей среды. В стандарте IEEE 802.22 применяется метод геолокации/базы данных и сканирования частотного спектра. В первом методе используется информация о расположении когнитивных устройств в сочетании с базой данных лицензированных передатчиков, что позволяет определить, какие каналы локально доступны для их повторного использования. В рамках спецификации предполагается применять спутниковое или наземное позиционирование. Расположение базовой станции должно быть известно с точностью до 15 м, а оборудования пользователя с точностью до

100 м.

Сканирование частотного спектра в анализе используемого спектра и определении, какие каналы заняты лицензированными передатчиками. Эта процедура проходит в обязательном порядке при включении нового оборудования в сеть. Кроме того, сканирование частот происходит периодически при работе системы. Управление сканированием осуществляется базовой станцией, которая не только посылает управляющие команды пользовательскому оборудованию, но и сама осуществляет сканирование частот. Такая система позволяет актуально поддержать информацию о состоянии радиоканала во всей зоне покрытия базовой станции и при необходимости своевременно менять рабочие частотные каналы.

Таким образом, управление спектром в стандарте IEEE 802.22 – это когнитивная функция на базовой станции, которая использует входные данные от функции сканирования спектра (SSF), геолокации, и действующей базы данных, чтобы принять решение о частотном канале который будет использоваться, а также ограничения на излучаемую мощность, которые накладываются для конкретного пользовательского устройства.

Требования к антеннам

Все узлы в сети IEEE 802.22 используют два типа антенн – направленные антенны для передачи данных и антенны сканирования. На базовых станциях, для передачи данных, используются обычные для систем мобильной связи антенны – секторные или всенаправленные. У пользователей применяются направленные антенны с коэффициентом усиления до 14 дБ. Антенны сканирования это всенаправленные антенны, обеспечивающие чувствительность к вертикальной и горизонтальной поляризации, что позволяет воспринимать сигнал от телевизионных станций и беспроводных микрофонов. У пользователя такая антенна должна быть установлена вне помещения на высоте 10 м над уровнем земли. Существенным недостатком стандарта IEEE 802.22 является невозможность поддержки технологий множественных антенн (MIMO) и формирования диаграммы направленности. Это связано с тем, что в диапазоне частот 54-862 МГц физически сложно обеспечить достаточное разнесение нескольких антенн, которое должно составлять не менее трех длин волн (то есть более 3 метров на средней частоте).

Перспективы развития в Украине

В нашей стране очень много свободных ТВ каналов, особенно в сельской местности, а с 2015 года их стало еще больше, так как были отключены аналоговые телеканалы, остались только цифровые. Но, по мнению специалистов, использовать данною технологию лучше в местах, где нет прямой видимости на базовые станции, работающие в диапазонах 2.4 и 5 ГГц, то есть использовать вместе с 2.4 и 5 ГГц. Такая конфигурация является самой продуктивной. Но пока что это всего лишь предположения. Данный вопрос нужно поднимать на высшем уровне, нужен специальный закон, позволяющий выделять соответствующие частоты для подобного использования, а этим пока еще никто не занимается.

Литература:

1. https://en.wikipedia.org/wiki/IEEE_802.22
2. http://asp24.com.ua/blog/standart-ieee-802-22-tehnologii-primenenie-perspektivy/
3. http://netobzor.org/stati/4131-chto-takoe-super-wi-fi-ili-ieee-802-22

Кольцова Анастасія
Національний гірничий університет
Факультет інформаційних технологій

м. Дніпро

IPTV, АБО ЗУСТРІЧ ДВОХ ПОКОЛІНЬ ТЕХНОЛОГІЙ

IPTV, або IP-телебачення (англ. Internet Protocol Television) — технологія цифрового інтерактивного телебачення в мережах передачі даних з використанням протоколу IP, нове покоління телебачення. Доставка контенту до клієнтського обладнання здійснюється через IP-мережу провайдера.

Як не дивно, але IPTV - це не телебачення, яке транслюють через Інтернет. Незважаючи на те, що скорочення "IP" походить від "Internet Protocol", це не означає, що люди можуть зайти на веб-сторінку, щоб подивитися телепередачу. IPTV означає метод передачі інформації через захищену керовану високошвидкісну мережу.

IPTV-мережі зазвичай створюються і супроводжуються великими телекомунікаційними провайдерами, які ставлять перед собою мету створити послугу, здатну конкурувати з існуючим цифровим і супутниковим ТБ. Рішення на базі IPTV містять багато способів моніторингу переваг і вибору глядачів, у зв'язку з чим IPTV є ідеальною платформою для персоналізованого рекламного таргетингу і електронної комерції.

В загальних випадках, це платформа, яку створює і контролює оператор телекомунікаційних структур. Споживач взаємодіє безпосередньо зі своїм оператором. У цьому сенсі оператор IPTV майже не відрізняється від існуючих кабельних телевізійних операторів.

Одна з основних властивостей IPTV - географічна прив'язка. Крім того, що інфраструктура IPTV фізично прив'язана до будинків, пристроїв і телевізорів споживачів, ще існує місцеве регулювання і політика, що також є факторами, що обмежують IPTV на географічному рівні.

IPTV пропонує той самий відеопродукт, який транслюють кабельні та супутникові мережі. При цьому використовуються вже випробувані схеми трансляцій на вимогу (on-demand) і pay-per-vew (сплата за переглянутий контент), імовірно з деякими додатковими можливостями і сервісами, а також іншої ціною.

Архітектура комплексу IPTV як правило включає в себе такі компоненти:

- Підсистема управління комплексом та послугами, яку ще називають «Проміжне програмне забезпечення» або «IPTV Middleware»;
- Підсистема прийому та обробки контенту;
- Підсистема захисту контенту;
- Підсистема відео серверів;
- Підсистема моніторингу якості потоків та клієнтського обладнання.

Головними перевагами IPTV є інтерактивність відеопослуг і наявність широкого набору додаткових сервісів (Video on Demand (VoD), TVoIP, Time Shifted TV, Network Personal Video Recorder , Electronic Program Guide, Near Video on Demand). Можливості протоколу IP дозволяють надавати не тільки відеопослуги, але й набагато ширший пакет послуг, зокрема інтерактивних та інтегрованих.

Крім основних IPTV може включати в базовий пакет послуг ряд додаткових сервісів (Video Telephony, Voting, Information Portals, Web, Games, MOD KOD). Це можливо на основі уніфікації і стандартизації різних кінцевих пристроїв, інтеграції звуку, відео і даних на основі IP-протоколу та надання послуг на єдиній технологічній платформі. IPTV дає користувачеві такі можливості, які не дасть просте телебачення, наприклад, адаптивне мовлення, висока якість відео та звуку, інтерактивність (можливість дивитися телепрограми у зручний час, і на будь-якому пристрої), «пауза» прямого ефіру.

В IPTV є можливість використовувати для одного відеоряду два канали звукового супроводу, або навіть більшу їх кількість, наприклад, українською та англійською мовами, самі канали при цьому можуть бути поліфонічними. Переваги IPTV перед кабельним та супутниковим ТБ:

- Нема потреби у витратах на придбання додаткового обладнання;

- Не потрібно встановлювати обладнання;
- Зображення DVD-якості, стереозвук;
- Можливість запису потокового відео на ПК користувача;
- Інноваційна послуга за доступною ціною.

Термін IPTV вперше з'явився в 1995 році, коли Джудіт Естрін і Білл Карріко відкрили фірму Precept Software. Precept розробила технологію «інтернет-відео» під назвою IP/TV. IP/TV був додатком з використанням багатоадресної магістралі (MBONE, multicast backbone), сумісний з ОС Windows та Unix-системами, який передавав одно- та багатоджерельний аудіо- та відеотрафік різної якості, використовуючи одноадресну (unicast) та багатоадресну (multicast) передачу даних через IP-протокол та з використанням транспортного протоколу в реальному часі (RTP), та протоколу керування в реальному часі (RTCP). Програмне забезпечення написали Стів Каснер, Карл Ауербах та Ча Чі Куан. Precept була придбана Cisco Systems в 1998 році Cisco зі збереженням товарного знаку IP/TV.

Kingston Communications, регіональний телекомунікаційний оператор у Великобританії, після проведення випробувань різних видів телебачення та технології «Video on Demand», у вересні 1999 року впровадила послугу KIT (Інтерактивне телебачення Kingston), яка полягала у транслюванні широкосмугового (broadband) інтерактивного IPTV через цифрову абонентську лінію (DSL). У жовтні 2001 року оператор впровадив додатковий сервіс - VoD, та утворив окремий контент-провайдер VoD. Kingston була однією з перших компаній в світі у впровадженні IPTV і VoD IP через ADSL в комерцію. Служба стала орієнтиром для різних змін до правил уряду Великобританії та умов користування IPTV. У 2006 році служба KIT була припинена, кількість абонентів знизилася від 10000 до 4000.

З часом технологія впроваджувалася по багатьох країнах, були винайдені нові сервіси, які впроваджувалися досить швидко, але в усіх технологіях для експлуатації або оновлення є проблеми та недоліки. Ця технологія була ускладнена низьким рівнем впровадження широкосмугового мовлення і відносно високою вартості встановлення проводів, здатних надійно переносити IPTV-контент до помешкань. Тим не менш, кількість абонентів IPTV, які мешкають у житлових будинках, за час існування зростала, оскільки, за даними Point Topic, лише у 1-ій чверті 2013 року кількість абонентів по всьому світу перевищив 79 мільйонів людей, а за даними на 2-гу чверть 2015-го року – 123 мільйони. Можна помітити зниження темпу зростання кількості абонентів, але зростання не зупиняється, з цього розуміємо, що технологію впроваджують поступово.

IPTV охоплює як трансляцію телебачення наживо (multicast), так і зберігання відео на вимогу VoD (unicast). Для відтворення потрібне обладнання з підтримкою multicast, підключене до будь-якої фіксованої або бездротової IP-мережі у формі або автономного персонального комп'ютера, або обмеженого вбудованого пристрою OS, такі як смартфон, планшет, ігрова консоль, підключений телевізор або телеприставки. Стиснення відео забезпечується кодеком H.263 або H.264, аудіо стиснене за допомогою кодеку на основі модифікованого дискретного косинус-перетворення (MDCT), інкапсульованого в будь-який транспортний потік MPEG, в потік RTP- або флеш-відео-пакетів для транслювання наживо або потокового відео VoD. Групове транслювання IP дозволяє надіслати дані кільком адресатам наживо за допомогою однієї групової адреси. H.264/AVC/MPEG-4 широко використовується для потокового інтернету більш високих бітрейт-стандартів, таких як H.261 і H.263, які були більш призначені для ISDN-відео-конференцій. H.262 / MPEG-1/2, як правило, не використовується в якості необхідної пропускної здатності для достатнього навантаження мережі, тому вони використовуються тільки в одиничних broadcast-посиланнях або для зберігання додатків.

В основі стандартів систем IPTV, основними використовуваними базовими протоколами є:

1) Потокових даних на основі постачання контенту від провайдера послуг:
   - IGMP для підписки на багатоадресні потоки, трансльовані наживо (телеканали) та для перемикання з одного потоку на інший (зміна телевізійного каналу). IP Multicast працює в локальних мережах (зокрема у мережах VLAN), а також у глобальних мережах.
2) Одноадресної передачі на основі веб для трансляції наживо або послуги VoD
   - Adobe Flash Player використовую протокол RTMP через протокол TCP зі встановленням та керуванням через транзакції AMF, XML або JSON.
   - Apple, IOS використовує адаптивну трансляцію HLS через HTTP зі встановленням та керуванням через вбудований файл плейлиста формату M3U.
   - Microsoft Silverlight використовує адаптивну трансляцію через HTTP
3) Багатоадресної трансляції наживо та одноадресної трансляції для використання VoD, основаних на веб:
   - IETF рекомендує RTP над UDP TCP або перевозить з установкою і використанням RTSP контроль над TCP.
4) Підключення телевізорів, ігрових приставок, телеприставок та мережевих персональних відеомагнітофонів:
   - місцевий контент в мережі використовує UPnP AV для одноадресної трансляції шляхом використання HTTP через TCP або для багатоадресної трансляції наживо шляхом використання RTP через UDP.
   - Контент на основі веб забезпечується або через вбудовані веб-плагіни, або через додатки на основі телевізійного широкоадресного мовлення, яке використовує мову підпрограмного забезпечення, наприклад, MHEG-5, що викликає завантаження вбудованого у мережу веб-браузера за допомогою використання плагіна Adobe Flash Player.

Останньою тенденцією у технології є винайдення гібридного IPTV. Гібридний IPTV - це комбінація традиційних мовленнєвих телевізійних послуг та відео, які можна отримати через керовані IP мережі або через громадський інтернет. Це зростаюча тенденція як для споживачів, так і для операторів платного телебачення. Популярність гібридного IPTV за останні роки зросла завдяки двом великим компаніям. З появою таких відеохостингів, як YouTube і Vimeo в середині 2000-х років, традиційні оператори платного ТБ під наростаючим тиском вирішили забезпечити своїх абонентів переглядом інтернет-відео (як професійних, так і користувацьких) на їх телевізорах. У той самий час, фахівці телекомунікаційних провайдерів IP-послуг шукали способи, як впровадити одночасно аналогові і цифрові наземні служби, не витрачаючи додаткових грошей та без складності передачі. Пропускна здатність є цінним активом для операторів, тому багато хто з них шукає альтернативні способи впровадження цих нових послуг без додаткових інвестицій в мережеву інфраструктуру.

Гібридна телеприставка (set-top) дозволяє отримати контент з різних джерел, у тому числі з наземного, супутникового та кабельного мовлення, які можна поєднати з переглядом відео через Інтернет шляхом з'єднання Ethernet на пристрої. Це дозволяє телеглядачам отримати доступ до великої кількості різноманітного контенту на своїх телевізорах без необхідності відкриття окремих вікон для кожного з сервісів.

Також гібридні IPTV-приставки дозволяють користувачам отримати доступ до ряду сучасних інтерактивних послуг, таких як VOD / телебачення catch-up, а також інтернет-додатків, в тому числі доступ з телевізора є до відео-телефонії, відеоспостереження, ігор, магазини та «електронного уряду».

З погляду платного ТБ-оператора, гібридна IPTV-приставка дає їм більшу довгострокову гнучкість, дозволяючи впроваджувати нові послуги та програми за вимоги

споживачів, зазвичай без необхідності оновлення обладнання або візиту інженера для переналаштування або заміни пристрою. Це зводить до мінімуму витрати на запуск нових послуг, збільшує швидкість виходу продуктів на ринок та обмежує порушення споживачами правил користування. Hybrid Broadcast Broadband TV (HbbTV) - консорціум індустріальних компаній - створив відкритий європейський стандарт для гібридних приставок, що примають широкомовленнєве та широкосмугове цифрове телебачення та мультимедійні додатки за допомогою єдиного користувацького інтерфейсу. Ці тенденції призвели до розробки гібридних трансляційних широкосмугових телеприставок, які містили як широкомовленнєвий тюнер та підключення до Інтернету – зазвичай через порт Ethernet. Перша комерційно доступна гібридна IPTV-телеприставка була розроблена компанією Advanced Digital Broadcast, розробником цифрових телевізійних апаратних та програмних засобів, в 2005 році платформа була розроблена для іспанського оператора платного телебачення Telefonica, і використовується як частина його сервісу Movistar TV. Запустили ж її для абонентського використання в кінці 2005 року.Альтернативний підхід - версія IPTV для кабельного телебачення, що має назву “Headend In The Sky”. Принцип її в тому, що декілька телеканалів поширюються через супутник до інтернет-провайдера або до точки присутності (point of presence, POP) провайдера IPTV-послуг шляхом інкапсульованого розподілу IP-пакетів між індивідуальними абонентами. Це може забезпечити величезний вибір каналів для абонентів, не перевантажуючи Інтернет-магістраль, проведену до POP, і дає можливість запропонувати IPTV-послуги для невеликих або віддалених операторів за межами досяжності станцій наземного широкосмугового зв'язку високої швидкості. Прикладом є мережа, що поєднує оптоволоконну та супутникову трансляцію, керована через супутник SES New Skies і транслює 95 каналів до Латинської Америки та Карибського басейну, керований IPTV-провайдером у Південній Америці.

Незважаючи на великі можливості, пропоновані Інтернетом і IP-технологіями, найбільш популярними видами телебачення в світі залишаються кабельне телебачення, ефірне та супутникове мовлення. І оператори в цьому сегменті не збираються здаватися без бою, тому ситуація навряд чи сильно зміниться в найближчі роки. Але все частіше звучать прогнози про те, що впродовж найближчих десяти років їм все ж таки доведеться сильно посунутися на користь нового виду ТБ. У нашій країні ситуація розвиватиметься схожим чином, але враховуючи інертність даного сегменту ринку, низьку платоспроможність населення і перепони з боку керівних органів, процес масового переходу до нового типу телебачення буде більш тривалим, аніж в економічно розвинених країнах.

Література:

1. *Журнал "Сети и Бизнес" - http://www.sib.com.ua*
2. *КТВ Зурбаган, кабельное телевидение, интернет, Конотоп - http://zurbagan.tv*
3. *Point Topic - The leading resource for worldwide broadband, IPTV and VoIP data - http://point-topic.com*
4. *Wikipedia – The Free Encyclopedia - https://en.wikipedia.org*

Новіцька Наталія Вікторівна
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

MOBILE ID

Технологія ідентифікації через смартфон. Завдяки новій технології можна буде отримувати через інтернет державні послуги,посвідчувати документи,які матимуть таку ж силу , як і паперові з печаткою та підписом, користуватись комерційними сервісами. А що ж таке Mobile ID?

Mobile ID — це технологія, яка дозволяє проводити електронну ідентифікацію особи для отримання електронних послуг.

Що потрібно для роботи Mobile ID?

Аби користуватись новою технологією через смартфон, потрібно взяти паспорт та ідентифікаційний код. Далі слід звернутися до офісу свого оператора мобільного зв'язку та оформити SIM-карту. Видачу таких карток контрактним клієнтам уже почали у «Київстарі». До середини 2018 року оформлятимуть таку послугу мобільної ідентифікації також у телеком-компаніях «Vodafone Україна» та Lifecell.

Mobile ID - послуга, яка надає можливість за допомогою мобільного телефону провести ідентифікацію особи та використовувати її електронно-цифровий підпис для доступу до електронних послуг і документообігу. Для цього сервісу потрібні звичайний мобільний телефон і спеціальна захищена SIM-карта, що забезпечує підтримку функції криптографічного захисту інформації.

Як працює нова послуга?

Mobile ID надає можливість за допомогою мобільного телефону провести ідентифікацію особи. Власник такого інедтифікатора також може використовувати її електронно-цифровий підпис для доступу до електронних послуг і документообігу. Для цього сервісу потрібні звичайний мобільний телефон і спеціальна захищена SIM-карта, що забезпечує підтримку функції криптографічного захисту інформації. Після отримання нової SIM-карти з індивідуальним цифровим підписом вже одразу можна активувати таку можливість. Після отримання нової картки на мобільний телефон буде надходити службове SMS. Таке повідомлення ініціює у телефоні процедуру накладання електронного цифрового підпису. У службовому SMS міститься унікальний код документа, який підписує користувач. Потім користувач вводить пін-код доступу до SIM-картки. Після цього вводить пін-код особистого ключа й отримує послугу за наданим підписом.

Які переваги надає Mobile ID?

Mobile ID дозволяє отримувати державні послуги віддалено через інтернет, користуватися комерційними онлайн-сервісами, наділяти електронні документи юридичною силою.

Ідентифікатор Mobile ID повинен забезпечити дистанційність, прозорість і якісний сервіс, чого б це не стосувалося — банку, лікарні, освіти, соціальної допомоги, державних послуг, землі, будівництва. Людина має можливість з допомогою свого телефону замовити та отримати послугу від держави.

Як камери впізнають власників смартфонів?

Технології розпізнавання облич використала компанія Apple у нових версіях її смартфонів. Замість ідентифікації по відбитку пальця нові iPhone будуть ідентифікувати користувача по обличчю – впізнавати його та розблоковувати телефон.Щоб технологія, яка отримала назву FaceID, працювала, нові смартфони отримали потужну фронтальну камеру та інфрачервоні освітлювачі, за допомогою яких смартфон створить тривимірну модель обличчя, збереже їх у своїй пам'яті і буде щоразу порівнювати з фото користувача. Цікаво, що смартфон буде розблоковуватися, лише коли людина дивиться прямо в камеру.

Розпізнавання обличчя користувача використовує й операційна система Windows, починаючи з версії Windows 8, проте перші версії інструменту працювали не завжди коректно.

Технології розпізнавання облич використовуються для підтвердження платежів, розпізнавання співробітників компанії на вході в офіс чи ідентифікації терористів.

Короткі висновки

Mobile ID- зручна технологія для суспільства.

Розпізнавання жестів ґрунтується на класичній математиці, а також нейромережах, машинному та глибинному навчанні У світі існують десятки технологій розпізнавання обличчя та об'єктів. Задача розпізнавання облич перестала бути серйозною математичною проблемою, а стала основою для різноманітних сервісів та додатків. Розрізняти об'єкти-

суть полягає в тому, щоб навчитися класифікувати об’єкти за певними характеристиками і відрізняти їх один від одного.

Література:

1. *https://espreso.tv/article/2017/10/12/scho_umiyut_systemy_rozpiznavannya_oblych_i_chomu_ce_nebezpechno*
2. *https://nachasi.com/2018/01/30/mobile-id-2/*
3. *https://www.epravda.com.ua/publications/2017/12/27/632567/*

Koltsova Anastasiia
National Mining University
Faculty of Information Technologies
Dnipro
Bondarenko Yevhenii
State University of Telecommunications
Faculty of Telecommunications
Kyiv

PIFA ANTENNA FOR MOBILE COMMUNICATION FACILITIES. MULTIDIMENSION OF CONSTRUCTIONS

Today, the state of affairs in the market of small-size antenna technology for mobile communications can be briefly described as a "boom for the introduction of antennas of the PIFA type", i.e. planar F-shaped antennas (Planar Inverted-F Antenns). The high demand for these devices is due to their advantages, such as a sufficiently broad band of operating frequencies (up to 10% of the resonance carrier), high efficiency (ratio of radiated power to input), reaching ~ 65%, relatively small dimensions and support for multi-range. In addition, antennas of this type are characterized by a sufficiently high gain in both the vertical and horizontal planes of polarization. It is because of this that they are promising for use in wireless communications, and not only. The growing popularity of PIFA is also associated with the development of wireless computer technologies. That is why the reader can be interested in a detailed consideration of the theoretical and practical aspects of implementing PIFA.

Single-band PIFA

The design of PIFA type antennas is more complicated than ILA, IFA and DIFA [1]. This leads to the complication of its design and analysis. The electrical characteristics of PIFA depend on the dimensions of the upper radiating plate, the ratio of the lengths of its sides, the height of this plate above the screen, the dimensions and position of the vertical grounding wall, the antenna feed point. The small dimensions of the PIFA antenna are possible due to the fact that its resonance frequency is determined mainly by the semiperimeter of the horizontal radiating plate. The width of the PIFA bandwidth depends directly on the width D of the vertical shorting plate. The largest band corresponds to the coincidence of the width of the vertical plate D and the length of the contacting side of the horizontal radiator W. For this, a 10% bandwidth of working frequencies is achieved for the ratio of the lengths of the sides of the horizontal plate W / L = 2 and its height above the screen h = 0.053l. When the ratio D / W is reduced to a level of 0.1 or less, the operating frequency range narrows to 1%. Minh-Chau T. Huynh [2] approached the calculation of the resonance frequencies of PIFA in the most conscientious manner, considering all the particular cases of the dependence of the resonant frequencies on the PIFA geometry. He obtained the following relationships for the resonant wavelength of PIFA:

The ratios obtained by the Minh-Chau T. Huynh can be regarded as basic for the approximate calculation of the PIFA dimensions at a given resonant frequency.

It should be noted that the width D of the vertical section affects not only the resonance frequency, but also the polarization of the radiation. This is confirmed by the dynamics of the surface currents of PIFA, depending on the ratio of its dimensions [3]. For many mobile phones, PIFA mounting with a narrow shorting vertical section is typical. However, the best VSWR

(VSWR) has a PIFA design with a ratio of D / W = 1. It is easy to see that the VSWR J 2 values correspond to the receive bandwidth of 8% of the central carrier. At the same time, the achieved positive effect is especially noticeable in comparison with VSWR dependence on frequency for a wire F antenna [1].

In addition to using the dielectric properties of the air environment, the space under the horizontal plate can be filled with a dielectric material in the PIFA design. This option was proposed by Ericsson Microwave Systems specialists for realization of communication via Bluetooth in the frequency range 2.40-2.48 GHz (l »12 cm) [4]. The measured bandwidth of such a PIFA with a dielectric gap at a resonant frequency of 2.46 GHz was 102 MHz. The expansion of the strip was facilitated by a rectangular cutout in the horizontal segment of the antenna. In fact, such an antenna is a microstrip version of PIFA. Therefore, in some publications, for the analysis of such devices, it is recommended to use the theory of microstrip or printed antennas.

Minh-Chau T. Huynh did not take into account the influence of the position of the feeder line connection point on the resonant properties of PIFA. However, according to the scientists of the Institute of Telecommunications of Portugal, changing the location of contact with the feeder can lead to a change in the resonance frequency of PIFA, and also entail a narrowing or widening of its bandwidth [5].

The lack of relationships that take into account the influence of the location of the feeder line forces the researchers to apply numerical optimization methods that allow using the "feeder effect" to achieve the required PIFA parameters. In particular, one of the directions for improving the technology of PIFA design is the optimization of the location of the feeder contact in conjunction with the selection of other geometric parameters of the antenna using genetic algorithms. A genetic search based on a 6-bit "chromosome" followed by modeling of the antenna variants by the FDTD method (finite element method with time separation) was used by the authors of [5]. The specified antenna bandwidth (cost function) was evaluated for each variant of the construction of PIFA (i.e., the corresponding "chromosome") by numerical simulation of its electrodynamics. The main block of the genetic algorithm, the "chromosome", is known to consist of "genes", described as sequences of units and zeros. In this case, each gene is associated with the parameter to be optimized.

For the PIFA considered in [5], the search for the optimal geometric configuration was carried out in the space of three controlled parameters - the feeder wire coordinates fx, fy and the height h of the horizontal plate. For these parameters, four possible discrete values were assigned, which corresponds to 2 bits of information. That's why the total number of bits in the "chromosome" was six. For each geometry, the bandwidth was calculated by simulation. The optimization criterion was the maximum bandwidth of the projected PIFA 2-GHz band. If during the optimization process a configuration variant was defined that satisfies the condition of reaching a bandwidth equal to or greater than the specified, the enumeration process ceased. It is significant that in this case the Minh-Chau T. Huynh relations were used as the initial approximation for constructing the first antenna model in the iteration process. As a result, for the PIFA 2-GHz band, the horizontal pad dimensions were 22x14 mm with the width of the grounding plate D = 2 mm. The feeder radius during the simulation was 0.45 mm and did not change during the search. The use of genetic optimization allowed finding a model with a bandwidth of 460 MHz and a minimum VSWR = 1.02 at a resonance frequency of 2.28 GHz. Such optimization could be carried out by the usual search of all possible parameter values, however, the genetic algorithm allows to shorten the search time to reasonable limits.

Further expansion of the PIFA bandwidth can be achieved by introducing into the antenna design an additional horizontal plate, in fact - the second floor removed from the screen by the height of h1 [5]. In the variant of double PIFA considered in [5], the feeder and the closing plate common for both floors were used. The dimensions of the horizontal segments were the same. Application of the optimization genetic algorithm allowed to obtain a variant of double PIFA with a bandwidth of 570 MHz with a minimum of VSWR = 1.09 at a frequency of 2.36 GHz. For this

model the coordinates of the feeder contact were set equal to fx = 6 mm, fy = 10 mm, the heights h = 4 mm, h1 = 8 mm at the radius of the wire feeder of 0.45 mm and the dimensions of both horizontal plates 22x14 mm.

In the optimization process, a 7-bit "chromosome" was used, in which an additional parameter (the height of the second plate) was represented by 1 bit.

The variant of PIFA, with the dimensions of the horizontal segments of 22x14 mm and the non-optimal values of the geometric parameters h = 6 mm, h1 = 10 mm, D = 2 mm and fx = 4 mm - considered by the same authors is characterized by a narrower bandwidth (14.5%) [6]. The value of the other coordinate of the feeder contact fy in [6] is for some reason not given, apparently, at that time the authors did not attach it to the influence of special significance. It was shown that for such an antenna, with increasing inter-segment distance and removing horizontal segments from the screen, the resonance wavelength of the radiation increases. The authors also noted the unevenness of the directional properties of the antenna, depending on the direction of arrival of the signals [6]. Unfortunately, information on the spatial selectivity of the optimized version of the double PIFA in [5] is not given.

The restrictions on the geometry of the double PIFA adopted in [5, 6], in principle, are not mandatory. This was confirmed by the further development of the two-storey concept of PIFA [7]. In these cases, the top plate is not connected to the feeder, which turns a two-story structure, in fact, into a hybrid of the planar inverted L-antenna (PILA) and PIFA. Differences in the dimensions of the plates and the conditions for their connection lead to a splitting of the frequency characteristic of the antenna in the vicinity of its resonance into two pronounced dips. For the double PIFA variant obtained using the optimization genetic algorithm, these frequency response dips were located so close to each other that the VSWR values merged into a continuous resonant minimum.

To determine the impedance of an antenna type PILA-PIFA, scientists from the Helsinki University of Technology proposed to use its equivalent circuit [7]. As seen from this scheme, the second floor corresponds to a series-connected capacitive element, which is due to the lack of a feeder contact.

The design, in which the lower horizontal plate is devoid of a shorting segment and connected only to the feeder, can be considered as a degenerate version of the double PIFA [2]. There is a capacitive connection between the two horizontal segments, allowing signals to pass from the feeder to both floors and back. This design with extended bandwidth is called WC-PIFA (Wideband Compact PIFA), i.e. "broadband compact PIFA" [2]. It was proposed, researched and patented by Minh-Chau T. Huynh in conjunction with Professor Virginia Tech Antenna College, Warren L. Stutzman [8]. In relation to the VSWR minimum, the bandwidth of the WC-PIFA variant was 36.3% of the carrier [2]. But in the patent [8], improved versions of the antenna with a bandwidth of up to 43-49% have been described. This is a very impressive result, if we take into account that the values of the band of the best PIFA instances are only about 10-12%. In this case, the dimensions of WC-PIFA without taking into account the screening segment, which the authors rightly regard as part of the antenna, can be noticeably smaller than the dimensions of the classical PIFA.

The disadvantage of the WC-PIFA antenna is the unequal selective selectivity for vertical and horizontal polarization waves. The greatest imbalance in the signal levels is observed in the z-x plane, which can lead to a deterioration in the reception quality of signals with the corresponding orientation of the antenna of the mobile terminal. However, the influence of the user's body inevitably makes adjustments to these characteristics. This is likely to be accompanied by alignment of the radiation patterns on waves of different polarizations.

It should be noted that WC-PIFA can also be performed with a dielectric layer between horizontal segments. Such an interlayer degrades the design frequency dependence of the VSWR antenna type WC-PIFA in free space. However, when the antenna is placed in a plastic housing,

such as a mobile phone, the interlayer reduces the influence of external objects, including the user's body, on the frequency response.

Finally, we compare the quality factor of WC-PIFA with the fundamental limits of this parameter [9]. It is noteworthy that the Q-factor of the WC-PIFA antenna, which can not be considered to be electrically small in size, agrees well with the boundary specified by Grimes [10].

It is important to note that in determining the radius of the sphere describing the antenna, Minh-Chau T. Huynh in [2] proposed to distinguish between infinite and finite in size screens. With an infinite screen (substrate) in the radian sphere, it is necessary to inscribe the antenna and its mirror image with respect to the conducting surface. This is the case when calculating the Q-factor of the PIFA placed above an infinite conducting plate. However, for finite screen sizes, as in WC-PIFA, the sphere described around the antenna, according to [2], should include a screen. This technique is the reason for such large differences in the positions of points corresponding to PIFA with an infinite screen and WC-PIFA. Unfortunately, the authors of [2, 9] confined themselves to specifying only one point for WC-PIFA on the graph, which is clearly insufficient to confirm the operability of the technique involving the inclusion of the screen in the inner volume of the spherical boundary. To verify the validity of such an approach, it would be necessary to investigate the quality factor of WC-PIFA with different sizes of the shielding plate. But this was not done.

In any case, the results obtained in [2, 9] allow us to conclude that the quality factor of the planar version of PIFA is closer to the fundamental limit than the quality factor of the wire versions of IFA and DIFA. However, it is not clear why the authors of [2, 9] used antenna designs that differ in their maximum dimensions for comparison. In addition, the data disagree with the statement that the WC-PIFA dimensions are smaller than the PIFA for the same frequency. It would be more correct to compare all the considered antennas at the same value of the product ka or the resonant frequency. But similar comparisons in the literature have not yet been encountered.

The obvious drawback of the considered "two-story" PIFA - a relatively large size. Therefore, the method of expanding the bandwidth of the type of antennas of this type due to the milling of slots of various geometries in a horizontally disposed plate has become more widespread [11, 12]. The cuts also increase the electrical length of the antenna, which makes it possible to reduce its dimensions, and at certain geometric PIFA ratios it can be given multi-band properties.

Multi-band PIFA

For the first time the possibility of realizing multi-band PIFA due to milling in a horizontal L-slotted plate was proposed in 1997 by scientists from the University of Birmingham [13]. The cut of the horizontal plate actually divided it into two independent segments (for frequencies of 900 MHz and 1.8 GHz). At resonant frequencies, the decoupling between the segments was 17 dB. At the same time, the bandwidth at 900 MHz was 63 MHz, and at a frequency of 1.8 GHz it was 110 MHz. The obtained results served as an impetus to the emergence of a new direction of designing PIFA, based on various configurations of slots. Initially, it was about sections of simple geometric shapes. Such forms in some cases allowed for an analytical calculation of the resonant frequencies. For example, for a two-frequency PIFA with a U-shaped slot, the lower resonant frequency is determined by the dimensions of the horizontal plate. It can be calculated from the ratio of Minh-Chau T. Huynh for the resonant wavelength of PIFA.

As the geometry of the sections becomes more complicated, the calculation of PIFA parameters and their optimization became possible only with the help of computer simulation in combination with the art of empiricism. This art was fully manifested, for example, in the construction of PIFA with a "meander" plate [3]. During the experiments it was found out that the presence of several identical slots allows to reduce the PIFA dimensions to 1/8 of the wavelength, without changing the bandwidth (about 10%). To reduce the height of the horizontal segment above the screen and provide broadband properties, a low-resistance resistor can be used instead of a vertical shorting section in a PIFA with a meander plate. The value of its resistance determines the operating frequency and bandwidth of the antenna (see table). It is easy to see that with

increasing resistor value the bandwidth of operating frequencies widens, reaching 11.2% (resistance of the resistor is 6.8 Ohm). However, it should be borne in mind that the inclusion of the resistor leads to a loss in gain of the antenna, estimated at 6 dB at a nominal value of 5.6 Ohm. In addition, too small a distance from the screen, which in the example considered is 0.01 wavelength of radiation, leads to a noticeable effect of the screen size on the electrical properties of PIFA. In particular, the relative bandwidth of the operating frequencies increases with the size of the grounded substrate. Its large dimensions make it possible to partially compensate for antenna gain losses caused by the resistive load. With a screen size of ~ 0.9 l, you can achieve an increase in the antenna gain to 5 dB. In addition, the extended screen serves as a reliable barrier to the propagation of radio waves towards the body of the user.

Minh-Chau T. Huynh in [2] paid much attention to the study of the effect of screen sizes on the properties of PIFA. However, it should be noted that his insufficient methodological skill did not allow to determine the influence of the screen on the properties of the PIFA, and not related to the change in its dimensions of the feeder contact movements. The thing is that Minh-Chau T. Huynh tried to compensate for the violation of the antenna matching conditions when changing the size of the square screen by moving the contact point of the feeder line with the horizontal PIFA segment along the x-axis passing through the center of the short-circuiting segment, achieving 50-ohms of the internal resistance of the line . From the data obtained by him it is not clear what influences the change in the characteristics of the antenna: the screen size or the coordinates of the feeder pad. Only with the transition to a rectangular shielding surface and a change in its dimensions along two axes, with the same coordinates of the feed contact of Minh-Chau T. Huynh managed to fix the influence of the screen itself. Along with the frequency response, as expected, the directional properties of the antenna also change.

Stable operation of PIFA with slots at several frequency resonances ensures their multi-range. However, in cases where the frequency multiplicity is not possible, it is often resorted to trivial solutions consisting of a combination of several different meanders [11]. Used and additional grounded screens in the form of passive PILA-antennas and capacitive loads. Adding load capacitances (line segments with negative reactance) makes it possible to shift the resonant frequencies to a lower frequency region.

An example of the frequency response of such an antenna design is shown in, and the characteristic cross sections of its directivity diagrams at resonant frequencies of 1710 MHz and 2170 MHz.

Research in this direction made it possible to obtain more complex than the meander, PIFA designs that ensure the operation of a mobile communication device simultaneously in four or five bands of the electromagnetic spectrum. A variant of the geometry of such an antenna that supports the work in the GSM band with VSWR J 2.5, and in the range of DCS, PCS, UMTS with VSWR. The main horizontally located antenna plate has a quarter-wave resonance, which in this case falls within the GSM band (935 MHz). Since the third harmonic of the main plate (2805 MHz) lies outside the next interesting band 1710-2170 MHz, the developers resorted to the help of a capacitive load, shifting the frequency of the third resonance to the range of DCS, PCS, UMTS. Additional grounded L-antennas (passive PILA) with their own capacitive loads allow to extend the bandwidth in a given portion of the spectrum. It should be noted that there are clearly defined frequency regions corresponding to the possibility of efficient reception of signals. This antenna, given, differs from an alternative quad-band solution proposed by specialists of the University of Queensland (Australia) [17]. Quartet resonance in it is achieved by the execution in a horizontal surface of three parallel slots of different lengths. In this case, the lower resonant frequency is determined by the dimensions of the plate, and the position and dimensions of the slits affect the higher resonances. The scientists of the university modeled the PIFA variant with the following geometric parameters (in millimeters): Ly = 51.5; L1 = 23.6; L2 = 29.9; L3 = 33.35; G1 = 6.0; G2 = 7.0; F = 22.0; Wx = 60.0; WA = 23.9; WB = 3,4; WC = 7.2; WD = 13.0, height - 4 mm, width of the short-circuiting segment - 5.5 mm. As a result of the simulation, it was found that at the

indicated geometrical ratios, the resonance in the reception of signals is provided at frequencies of 870 MHz, 1.8 GHz, 2.04 GHz and 2.4 GHz with passband bandwidths of 10 dB-329 MHz (37 , 8%), 172 MHz (9.6%), 192 MHz (9.4%) and 247 MHz (10.3%), respectively. As a result, the antenna can operate in the frequency bands of mobile communication systems of the GSM900, DCS1800 and UMST (1983-2175 MHz) standards, as well as the frequencies of the Bluetooth standard (2373-2620 MHz).

From the calculated frequency characteristics of the simplest quad-band PIFA, it can be seen that the conditions for receiving signals at the higher resonance deteriorate. This entails corresponding distortions in the antenna pattern. The obtained results clearly illustrate the possibilities of multiband radiation and PIFA reception of both horizontally and vertically polarized waves with a single-port feeder [17]. This is why PIFA is preferred in mobile communications, where an arbitrary orientation of the antenna in space is possible. In addition, as noted in [17], in the case of double polarization signals, PIFA selects both orthogonal field components with an almost equal transmission coefficient, whereas one of the polarization components dominates the microstrip antennas.

Optimizing the location and dimensions of the slots in the structure is an extremely difficult task. Small changes in geometric dimensions can lead to a noticeable deterioration in the efficiency of the antenna. Therefore, in numerical simulation, it is necessary to minimize the step of discretization of the optimized quantities. This is confirmed by the results of calculating the frequency response of the simplest quad-band PIFA for the sample lengths of the slit L1. Therefore, the trivial solution proposed by scientists from the University of Queensland, can be considered unpromising for serially produced antennas, differing in the technological spread of geometric parameters. And even more so do not try to distribute this solution to antennas with a large number of operating ranges.

The first of the known five-band antennas was developed by the specialists of Chalmers University of Technology (Sweden) [16]. Its dimensions and appearance are the development of the antenna design. The main task in designing this antenna was to provide the same resonant frequencies as the antenna, with the addition of a 5-GHz WLAN band. The extent to which this is possible can be judged from the results of the resulting bandwidth of the VSWR antenna no worse than 2.5: 70 MHz in the GSM band (870-940 MHz), 476 MHz in the DCS / PCS / UMTS band (1608-2804 MHz) and 1128 MHz in the WLAN band (4863-5991 MHz). The coverage of the 5-GHz band is achieved by combining the higher harmonics of the main plate with a capacitive load (5.3 GHz) and the seventh harmonic of the additional (No. 1) L-antenna (5.9 GHz). Parasitic reception bands around 3.6 and 4.5 GHz are easily suppressed by the selective circuits of signal processing equipment.

Thus, the PIFA antennas of multi-band mobile communication devices evolved, in fact, into a complex antenna complex consisting of several interconnected active and passive elements [18]. In fact, the combination of different in design segments in a single multi-band antenna module has become the main method in the arsenal of developers of broadband radio equipment. Naturally, the variants of constructive solutions considered here cover only the most characteristic, key approaches to designing antennas of the PIFA family. Far from each of them will be in demand by manufacturers of serial devices. Most will remain the historical backdrop of the theory's progress. Among these, for example, are PIFA-like antennas with an extended three-dimensional topology, called "Bent Inverted-F Antenna, BIFA" [19]. These are the costs of evolutionary selection. Among the favorites - a variety of PIFA-designs, including with integrated microstrip and dielectric resonant antennas. Appropriate technical solutions will be considered in the next issue of the journal.

Literature:

1. Slyusar V.I. Multi-band antennas for mobile communications. - ELECTRONICS: NTB, 2006, №8.

2. Minh-Chau T. Huynh. A Numerical and Experimental Investigation of Planar Inverted-F Antennas for Wireless Communication Applications. – In: Master Thesis of Science in Electrical Engineering. – Virginia Polytechnic Institute and State University. – Blacksburg, Virginia. – Oct. 19, 2000. – 123 p. – http://scholar.lib.vt.edu/theses/available/etd-10242000-22130026/unrestricted.
3. Nathan P. Cummings. Low Profile Integrated GPS and Cellular Antenna. – In:Master Thesis. – Blacksburg, Virginia Polytechnic Institute. – Oct. 31, 2001.– http://scholar.lib.vt.edu/theses/available/ etd-11132001-145613/unrestricted/etd.pdf.
4. Redvik J. Overview of Small Antennas at EMW.– In:
COST 260 Management Committee and Working Groups Meeting, Gothenburg, Sweden, May 2–5, 2001. – Small Antenna Group Antenna Research Center. – Ericsson Microwave Systems AB. – http://www.rc.fer.hr/ cost260/gothenbu/gop33.pdf.
5. Pinho P., Pereira J. F. Rocha. Optimisation of a PIFA Antenna Using Genetic Algorithms. – In: 3rd Conference on Telecommunications (ConfTele 2001). – April 23–24,
2001. – http://www.co.it.pt/conftele2001/proc/ pap060.pdf.
6. Pinho P. and Pereira J.F. Rocha. Design of a PIFA antenna using FDTD.– In: 2nd COST 260 Workshop on Smart Antenna Computer Aided Design & Technology. –
Aveiro, Nov. 3–5, 1999. – http://www.rc.fer.hr/ cost260/aveiro/p110.pdf.
7. Ollikainen J., Vainikainen P. Design and Bandwidth Optimization of Dual-Resonant Patch Antennas. – Helsinki University of Technology. Radio Laboratory Publications. REPORTS 252. – Espoo. March, 2002. – http://lib.tkk.fi/ Diss/2004/isbn9512273810/article1.pdf.
8. Patent 6,795,028 USA. H01Q 1/24. Wideband Compact Planar Inverted-F Antenna/ Warren L. Stutzman, Minh-Chou Huynh. – Date of Patent: Sept. 21,2004. – PCT Filed: Apr. 27, 2001.
9. Stutzman W. and Davis B. Antennas for Wireless Communications – Basic Principles and System Applications.– Virginia Tech Antenna Group. – June 9, 2006. – http://wireless.vt.edu/tutorials/Stutzman_Davis.pdf.
10. Слюсар В.И. 60 лет теории электрически малых антенн. Некоторые итоги.– "ЭЛЕКТРОНИКА: НТБ, 2006, № 6.
11. Kin-Lu Wong. Planar Antennas for Wireless Communications. – New York, Wiley-Interscience.
2003, 301 p.
12. Causley A.J. Design of Conformal Antennas for Telephone Handsets. – In: Bachelor of Engineering Honours Thesis. – The University of Queensland. 2002, 117 p. – http://innovexpo.itee.uq.edu.au/2002/ projects/s354019/thesis.pdf.
13. Liu Z.D., Hal P.S., &. Wake D. Dual Frequency Planar Inverted-F Antenna.– IEEE Transactons on Antennas and Propagaton. Oct. 1997, v.45, N 10, p. 1451–1457.
14. Wan Tsui Fung J. A Small Antenna for Wearable Application. – Queen Mary University of London. – Department of Electronic Engineering. 2003, 75 p. – http://www.elec.qmul.ac.uk/staffinfo/davew/ reports_pdfs/IC_projects/IC2003/ic3016-1_report.pdf.
15. Ollikainen J., Kivekas O., Toropainen A. and Vainikainen P. Internal Dual-Band Patch Antenna for Mobile Phones.– In: Proceedings of the AP2000 Millennium Conference on Antennas & Propagation. Davos, Switzerland, April 9–14 2000. – http://lib.tkk.fi/Diss/2004/isbn9512273810/article7.pdf.
16. Ciais P., Luxey C., Diallo A., Staraj R.,. Kossiavas G. Design of Internal Multiband Antennas for Mobile Phone and WLAN Standards. – In: Joint COST 273/284 Workshop on Antennas and Related System Aspects in Wireless Communications, June 7–10, 2004. – Chalmers University of Technology Gothenburg, Sweden. – http://www.s2.chalmers.se/costworkshop

Свердлюк Роман Ігорович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м.Київ

RED5 МЕДІАСЕРВЕР

Red5 є вільним програмним забезпеченням потокове медіа - сервер реалізований в Java, яка надає послуги , аналогічні тим , які пропонуються у власність Adobe Flash Media Server і Wowza Streaming Engine

Red5 є відкритим вихідним кодом. Це медіа-сервер для живих потокових рішень усіх видів. Він розроблений, щоб бути гнучкими з простою архітектурою плагіна, який дозволяє налаштовувати практично будь-які VOD і сценарії потокових. Red5 був і в даний час використовується тисячами компаній включаючи Amazon та Facebook.

Вперший створений в 2005 році групою розробників, на основі Real Time Messaging Protocol, як альтернатива Flash Communication Server, Red5 тепер використовується для потоковим Flash включаючи HLS, WebSockets, and RTSP. Проект був створений в рамках

Google Summer of Code, команда Red5 в даний час будує підтримку WebRTC, щоб включити потокову передачу в браузері без плагіна.

Red5 Pro, платна, ліцензійна версія Red5 з SDKs для мобільного (Android і IOS) і високої масштабованості кластеризації доступна на http://red5pro.com .

Завдяки використанню Red5 Media Server, ви розробляєте дійсно відкриту і розширювану платформу, яка може бути використані в відеоконференціях, ігрових стрімах багатокористувацьких і програмного забезпечення корпоративних додатків.

Red5 Open Source Flash Server з підтримкою Java підтримує:

- Потокове відео (FLV, F4V, MP4, 3GP)
- Streaming аудіо (MP3, F4A, M4A, AAC)
- Запис користувацьких прямих включень (FLV and AVC+AAC in FLV container)
- Можливість ділитись файлами
- Стріми та включення в реальному часі
- А також протоколи: RTMP, RTMPT, RTMPS, and RTMPE
- Порівнянння Wonwza та RED5

Література:

1. *red5.org*
2. *ru.wikipedia.org/wiki/Red5*

Король-Королевський Кірілл Андрійович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м.Київ

ТЕХНОЛОГІЯ 5G МОЖЕ ВИЯВИТИСЯ НЕ ТАКОЮ, ЯК МИ ОЧІКУЄМО

"Швидше вище сильніше!" - каже олімпійський гасло. Тому перша демонстрація нового покоління бездротових технологій під час зимової Олімпіади здавалася цілком доречною. Коли розробка остаточно завершиться, 5G повинен запропонувати користувачам 20 гігабітну швидкість інтернету, випереджаючи 4G вдвічі. І при цьому демонструвати час відповіді нижче однієї мілісекунди.

Таким чином, нова мережа зможе передавати відео високої роздільної здатності за дві секунди, а відповідати на запити зі швидкістю моргання ока. Але 5G - це не тільки більш швидке бездротове з'єднання.

Про це пише The Economist, додаючи, що технологія повинна відкрити дорогу для цілої плеяди нових послуг. Одна з них може пропонувати щось з віртуальної або розширеною реальністю. На Олімпіаді в Південній Кореї, наприклад, за багатьма учасниками стежили панорамні камери. І завзяті фани могли надягти спеціальні окуляри і відправитися таким чином прямо на поле змагань. Але 5G повинен стати сполучною тканиною для всіх інтернет речей, об'єднуючи все від смартфонів до бездротових сенсорів, від виробничих роботів до безпілотних автомобілів. Це буде можливо завдяки технології, яка називається "розшарування мереж", яка дозволить операторам швидко створювати мережі на вимогу, надаючи кожному з приладів саме такий зв'язок, який їм потрібен.

Незважаючи на свою універсальність, поки не відомо, як швидко відбудеться запуск 5G. Найбільшим гальмом для цього буде економіка. Коли компанія GSMA в минулому році запитала у директорів 750 телеком-компаній про найбільшу перешкоду для впровадження 5G, більше ніж половина з них послалася на відсутність реального обґрунтування. Люди може і хочуть більш високу пропускну здатність мережі, але вони не хочуть платити за це. І такий стан речей навіть приманка з віртуальною реальністю навряд чи змінить.

Побудова самої інфраструктури для 5G теж не буде дешевою. Тому що для роботи на вищих частотах буде потрібно більше антен, базових станцій і оптоволоконних кабелів для з'єднання.

Аналітики очікують, що оператори зв'язку виведуть 5G на ринок більш поступово, ніж попередні покоління технології бездротового зв'язку, і тільки в тих місцях, де це буде вигідно. Деякі спочатку використовують технологію для забезпечення надшвидкого "фіксованого" бездротового зв'язку. Це буде зробити простіше. Інші ж спробують побудувати покриття в густо населених містах. Іншими словами, 5G може повторити досвід 3G, який був запущений на початку 2000-х років. Технологія розчаровувала до тих пір, поки не знайшла ідеальне застосування з появою смартфонів, але це сталося майже через десятиліття. І тільки з 4G бездротовий мобільний інтернет виконав обіцянки, які давалися ще при запуску 3G. Наприклад, транслювати відео з мінімальними затримками вдалося лише з появою наступного покоління. Тому не виключено, що для отримання істинного 5G, людям доведеться почекати його наступника.

Література:

https://zn.ua/TECHNOLOGIES/tehnologiya-5g-mozhet-okazatsya-ne-takoy-kak-ee-predstavlyayut-the-economist-275204_.html

Холявко Олександр Юрійович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м.Київ

АТАКИ ПОВ'ЯЗАНІ З RFID

RFID (Radio Frequency IDentification) - широковикористована технологія автоматичної ідентифікації, в якому за допомогою радіосигналів зчитуються і записуються дані. Дані зберігаються в так званій RFID - мітці. RFID-система складається з рідера й мітки. Хоч сьогодні RFID вважається сучасно і безпечною технологією я б хотів розказати про вразливості цієї системи. Нижче представлений невеликий список вживаних атак:

- Dos-атака
- RFID-Zapper
- Клонування
- Підміна вмісту пам'яті RFID-міток
- Атаки на організації через RFID-мітки

Dos-атака

RFID першого покоління схильні Dos-атаці. Суть в тому, що чіпи цього покоління використовують діапазон 902-938 МГц, розділений на канали. Даний діапазон можна заглушити з відстані в 1 м. За допомогою нескладного радіопередавача який буде перемикатися з одного каналу на інший, а чіп в силу своєї пасивності не може змінити діапазон. У зв'язку з цим наводиться досить абстрактне порівняння з Dos-атакою.

RFID-Zapper

Наступна атака - це просте знищення мітки. Двоє хлопців з лав «Хаосу» прийшли до висновку, що перебування чіпа в мікрохвильовці протягом короткого часу є найдієвішим способом знищення мітки. У зв'язку з цим був розроблений девайс RFID-Zapper, який створює сильне електромагнітне поле, яке вбиває пасивні мітки.

Клонування

Джонатан Вестхьюз (Jonathan Westhues) - студент, який створив пристрій, що дозволяє клонувати мітки. Девайс названий proxmark. Він легко поміщався в кишеню і при досить близькій відстані можна непомітно клонувати мітку.

Підміна вмісту пам'яті RFID-міток

На завершилася хакерській конференції Defcon німецький експерт інфосека Лукас Грюнвальд (Lukas Grunwald) продемонстрував, як вміст електронного паспорта може бути легко перенесено на будь-яку іншу радіомітку, за допомогою програми RFDump, яка вміє зчитувати, редагувати, записувати (якщо це можливо) дані RFID-міток.

Після створення своєї програми Лукас і Борис зайнялися активним вивченням можливості злому різних RFID-систем. Спочатку вони вивчили RFID-систему місцевого університетського кафе, де дані про суму на рахунку клієнта зберігалися прямо на картці. Харчування там стало для них безкоштовним. Далі вони зупинялися в готелях і готелях, в яких для входу в номер використовувалися proximity-карти, і Грюнвальд після вивчення 2-3 карт міг створити майстер-карту, що відкриває будь-які двері. Уразливими виявилися і системи супермаркетів, де почали застосовувати RFID як альтернативу штрихкод. Хакери отримали можливість за допомогою кишенькових комп'ютерів поміняти мітки дорогих товарах на менш дорогі, «рятуючи» таким чином свою готівку. За словами Грюнвальда, 3/4 всіх вивчених їм RFID-систем виявилися так чи інакше уразливі.

Атаки через RFID-мітки

Насправді через редагування мітки можна отримати доступ до комп'ютера і тим самим здійснювати різного роду атаки. Уразливі місця RFID-мітки: SQL-Injection, web-інтерфейси, де не виключена можливість впровадження шкідливого коду.

Припустимо, в RFID-системі використовуються тільки мітки з об'ємом пам'яті 128 байт. Програміст, який писав додаток що обробляє вміст тегів, полінувався зробити перевірку на довжину цього самого вмісту. В результаті є можливість для переповнення буфера, адже хитрий хакер може підсунути мітку з вмістом більше ніж 128 байт, запровадивши туди і вірусний код.

Приклади реальних атак

Щоб було ясно які види проблем можуть виникати від RFID-хакінга розглянемо сценарій реальної атаки.

- «Жартівник» йде в супермаркет, в якому сканує продукти в кошиках. Продукція магазину оснащена RFID-мітками, а не штрих-кодами. Багато супермаркетів планують ввести систему RFID, оскільки сканування відбувається набагато швидше. «Жартівник» вибирає продукт, наприклад, шоколадну пасту, сканує і йде на касу його оплачувати. Прийшовши додому, він видаляє і знищує RFID-позначку (знищити мітку можна способами, описаними в пункті RFID-Zapper). Потім він бере порожні RFID-мітки і пише експлойт на комп'ютері, який надалі прикріпить до мітки. Далі інфікована мітка прикріпляється до шоколадної пасти і відноситься в магазин. «Жартівник» знову її купує, касир сканує і в цей сумний момент заражається вся база даних супермаркету.

- Ігри нашого «жартівника» тривають. У нашого героя є кішка, у якої є підшкірна ID-мітка, яку «жартівник» може перезаписати на який-небудь експлойт з використанням комерційно доступного обладнання. Далі, він йде до ветеринара зі скаргою, що кішка завжди вимагає їжі. Ветеринар сканує і відбувається те ж саме, що і в попередньому оповіданні - заражається база даних і дана дія призводить до хаосу.

- І найстрашніша частина. Аеропорти теж планують ввести RFID-мітки, які будуть кріпитися до багажу. Це обумовлено тим, що RFID-мітки можливо зчитувати на великій відстані, ніж штрих-коди багажу. Принцип дії той же самий - приходить злий мандрівник з інфікованою міткою, його сканують. Тільки наслідки набагато небезпечніше - можуть бути заражені сотні аеропортів по всьому світу. Багато компаній на даний момент стверджують, що їх ПЗ відображають дані види атак.

Література:

1. https://habrahabr.ru/post/148663/

Говгаленко Максим Петрович

Державний Університет Телекомунікацій
Факультет Телекомунікацій
м. Київ

АНАЛІЗ ТЕХНОЛОГІЇ ДЛЯ M2M МЕРЕЖ З ВЕЛИКОЮ ПЛОЩЕЮ ПОКРИТТЯ

У зв'язку зі значною кількістю різних технологій радіозв'язку, що застосовуються для підключення пристроїв IoT, і великого різноманіття смуг радіочастот, в звіті наведено детальний опис класів таких технологій разом з конкретними прикладами технологій. Особливу увагу слід приділити новому класу радіотехнологій, оптимізованих для обслуговування різних датчиків і сенсорів, що працюють довгий час від батарейок і маютьвелику дальність, отримав назву LPWAN

Додатки M2M, яким необхідна велика дальність зв'язку або велика зона покриття, широко використовують стільникові мережі. Найкращою стільникового технологією в даний час є UMTS, частково через її низьку вартість, а також тому, що це єдина технологія передачі даних, яка в даний час забезпечує покриття на національному рівні. Однак останнім часом розробляється багато технологій для роботи в безліцензійних смугах частот, які націлені на даний сегмент застосувань M2M. Зокрема, інтерес проявляється до конкретних технологій M2M, які оптимізовані для виконання великого числа з'єднань, але при відносно невеликих обсягах, переданих даних.

В першу чергу дані технології передбачається використовувати в різних системах інтелектуального обліку. Інтелектуальні лічильники все частіше застосовуються в системах по оптимізації використання електроенергії. Як доповнення до стільникового UMTS-мережі для передачі даних від інтелектуальних лічильників до мережевого вузла будуть використовуватися вузькосмугові системи в окремих смугах частот. Існує ряд комерційних компаній, які пропонують розгортання виділеної бездротової вимірювальної інфраструктури в це дозвіл частот 410-430 МГц, і які планують використовувати існуючі мережі для забезпечення великого охоплення території в поєднанні з низьким енергоспоживанням комплектуючих системи.

Бездротові технології M2M, що не відносяться до стандартів стільникового зв'язку або мобільного широкосмугового доступу, але забезпечують широке охоплення.

У 2015 році Semtech Corporation і дослідницький центр IBM Research був представлений новий відкритий енергоефективний мережевий протокол LoRaWAN (Long Range Wide Area Networks) для бездротової передачі даних з і на пристрої IoT, а також був створений альянс LoRa Alliance для просування даного стандарту[1]. Стандарт є відкритим за винятком реалізації на чіпі, яка контролюється Semtech Corporation.

В основу сигналу LoRa покладено канал 125 кГц з сигналом на основі розширення спектра шляхом лінійної частотної модуляції (CSS - chirp spread spectrum) з інтегрованою прямий корекцією помилок FEC. Однак основною особливістю LoRa стало створене навколо стандарту співтовариство, яке почало активно впроваджувати даний стандарт як в якості операторської технології (країни Європи), так і в якості локальних рішень для окремих будівель або невеликих підприємств (країни Азії). Зокрема, даний стандарт був підтриманий деякими великими стільниковими компаніями, що ще більше підштовхнуло розвиток екосистеми для даного стандарту. Відкритість бізнес-моделі стандарту (за винятком чіпа) дозволила операторам інтегрувати рішення LoRa в свою діючу інфраструктуру. Загальна схема організації сервісу на основі LoRa показана на рис.1. Відмінністю цієї схеми від таких технологій як «Стриж» та Sigfox є можливість організації власних серверів на базі одного з доступних програмних рішень від спільноти розробників LoRa.

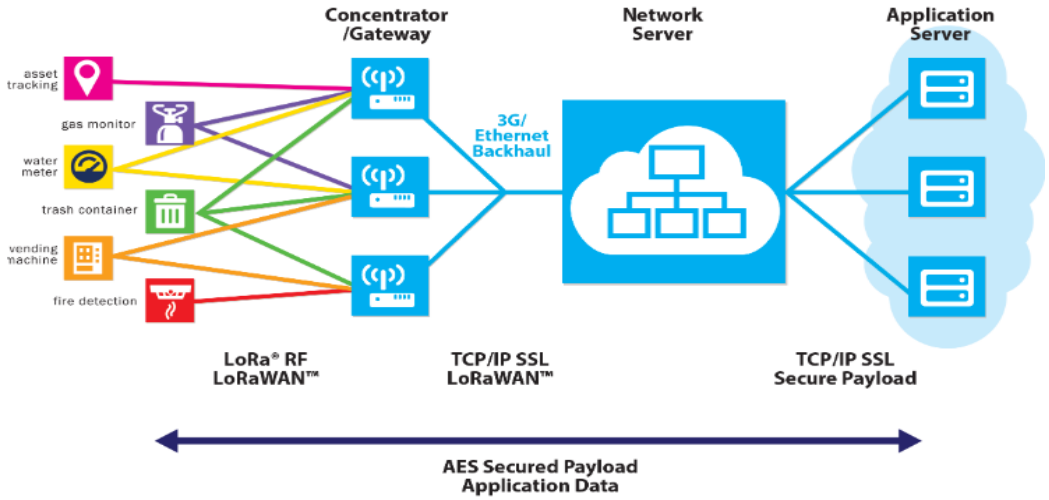


Рисунок 1 - Схема організації мережі LoRa

Ключові канали оповіщення і зв'язку з пристроями для Європейського ринку зосереджені в смугах радіочастот 868.0-868.6 Мгц і 869.4-869.65 МГц. З урахуванням перевантаженості даних каналів в Європі LoRa Alliance зміг пролобіювати з іншими організаціями виділення у 2017 році чотирьох додаткових каналів в діапазоні 865-868 МГц для пристроїв малого радіусу дії.

Література:

1. Augustin A.; Yi J.; Clausen T.; Townsley W.M. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. Sensors 2016, 16, 1466.

2. Koucheryavy, A. E. Internet of Things // Electrosvyaz'. 2013. No. 1. pp. 21–24.

Гомзяк Ярослав

ДержавнийУніверситетТелекомунікацій

Факультет Телекомунікацій

м. Київ

MULTIPROTOCOL LABEL SWITCHING

MPLS - багатопротокольна комутація по мітках - механізм в високопродуктивної телекомунікаційної мережі, який здійснює передачу даних від одного вузла мережі до іншого за допомогою міток.

MPLS є масштабованим і незалежним від будь-яких протоколів механізмом передачі даних. У мережі, заснованої на MPLS, пакетам даних присвоюються мітки. Рішення про подальшу передачі пакета даних іншого вузла мережі здійснюється тільки на підставі значення присвоєної мітки без необхідності вивчення самого пакета даних. За рахунок цього можливе створення наскрізного віртуального каналу, незалежного від середовища передачі і використовує будь-який протокол передачі даних.

MPLS дозволяє досить легко створювати віртуальні канали між вузлами мережі.Технологія дозволяє інкапсулювати різні протоколи передачі даних. Основною перевагою MPLS є незалежність від особливостей технологій канального рівня, таких як ATM, Frame Relay, SONET / SDH або Ethernet; відсутність необхідності підтримки декількох мереж другого рівня, необхідних для передачі різного роду трафіку.

По виду комутації MPLS відноситься до мереж з комутацією пакетів. Технологія MPLS була розроблена для організації єдиного протоколу передачі даних як для додатків з комутацією каналів, так і додатків з комутацією пакетів (маються на увазі програми з датаграммною передачею пакетів).

MPLS може бути використаний для передачі різного виду трафіку, включаючи IP-пакети, осередки ATM, фрейми SONET / SDH і кадри Ethernet. Для вирішення ідентичних завдань раніше були розроблені такі технології, як Frame Relay і ATM. Багато інженерів вважали, що технологія ATM буде замінена іншими протоколами з меншими накладними витратами на передачу даних і при цьому забезпечують передачу пакетів даних змінної довжини з встановленням з'єднання між вузлами мережі.

Принцип роботи

Технологія MPLS заснована на обробці заголовка MPLS, який додається до кожного пакету даних. Тема MPLS може складатися з однієї або декількох «міток». Кілька записів (міток) в заголовку MPLS називаються стеком міток .

Формат запису в стек міток

32біта			
20 біт	**3 біта**	**1 біт**	**8 біт**
Label	**TC**	**S**	**TTL**

Кожен запис в стек міток складається з наступних чотирьох полів: •значення мітки(Label) займає **20 біт**;
• поле «клас трафіку» (Traffic class) використовується для реалізації механізмів якості обслуговування (QoS) і явного повідомлення (до RFC 5462 це поле називалося Exp займає **3 біти;**

• прапор «дно стека» (Bottom of stack) якщо прапор встановлений в 1, то це означає, що поточна мітка остання в стеці; займає **1 біт;**

• поле TTL (Time to live) використовується для запобігання петель MPLS комутації; займає **8 біт**.

У MPLS-маршрутизаторі пакет з MPLS-міткою комутується на наступний порт після пошуку мітки в таблиці комутації замість пошуку по таблиці маршрутизації. При розробці MPLS пошук міток і комутація по мітках виконувалися швидше, ніж пошук по таблиці маршрутизації або RIB (Routing information base - інформаційна база маршрутизації), так як комутація може бути виконана безпосередньо на комутаційної фабриці замість центрального процесора. Маршрутизатор, розташовані на вході або виході MPLS-мережі, називаються LER (Label edge router - граничний маршрутизатор міток). LER на вході в MPLS-мережа додають мітку MPLS до пакету даних, а LER на виході з MPLS-мережі видаляє мітку MPLS з пакета даних.

Порівняння MPLS і IP

MPLS як протокол некоректно порівнювати з протоколом IP, оскільки MPLS працює спільно з IP і протоколами маршрутизації (IGP).

Основні переваги технології IP / MPLS: більш висока швидкість просування IP-пакетів по мережі за рахунок скорочення часу обробки маршрутної інформації; можливість організації інформаційних потоків в каналах зв'язку. За допомогою міток кожному інформаційному потоку (наприклад, несе телефонний трафік) може призначатися необхідний клас обслуговування (CoS).

Література:

https://ru.wikipedia.org/wiki/MPLS

Жук Виктор Юрьевич
Государственный Университет Телекоммуникаций
Факультет Телекоммуникаций

г. Киев

ТЕХНОЛОГИЯ NFC

Near field communication, NFC («коммуникация ближнего поля», «ближняя бесконтактная связь») — технология беспроводной передачи данныхмалого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров; анонсирована в 2004 г. NFC нацелена прежде всего на использование в цифровых мобильных устройствах NFC — это беспроводная короткодистанционная технология, которая работает на расстоянии не более 10 сантиметров. NFC работает на частоте 13,56 МГц. NFC всегда включает инициатор и цель; инициатор активно генерирует радиочастотное поле, которое может влиять на пассивную цель. Также возможна NFC-связь между двумя устройствами при условии, что оба устройства включены. Технология NFC делает не нужными многие другие устройства, и элементы. Только смартфон, с чипом NFC используемый в качестве основного объекта повседневной жизни, будет достаточен для реализации всех ежедневных действий. Смартфоны могут быть использованы для блокировки / разблокировки дверей дома, автомобиля и офиса, оплаты за покупки, обмена визитными карточками, оплаты общественного транспорта.

Существуют три основных области применения NFC:

1) эмуляция карт: устройство NFC ведет себя как существующая бесконтактная карта;
2) режим считывания: устройство NFC является активным и считывает пассивную RFID-метку;
3) режим P2P: два устройства NFC вместе связываются и обмениваются информацией.

Рабочее расстояние с компактными стандартными антеннами: до 10 см; Поддерживаемая скорость передачи данных: 106, 212, или 424 Кбит.Существуют два режима:

Пассивный режим связи: устройство инициатор обеспечивает несущее поле, а целевое устройство отвечает посредством модулирования имеющегося поля. В этом режиме целевое устройство может вытягивать свою рабочую мощность из предоставленной инициатором электромагнитной области, таким образом делая целевое устройство ретранслятором.

Активный режим связи: и инициатор, и целевое устройство взаимодействуют путём поочередного создания своих собственных полей. Устройство дезактивирует своё радиочастотное поле в то время, как оно ожидает данных. В этом режиме у обоих устройств должно быть электропитание.

Для передачи данных NFC использует два различных вида кодирования. Если активное устройство передает данные со скоростью 106 кбит, тогда используется модифицированный код Миллера с 100 % модуляцией. Во всех других случаях используется манчестерское кодирование с коэффициентом модуляции 10 %.

Устройства NFC в состоянии одновременно и получать, и передавать данные. Таким образом, они могут контролировать радиочастотное поле и обнаруживать противоречия, если полученный сигнал не соответствует переданному.

И всё же, основная область применения технологии NFC в наши дни - безконтактные платежи. Таким образом, в Украине услуга NFC-платежей уже давно появилась в некоторых украинских банках. В начале 2017 года «ПриватБанк» запустил обновленный мобильный кошелек в приложении «Приват24». Расплачиваться в магазинах с помощью смартфона также могут клиенты «Сбербанка» (Сбер PAY), «Кредобанка» (KredoPay) и «Укрэксимбанка».

Технология Android Pay от Google стала доступной с ноября этого года.

Литература:

1) http://www.mdpi.com/1424-8220/15/6/13348/htm
2) http://nfc-ukraine.com
3) https://ru.wikipedia.org/wiki/Near_Field_Communication

Авраменко Олексій Юрійович
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

VIRTUAL REALITY: THE NEXT GENERATION OF EDUCATION, LEARNING AND TRAINING

When people hear about virtual reality (VR), images of a person wearing a headset and holding a gaming console usually come to mind. However, for the education sector, VR is an opportunity to finally connect with both learners and teachers in a novel and meaningful way. For example, EON Reality collaborated with Oral Roberts University to create the Global Learning Center, a dedicated facility for augmented and virtual learning. As the global executive director of the global VR/AR Association, I've watched our 3,900-plus registered companies work on best practices, guidelines and standards to accelerate the VR/AR industry for all, one committee in particular being devoted to education and training.

Today, VR can enable experiential learning by simulating real-world environments. Students can test their skills, record their work and interact with experts all within VR. Students have responded overwhelmingly positively to active learner engagement. A recent study shows that "93 percent of teachers say their students would be excited to use virtual reality and 83 percent say that virtual reality might help improve learning outcomes." This points to a universal trend as these students will soon enter universities and then the workforce, where job training scenarios will become the new classroom.

For visual learners and individuals with learning challenges, VR provides an alternative medium to meet their needs. Likewise, educators see increased engagement levels and improved test scores across the board with VR education programs. Hands-on learning techniques like VR education directly contribute to increased cognitive memory.

The benefits of incorporating VR/AR tech into educational experiences include better, more immediate engagement and the opportunity for learners to "feel" the experiences and better remember and express what they learned. A student can experience what was not possible to experience before and become better prepared for when such experiences occur in the real world. The basic functionality of VR in education is to bring learning to life via a virtual environment. The more a learner is able to participate in life-like engagement, the easier it is to personally feel a connection to the subject material, making it easier for application and retention of the subject matter. The most popular trends in VR learning include enterprise and education. In enterprise, Walmart is using VR to help train its employees on topics like management and customer service. Soon, all 200 of the company's U.S. training centers will use VR instruction to educate the estimated 150,000 employees going through the program annually. In education, there's Star Chart, an iOS and Android app with over 20 million users that brings the universe a little closer. Users learn about astronomy by pointing their phones to the sky at night and utilize other features to learn about planets and space discovery. It’s important to pay attention to this trend and adopt VR solutions in your organization to educate employees in new and better ways and teach students with more engaging and effective tools. However, like many new technologies before it, awareness is the first barrier to entry followed by cost and content. Many are still not aware of VR training solutions that are proving to be effective. At The VR/AR Association we are doing our part to promote the industry and help organizations locate the best VR solutions for their use case. Meanwhile, quality VR headsets come at around $399 (already down from $599 ore more just a few months ago). Cost is steadily declining our research points to $199 being the sweet spot price

point for “mass adoption.” Finally, better content — specific for each use case — is needed and is being created for enterprise use cases and educational curriculums. In 2018, we will see the costs decrease, better content emerge and more awareness spread, which will propel the VR/AR education market to high growth. Ultimately, VR in education will revolutionize not only how people learn but how they interact with real-world applications of what they have been taught. Imagine medical students performing an operation or geography students really seeing where and what Kathmandu is. The world just opens up to a rich abundance of possibilities.

Література:
1. *https://en.wikipedia.org/wiki/Virtual_reality*
2. *https://blogs.wsj.com/digits/2016/04/07/online-high-school-in-japan-enters-virtual-reality/*

Каграманова Юлия Константиновна
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
г. Киев

WEBRTC

WebRTC — проект с открытым исходным кодом, предназначенный для организации передачи потоковых данных между браузерами или другими поддерживающими его приложениями по технологии точка-точка.

WebRTC - это открытая инфраструктура для Интернета, которая позволяет общаться в режиме реального времени в браузере. Он включает в себя фундаментальные строительные блоки для высококачественной связи в Интернете, такие как сетевые, аудио и видеокомпоненты, используемые в приложениях голосовой связи и видеочата.
Эти компоненты, реализованные в браузере, могут быть доступны через JavaScript API, что позволяет разработчикам легко реализовать свое собственное веб-приложение RTC.
Усилия WebRTC стандартизируются на уровне API на уровне W3C и на уровне протокола в IETF.

Почему я должен использовать WebRTC?

Мы думаем, что вы захотите создать свое следующее приложение для видеочата с помощью WebRTC. Вот почему: Ключевым фактором успеха Интернета является то, что его основные технологии, такие как HTML, HTTP и TCP / IP, являются открытыми и свободно реализуемыми. В настоящее время нет бесплатного, высококачественного и полного решения, которое позволяет общаться в браузере. WebRTC позволяет это. Уже интегрирована с лучшими в своем классе голосом и видеомоделями, которые были развернуты на миллионах конечных точек за последние 8+ лет. Google не взимает роялти за WebRTC. Включает и абстрагирует ключевые технологии обхода NAT и брандмауэра, используя STUN, ICE, TURN, RTP-over-TCP и поддержку прокси. Основывается на силе веб-браузера: сигнализация тезисов WebRTC, предлагая машину состояния сигнализации, которая напрямую отображается PeerConnection. Поэтому веб-разработчики могут выбирать протокол выбора для своего сценария использования (например, без ограничений, SIP, XMPP / Jingle и др.).

Какие другие компоненты включены в пакет WebRTC?

аудио

WebRTC предлагает полный стек для голосовой связи. Он включает в себя не только необходимые кодеки, но и другие компоненты, необходимые для отличного пользовательского опыта. Это включает в себя программную акустическую эхоподавление (AEC), автоматическое управление усилением (AGC), шумоподавление, подавление шума и аппаратный доступ и управление на нескольких платформах.

видео

Проект WebRTC основывается на кодеке VP8, представленном в 2010 году в рамках проекта WebM . Он включает в себя компоненты для скрытия потери пакетов и очистки шумных изображений, а также возможности захвата и воспроизведения на нескольких платформах.

сеть

Динамические буферы дрожания и методы скрытия ошибок включены для аудио и видео, которые помогают смягчить последствия потери пакетов и ненадежных сетей. Также включены компоненты для установления однорангового соединения с использованием ICE / STUN / Turn / RTP-over-TCP и поддержки прокси.

Литература:
1. ru.wikipedia.org/wiki/WebRTC
2. webrtc.org/faq/#what-is-webrtc

Волков Вадим Олегович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м. Київ

3D ІНТЕРНЕТ. КОРИСТЬ І ПЕРСПЕКТИВИ ЙОГО РОЗВИТКУ

Об'ємне бачення світу на зображенні. Про це люди мріяли ще до появи фотографії. Перший стереоскоп в 1838 році представив світу Чарльз Уїтсон. У його пристрій поміщалися дві намальовані тушшю картинки, що відрізняються для правого і лівого ока. Саме завдяки невеликій відмінності таких картинок, людський мозок був здатний «намалювати» об'ємне зображення, поєднуючи два плоских зображення в одне. Той же принцип формування тривимірної картинки використовується в сучасних технологіях 3D-бачення: нам здається, що замість двох плоских зображень очі бачать об'ємні предмети під різними кутами, як в реальному житті. Тривимірна графіка - розділ комп'ютерної графіки, сукупність прийомів і інструментів (як програмних, так і апаратних), призначених для зображення об'ємних об'єктів.

Інтернет переживає кризу середнього віку: коли йому виповнилося 40, він почав переходити в 3D вимір. Розвиток все ще перебуває на ранній стадії, але ідеологи данного явища вважають його природним і неминучим, вважаючи, що в найближчі роки очікується масове поширення 3D Інтернету. 3D зробить глобальну мережу більш соціальною і відкриє людям неймовірні можливості в освіті, бізнесі та медицині. Яні Піркола, першопроходець в цій сфері, передбачає, що пік використання 3D Інтернету буде в 2018 році, коли молодші користувачі очолять цей процес. І, за словами фахівця, він увійде в тренд набагато швидше, ніж 2D Інтернет. Що таке 3D Інтернет? Уявіть собі його як набір взаємозв'язаних віртуальних світів. Користувачі можуть відвідувати їх, споживаючи послуги, і «переміщуватися» з одного в інший. Віртуальні світи використовують багато технологічних компонентів 2D Інтернету - браузер, пошукові машини і сервери. Але особливістю, яка відрізняє данний вид Інтернету від традиційної всесвітньої павутини є 3D комп'ютерна графіка і, в багатьох випадках, аватари. Останні, як вважає Піркола, зроблять його набагато соціальнішим за свого попередника. «Читаючи будь-який документ, ви зможете побачити інших користувачів, які читають цей документ. Ви будете природно пов'язані з людьми, які мають спільні з вами інтереси і споживають ті ж самі послуги, »- прогнозує він.

Одне застереження: якщо ви очікуєте того, що пошук в 3D Інтернеті буде виглядати як нескінченна комп'ютерна гра з приголомшливою графікою, то будете розчаровані. Піркола звертає увагу на те, що віртуальні світи в високоякісних комп'ютерних іграх є результатом роботи багатьох художників і мають бюджети зрівняні з бюджетами

кінофільмів. У порівнянні з ними, 3D Інтернет може виглядати тьмяно. «3D службам буде потрібно частково пожертвувати зовнішнім виглядом і швидкістю,» - говорить Піркола.

Зараз існують міріади віртуальних світів по всьому світу з різними 3D платформами, як-то: Open Wonderland, MeshMoon, OpenSim і Sirikata. Однак, на сьогоднішній день каменем спотикання є відсутність загальноприйнятих стандартів для забезпечення їх сумісності.

2D графічний інтерфейс досяг межі своїх можливостей і настав час рухатися вперед і освоювати світ 3D.

Література:
1. https://nvworld.ru
2. https://knowledge.allbest.ru
3. http://venture-biz.ru

Марковський Сергій Андрійович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м. Київ

МЕРЕЖІ 5 ПОКОЛІННЯ

Багато українців все ще чекають приходу в їх міста та села мереж 3G, в той час як у світі активно обговорюється майбутня поява мереж п'ятого покоління.Мережі 3G були революцією, що дозволила здійснювати відеодзвінки і дивитися потокове відео на мобільних пристроях. Мережі 4G, які в Україні тільки почали розвиватися, принесли не тільки велику швидкість і пропускну здатність, але й можливість революціонізувати багато сфер бізнесу завдяки швидкісному мобільному підключенню до мережі.

Що розуміється під терміном мережі п'ятого покоління (5G)?

5G – це назва технології, яка слідуватиме за 4G-мережами, що вже існують. Незважаючи на активне тестування, його стандартизація очікується не раніше 2020 року. По суті, п'яте покоління – це не один стандарт, а цілий комплекс технологій, як вже наявних, так і абсолютно нових.

Наскільки це швидше, ніж 4G і ті ж 3G мережі, які є сьогодні в Україні?

Варто розрізняти максимально можливу швидкість з технічної точки зору, і реальну швидкість, яка буде доступна користувачам. Так, під час тестування досягали пікових показників 25,3 Гбіт/с.

Якщо говорити про швидкості комерційних мереж, очікується, що в 5G вони досягнуть 10 Гбіт/с. Простіше кажучи, ви зможете завантажувати Full HD-фільми за лічені секунди. Для порівняння, максимально можлива швидкість нинішніх 3G-мереж в Україні – 63 Мбіт/с, а реально доступна для абонентів – близько 5-10 Мбіт/с, що залежить від якості покриття мережі, а також навантаження на мережу, яку створюють мобільні абоненти.

Важливо відзначити, що вперше в історії розвитку телекомунікацій швидкість не буде визначальним фактором. Більш важливим стане надійність мереж, нульова затримка і здатність підлаштовуватися під конкретні завдання і потреби додатків.

За рахунок чого досягається можливість такого приросту в швидкості та пропускної здатності?

Досягти таких показників буде можливо завдяки комбінації багатьох факторів. По-перше, планується використовувати більш широкі смуги частот, а удосконалений 5G радіоінтерфейс дозволить пропускати в кілька разів більше даних.

По-друге, швидкість і пропускну здатність збільшить застосування технології Massive MIMO, яка передбачає використання кількох антен на прийомопередавачах. Ця технологія застосовується вже зараз в наявних мережах 4G, але в майбутньому кількість антен буде збільшено.

Важливою відмінністю мережі п'ятого покоління буде її можливість «підлаштовуватися» під абонента. На практиці це означає, що 5G буде «дробити» мережу на віртуальні сегменти (network slicing), кожен з яких буде виділено під певні потреби. Це дасть можливість її одночасного максимально ефективного використання для різних додатків – це буде єдина мережа для мільйонів різних потреб!

Основні технології

Досягнення поставлених показників роботи мереж п'ятого покоління потребуватиме використання нових технологій. Зокрема, очікується, що в мережах 5G буде використано такі технології:

Передавання даних радіохвилями у міліметровому діапазоні (буде обраний сегмент в діапазоні 30-300 ГГц).

Малі базові станції повинні розв'язати проблеми із швидким згасанням міліметрових хвиль. Очікується, що ці станції матимуть низьке енергоспоживання, малі габарити, будуть портативними а оператори стільникового зв'язку матимуть можливість встановлювати їх тисячами на відстані 250 м одна від одної.

Базові станції матимуть масиви MIMO. Технологія MIMO вже наявна в базових станціях 4G, але в них є лише 8 портів для передачі та 8 для отримання даних. В базових станціях 5G таких портів вже буде порядку кількох сотень.

Потреба у технології BeamForming продиктована проблемами з інтерференцією хвиль через збільшення портів вводу-виведення MIMO.

Передавання даних між абонентом та базовою станцією в режимі повного дуплексу.

Як зміниться світ?

П'яте покоління мереж виступить в ролі базису, на якому трансформується бізнес, суспільство і держава. Хоча воно тільки розробляється, вже зараз зрозуміло, що вплив і ефект вийде далеко за межі телекомунікацій. Мобільні мережі будуть важливою частиною економіки, адже вони зможуть забезпечити розвиток ключових галузей. Виникає небачений раніше ринок, обсяг якого, як припустила компанія Ericsson, перевищить у 2026 році півтрильйона доларів США на рік. Це все було б порожніми словами без якісних прикладів. Так, наявність практично нульовий затримки дозволить віддалено управляти важкою промисловістю, що знизить вартість виробництва і підніме безпеку співробітників на небачений раніше рівень. Можуть бути застосовані мережі п'ятого покоління і в хірургії. Адже завдяки ним можна буде забезпечувати безперебійну передачу всієї важливої інформації в потрібному розширенні, що дозволить лікарям оперувати людей з будь-якої точки земної кулі. На наших очах виникає нова транспортна система. Так, небезпідставно вважається, що під час початку впровадження 5G в 2020 році по дорогах буде їздити вже понад десять мільйонів розумних машин.

Література :

1.http://hi-news.pp.ua/tehnka-tehnologyi/6881-merezha-5g-oglyad-opis-ta-shvidkst-standarti-stlnikovogo-zvyazku.html

2.https://uk.wikipedia.org/wiki/5G

3.https://nv.ua/ukr/science/lectures/lektorij-shcho-take-5g-i-merezhi-novogo-pokolinnja-zminjat-svit-938166.html

4http://www.bbc.com/ukrainian/science/2014/12/141204_5g_technology_it

Димарчук Дмитрій Сергійович

Державний університет телекомунікацій

Факультет Телекомунікацій

м. Київ

ЗВ'ЯЗОК НА БОРТУ ЛІТАКА

У даний час стільниковий зв'язок отримав дуже широке поширення і проник практично в усі, навіть найвіддаленіші куточки. Користуватися мобільним телефоном ми

можемо в магазині, кінотеатрі, автомобілі, поїзді і навіть в метро. Практично єдиним місцем, де ми не можемо користуватися стільниковим зв'язком в повній мірі - це небо. Літаками користується найбільш активна і ділова частина населення: бізнесмени, банкіри, дипломати. Багато з них проводять на телефоні по кілька годин на день, здійснюючи дзвінки, обмінюючись короткими повідомленнями, перевіряючи електронну пошту і подорожуючи по Інтернет. Стільниковий зв'язок дає їм одне з найголовніших переваг - це мобільність. Однак опиняючись на борту літака, вони виявляються як без рук. Зв'язок із зовнішнім світом виявляється втраченої на кілька годин.

Стільниковий зв'язок з'явився в 1980 році і приблизно в цей же час на цивільних пасажирських літаках з'явилася можливість здійснювати голосові виклики. Зв'язок надавалася за допомогою спеціальних бортових бездротових телефонів. До сих пір багато авіакомпаній дозволяють здійснювати дзвінки під час польоту, а пасажири першого класу навіть можуть отримати персональний телефон на час польоту. Однак такий сервіс не дозволяє все того, що могла б запропонувати стільниковий зв'язок. Зокрема бортові телефонні системи не надають доступ в мережу Інтернет, який є невід'ємним атрибутом сучасного життя.

***Що ж заважає користуватися стільниковим зв'язком в стільниковому телефоні*?** На то існує цілий ряд законодавчих бар'єрів, проблем із забезпеченням безпеки, а також питання з економічною ефективністю. Не секрет, що і стільниковий зв'язок, і бортові системи літака використовують радіозв'язок. Тому виникає ймовірність появи інтерференції між ними, тобто взаємовпливу. Очевидно, що перешкоди в роботі радіо пристроїв літака, до яких відносяться радіозв'язок з диспетчерською службою, бортовий радар, телеметричні системи і ін. можуть привести до виникнення, як мінімум, позаштатної ситуації що може, в кінцевому рахунку, вплинути на безпеку польоту. Багато хто скептично ставиться до такої небезпеки, посилаючись на те, що всі системи літака надійно захищені від дії зовнішніх радіопристроїв, і, крім того, використовуються різні частотні діапазони. Однак факти говорять зворотне: наприклад, з 2000 по 2005 рік було зареєстровано 20 інцидентів на різних рейсах, причинами яких було названо використання стільникового зв'язку. Тому в законах багатьох держав і політиків безпеки авіакомпаній накладена заборона навіть на включення стільникових телефонів на борту. Ще однією важливою причиною заборони використання стільникового зв'язку під час польотів служить загроза терористичних актів. Часто саме за відправкою сигналу на мобільний телефон дистанційно активуються вибухові пристрої. Особливо після подій 11 вересня в США це стало ще однією суттєвою причиною заборони стільникового зв'язку в літаках.

Незважаючи на зазначені вище причини, стільниковий зв'язок все-таки взяла своє. У 2007 році авіакомпанія Emirates Airline надала можливість своїм пасажирам здійснювати голосові дзвінки і відправляти SMS під час польоту на крейсерській висоті. Відразу після неї ще кілька міжнародних компаній дозволили користуватися стільниковим зв'язком на борту. Таке рішення було засноване в першу чергу на те, що немає чітких доказів впливу стільникового зв'язку на бортові системи, тому що щоб остаточно підтвердити або спростувати цю гіпотезу необхідні довготривалі комплексні дослідження, які поки ще ніхто не проводив.

Розглянемо принципи функціонування стільникового зв'язку на борту літака. Для забезпечення радіо покриття в салоні літака зазвичай застосовуються так звані піко (фемто) базові станції (БС). На землі вони застосовуються для поліпшення покриття в торгових приміщеннях та офісах. У деяких реалізаціях піко БС являє собою антену і приймач, об'єднані в невеликому корпусі, який важить близько 1 кг і легко монтується на стіні в салоні. Для передачі сигналу від БС до іншої мережі застосовуються супутникові канали зв'язку - практично єдиний варіант в таких умовах. Саме з цим пов'язана одна з найголовніших проблем, тому що супутниковий зв'язок - це досить дорогий вид зв'язку. Проблема посилюється, що в літаку не весь час знаходяться абоненти, а канал зазвичай

орендується цілодобово і навіть під час польоту 60% взагалі відмовляються користуватися стільниковим зв'язком через її високу вартість. У деяких економічних розрахунках, навіть не дивлячись на високу (іноді 10 кратну) вартість послуг зв'язку, термін окупності складає більше 10 років. Для телекомунікаційного ринку такі проекти не вважаються привабливими.

Не дивлячись на зазначені вище недоліки використання стільникового зв'язку на борту літака багато авіакомпаній все-таки надають цей сервіс. Оператори стільникового зв'язку зацікавлені в такій рекламі своїх послуг, а власники авіакомпаній прагнуть надати максимально широкий набір послуг під час польотів. Однак через питання безпеки зазвичай користування стільниковим телефоном все-таки обмежена. Деякі авіакомпанії дозволяють користуватися тільки SMS і Інтернет, інші просять вимкнути свій телефон під час зльоту і посадки літака. У США стільниковим телефоном можна користуватися на борту літака, але тільки поки він знаходиться на землі. У 2010 році один з українських операторів уже анонсував запуск в тестову експлуатацію бортовий стільникового зв'язку на деяких авіарейсах.

Висновок: розглянуті вище аспекти застосування стільникового зв'язку на борту літака показують неоднозначність ставлення до цього в різних країнах і авіакомпанія. Важливим є те, що в сучасному світі залишатися ізольованим від зовнішнього світу, нехай навіть і на кілька годин, стає все важче. Тому можна з упевненістю стверджувати, що стільниковий зв'язок буде поступово проникати в сферу авіарейсів все більше і більше з кожним роком.

Література:

1. http://celnet.ru/airsot.php
2. https://www.billing.ru/blog/kak-rabotaet-svyaz-na-bortu-samoletov
3. http://tvoipolet.ru/princip-raboty-sotovoj-svyazi-v-samolete/

Кадун Богдан Ігорович
Державний Університет Телекомунікацій
Факультет Телекомунікації
м.Київ

РОЗУМНЕ МІСТО, РЕАЛІЗАЦІЯ ЗА ДОПОМОГОЮ 5G

Ми всі знаємо, що 5G значно покращить взаємодію з світовою павутиною мільйонів користувачів смартфонів. Можливо, ви також чули, що це допоможе нам покращити наші будинки через Internet of Things (IoT). Але 5G це не тільки вища швидкість передачі даних. Це дещо більше.

На базовому рівні 5G забезпечить значно більші швидкості передачі даних, набагато більшу ємність даних, краще охоплення, збільшить кількість підключених людей одночасно, та меншу затримку - або швидший час відгуку - ніж 4G. Це дозволить впровадити таку річ як розумне місто.

Що таке "розумне місто"?

Це трохи туманний термін, але, мабуть, корисно сказати, що концепція "розумного міста" є логічним завершенням "Інтернету речей".

Побудований на принципі «розумного дому», але застосовується до набагато більшого масштабу. Розумне місто - це різні види інфраструктури, що з'єднані між собою, і взаємодіють.

Як пояснює це ініціатива *Bristol Is Open*: "Використання сенсорів даних, розумні технології міста зможуть реагувати в реальному часі на щоденні події, включаючи затори, видалення відходів, розважальні заходи, енергопостачання та багато іншого".

Наприклад, в розумному місті, розумні автомобілі зможуть спілкуватися зі смартфонами пішоходів, зі світлофорами та іншими автомобілями для прогнозування умов руху і навіть (коли автоматичні автомобілі, буз водіїв стануть практичною реальністю) уникнути зіткнень. У розумному місті, автомобілі також зможуть спілкуватися з вуличним освітленням у районі, на якому вони проїжджають, таким чином, будуть горіти лише ті дороги, які активно використовуються, заощаджуючи владу та гроші міста, зберігаючи при цьому водіїв. З цією метою потрібна нова мережа мобільних мереж, яка може обробляти масово збільшене навантаження на дані, що вимагатиметься. Ми, звичайно, говоримо про 5G.

Що потрібно для впровадження в життя проекту «Розумне місто», і яка ситуація в Києві.

- *Міський Дата-центр*
  (Уже є в наявності. Тут буде акумулюватися і оброблятися вся інформація міських систем і сервісів. Розрахований на 22 юніта. Для прикладу, одна камера генерує близько 32 Гбайт на добу. Архів відео стрімко зростає.)
- *Камери*
  (У Києві вже є 4100 спеціальних камер HikVision і Huawei. Наступний етап - покрити всі в'їзди і виїзди з міста (61), входи / виходи в метрополітен, 120 світлофорних об'єктів (тобто перехресть). Також будуть оснащені камерами основні місця скупчення людей на рівні районів міста, основні транспортні розв'язки.)
- *Ситуаційний центр*
  (Був відкритий менше року тому. Штат - 25 осіб. Обладнаний екраном на всю стіну, на який виводиться зображення камер з високою роздільною здатністю.)
- *Опорна мережа*
  (У процесі створення. Передбачає об'єднання 54 структурних підрозділів КМДА в єдину високошвидкісну захищену мережу. Було прийнято рішення не орендувати комерційні мережі, а будувати міську мережу. План - покрити оптоволоконною мережею весь Правий берег, а до кінця року - і Лівий.)

На даний момент у всій цій схемі не вистачає саме мережі 5-го покоління, саме вона виконала б роль зв'язуючого елемента в цій структурі, адже тільки завдяки тим якостям які описані вище можливе впровадження саме «Розумного міста».

Коли буде впроваджений стандарт 5-го покоління?

Група з просування 5G в Китаї завершила внутрішні випробування технології, тепер переходить до відкритого тестування. У пекінському районі Хуайжоу планується наймасштабніші в світі польові випробування 5G, в яких візьмуть участь провідні світові виробники телекомунікаційного обладнання. Міністерство промисловості та інформатизації КНР 22 лютого оприлюднило інформацію про те, що другий етап китайських досліджень і розробок був офіційно запущений у вересні 2016 року, в тестуванні взяли участь такі підприємства як Huawei, ZTE, Datang, Nokia, Samsung та інші. Стало відомо, що в пекінському районі Хуайжоу плануються наймасштабніші в світі польові випробування 5G.

Глава телекомунікаційного відділу Міністерства промисловості і інформатизації КНР Вень Ку раніше говорив, що до кінця 2018 року буде сформований стандарт першої версії 5G. В даний час Китай прискорює наукові дослідження і розробку технології 5G.

Література:

1. http://www.idc.asia;
2. https://5g.co.uk/;
3. http://1234g.ru/5g;
4. http://wiki.kspu.kr.ua/;
5. https://habrahabr.ru/

Кадюк Ростислав Сергееви
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
г.Киев

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

За последнее время состояние телекоммуникационных сетей сильно изменилось в лучшую сторону. В данный момент сложно предсказать, как они будут выглядеть в будущем. Но даже сейчас можно наблюдать перспективные разработки: мощные сети передач и коммутации пакетов, высокоскоростные линии доступа, оптические телекоммуникационные технологии и т.д., которые и определяют следующие поколения телекоммуникационных сетей. Выделяются три этапа развития телефонных сетей общего пользования, которые принято считать основными. SDN стали развиваться в1980-х годах, после того как появились цифровые системы передачи. Но несмотря на создание интегральной сети, которая позволяла предоставляла различные виды услуг связи, основным приложением по - прежнему осталась услуга телефонии. Сети ISDN Фролов А.В., Фролов Г.В. Локальные сети персональных компьютеров. - М.: "Диалог-МИФИ"2002. С-108 использовали цифровые системы передачи и цифровые узлы коммутации. Для того чтобы организовать взаимодействия аппаратуры узлов коммутации между собой и с подключаемым терминальным оборудованием были установлены более мощные системы сигнализации. Они позволили передавать сигнальную информацию, связанную с установлением базового вызова, а также сведения, относящиеся к состоянию элементов сети связи, маршрутизации вызовов, согласованию параметров передачи и т.д. Так как до появления ISDN уже были созданы сетевые структуры в рамках POTS, то новое оборудование должно было взаимодействовать с существующими сетевыми фрагментами без снижения качества их работы и сокращения функциональных возможностей по предоставлению услуг доступа. Поэтому существующая сетевая структура для предоставления услуг телефонии до сих пор имеет в своем составе сетевые фрагменты как на основе решений POTS, так и на основе ISDN. Появление Интернета привело к увеличению разветвленности и повышению емкости сети. Возникла потребность в изобретении сетевой структуры, такой же масштабной как телефонная сеть общего пользования (ТфОП). Но использование двух сетевых структур было экономически не выгодно. Поэтому необходимо было разработать технологию, которая обеспечит передачу различных видов информации и предоставление различных видов услуг связи в единой сетевой структуре. Этот метод передачи информации основан на коммутации пакетов. Так появились сети третьего поколения - сети NGN (Next Generation Network). NGN - это гетерогенная мультисервисная сеть, основанная на пакетной коммутации, и обеспечивающая предоставление практически неограниченного спектра телекоммуникационных услуг. При этом NGN в качестве технических средств использует аппаратно - программные средства, ориентированные на стек протоколов TCP/ IP. Традиционные сети не могут поддерживать обмен трафиком в формате IP, поэтому необходима реконструкция всей архитектуры сети: транспортной инфраструктуры, уровня доступа и сетевой иерархии.

Литература:

1. Ануфриев, А. Стандарт DVB-S2 как средство развития новых сервисов на спутниковых сетях связи / А. Ануфриев // Broadcasting. Телевидение и радиовещание. - 2010. - № 3. - С.48-50.

2. Блэк Ю. Сети ЭВМ: Протоколы, стандарты, интерфейсы: Пер. с анг. - М.: Мир, 2010. - 224с.

3. Бойдо В.Л. Вычислительные системы, сети и телекоммуникации. СПБ.: Питер, 2011 - 120с.

4. Велихов А.В., Строчников К.С., Леонтьев Б.К. Компьютерные сети: Учебное пособие по администрированию локальных и объединенных сетей. - М: Познавательная книга-Пресс, 2011 - 320 с.

Кращенко Дмитро Денисович
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

МЕТОДИ І ТЕХНОЛОГІЇ ЗАХИСТУ ВІД ШКІДЛИВИХ ПРОГРАМ

Для захисту від шкідливих програм і комп'ютерного шахрайства існують і застосовуються різні методи боротьби з ними. Це методи юридичні, освітні та технічні.

У всіх комп'ютеризованих країнах прийняті закони, що забороняють створення і поширення вірусів і інших типів шкідливих програм. До того ж часто дії інтернет-злочинців потрапляють під абсолютно некомп'ютерні статті кримінальних кодексів - наприклад, шахрайство, вимагання, неправомірний доступ до конфіденційної інформації і т.д. Дані закони регулярно застосовуються на практиці. Однак слід визнати, що часто подібні злочини скоюються технічнj грамотними фахівцями, і це досить серйозно ускладнює розслідування злочину. Плюс до того більшість кримінальних атак залишаються поза увагою поліції. З цих причин виключно юридичними методами можна знизити загальний рівень комп'ютерної злочинності, але повністю перемогти не можна.

Другим важливим методом захисту від комп'ютерних зловмисників є навчання користувачів і суворе дотримання основних правил поведінки в мережі. Всього є три основних правила, які правильні як для домашніх, так і для корпоративних користувачів:

Обов'язкове використання антивірусного захисту.

Якщо ви не є експертом з комп'ютерної безпеки, то краще за все вас захистить надійний антивірусний захист і захист від мережевих атак (брандмауер) - довірте свою безпеку професіоналам. Більшість сучасних антивірусних програм захищають від найрізноманітніших комп'ютерних загроз - від вірусів, хробаків, троянських програм і рекламних систем. Інтегровані рішення з безпеки також ставлять фільтр проти спаму, мережевих атак, відвідування небажаних і небезпечних інтернет-ресурсів і т.д.

Не слід довіряти всій інформації, що надходить на комп'ютер - електронним листам, посиланням на веб-сайти тощо.

Ніколи не слід відкривати файли і посилання, що приходять з невідомого джерела. Навіть якщо повідомлення отримано з джерела відомого (від знайомого або колеги по роботі), але присланий файл або посилання приходить для вас несподівано, - краще перепитати про справжність повідомлення, оскільки зворотня адреса в електронній пошті легко підробляється. Інтернет - досить небезпечне місце, де слід поводитися обережно.

На жаль, жорсткі обмежувальні заходи можуть конфліктувати з побажаннями кожного конкретного користувача або з бізнес-процесами підприємства, - в таких випадках треба шукати баланс, причому в кожному окремо взятому випадку цей баланс може бути різним.

Слід звертати велику увагу на інформацію від антивірусних компаній і від експертів з комп'ютерної безпеки.

Зазвичай вони своєчасно повідомляють про нові види інтернет-шахрайства, нові віруси, епідемії і т.д. - приділяйте більше уваги подібній інформації.

Використання антиспамових фільтрів допомагає захиститися і від деяких поштових черв'яків. Найочевидніше застосування - це при отриманні першого зараженого листа (за відсутності антивіруса це можна визначити за непрямими ознаками) відзначити його як небажане і надалі всі інші заражені листи будуть заблоковані фільтром.

Поштові черв'яки відомі тим, що мають велику кількість модифікацій незначно відрізняються один від одного. Тому антиспамовий фільтр може допомогти і в боротьбі з новими модифікаціями відомих вірусів. У цьому сенсі антиспамовий фільтр навіть ефективніше антивіруса, так щоб антивірус виявив нову модифікацію необхідно дочекатися оновлення антивірусних баз.

У будь-якому випадку, антивіруси є найефективнішими засобами захисту від вірусів, і їх використання на робочих станціях обов'язково.

Література:
1.http://uareferat.com/%D0%A8%D0%BA%D1%96%D0%B4%D0%BB%D0%B8%D0%B2%D1%96_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B8_%D0%BA%D0%BB%D0%B0%D1%81%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F_%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83

Ніколаєнко Валерія Ігорівна
Державний університет телекомунікацій
Факультет Телекомунікацій
м.Київ

ІННОВАЦІЙНІ МЕТОДИ КРИПТОГРАФІЇ НА ПРИКЛАДІ МЕСЕНДЖЕРА TELEGRAM

У сучасному світі основна частина інтернет спілкування зосереджена на системах обміну миттєвими повідомленнями. І тут для будь-якого користувача з'являється основне питання: «Наскільки конфіденційне моє спілкування?». Очевидно, що всі криптографічні способи захисту повинні мати принаймні дві основні властивості: приватність та цілісність повідомлень. Приватність передбачає відсутність доступу третьої сторони до особистих даних та повідомлень, а цілісність, у свою чергу, захист від зловмисних атак заміни та випадкових спотворень. Звідси робимо висновок: основна задача розробників месенджерів – ефективна функція шифрування.

Досить цікавим та яскравим прикладом є мультиплатформенна служба миттєвих повідомлень – Telegram. Даний месенджер окрім звичного чату передбачає, так звані, «секретні» онлайн діалоги.

Для початку розглянемо хмарний, тобто звичайний чат. Його шифрування відбувається наступним чином: співрозмовник А відправляє повідомлення → воно шифрується спеціальними протоколами до вигляду незрозумілого поєднання символів → у такому вигляді зберігається в історії на пристрої користувача А → зашифрований текст переходить на сервер, де зберігається у тому ж вигляді → повідомлення приходить на пристрій отримувача Б і зберігається так само (в історії у зашифрованому вигляді) → за допомогою протоколів відбувається дешифрація даних → користувач Б отримує початкове повідомлення ідентичне відправленому. Даний приклад криптографії є потенційно більш доступним для третіх осіб, так як ключі шифрування зберігаються на серверах компанії, тому що навіть найбільш захищений сервер має певні можливості для доступу хакерів до приватної інформації користувачів.

Тепер перейдемо до секретного чату, тут вже маємо реалізовані додаткові механізми захисту. Схема передачі повідомлення подібна до попередньої але містить деякі зміни: повідомлення не йдуть на сервер, а оминаючи його, потрапляють безпосередньо на пристрій учасника діалогу; переписка автоматично самознищується на пристроях через певний час; при видаленні в одного зі співрозмовників секретні повідомлення видаляються і в іншого; ключ шифрування прив'язується до конкретного пристрою, при його зміні не вдасться відновити повідомлення секретних чатів. Саме ця особливість передачі даних практично зводить нанівець вірогідні можливості втручання у особисті голосові або текстові повідомлення.

Для реалізації секретного чату використовується End-to-End шифрування, для месенджера був створений спеціальний протокол MTProto, який передбачає використання кількох протоколів шифрування – сервер-сервер та клієнт-сервер. А як відомо, застосування комбінованих методів захисту ускладнює можливість доступу третіх осіб у геометричній прогресії. Його робота базується на основі наступних алгоритмів:

- AES – симетричний 256-бітний алгоритм блочного шифрування, що є принятим в якості стандарту шифрування урядом США
- RSA – криптографічний алгоритм, основою якого є обчислювальна складність задачі факторизації великих цілих чисел
- Протокол Діффі-Геллмана – метод обміну криптографічними ключами, який дозволяє отримати захищений від підмін, але незахищений від прослуховування секретний ключ кільком співрозмовникам
- SHA-1 та MD5 – хеш-функція, що використовується для безпечного хешування.

Маючи можливість використовувати сучасний месенджер, користувач має практично 100% гарантію, що його особиста інформація потрапить саме туди, куди має, а можливість перехоплення чи зміни голосових або текствових повідомлень практично відсутня.

Таким чином, можна зробити висновок, що технології шифрування не стоять на місці, заходячи все більше сфер застосування, і саме обмін повідомленнями дозволяє відчути їх переваги кожному, хто має доступ до мережі інтернет.

Література:

1.telegram.org/faq
2.Jakob Jakobsen. A practical cryptanalysis of the Telegram messaging protocol. Master Thesis, Aarhus University (Available on request)., 2015
3.core.telegram.org/mtproto
4.Jonathan Katz and Yehuda Lindell. Introduction to modern cryptography. CRC Press, 2014

Сердюк Інна Олегівна
Державний Університет Телекомунікацій
Факультет Телекомунікації
м.Київ

НЕЙРОМОРФНІ ЧІПИ: ІНШИЙ ПОГЛЯД НА МАШИННЕ НАВЧАННЯ

Вам відомо, що людський мозок — найдосконаліший процесор у Всесвіті з тих, що ми знаємо? Він здатний обробляти інформацію зі швидкістю світла, не витрачаючи при цьому багато енергії (і практично не займаючи місця).

Сучасні комп'ютери, якими користується більшість із нас, створені на підставі так званої архітектури фон Неймана. Цей метод добре підходить для рішення рівнянь та запуску різних алгоритмів, але не для обробки зображень або звуку. І хоча в 2012 році Google навчила штучний інтелект розпізнати кішки на відео, для цього компанія потребувала 16 тис. процесорів.

Тому людство працює над введенням нових архітектур, які дозволять машинам більш ефективно взаємодіяти з оточенням. Одним з таких рішень стали нейромформові чіпи, про які ми хочемо розповісти в сьогоднішній матеріалі.

Нейроморфні чіпи моделюють те, як наш мозок обробляє інформацію - як мільярди нейронів і трилійони синапсів реагують на сигнали від органів відчуття. Зв’язки між нейронами також постійно змінюються, реагуючи на зображення, звуки та ін. Цей процес ми з вами називаємо навчанням. Ідея полягає в тому, щоб змусити чіпи робити те ж саме. Навіть якщо нейроморфні чіпи будуть вступати в "продуктивність" реального мозку, вони все одно обгонять сучасні комп'ютери у питаннях навчання та обробки сенсорної інформації.

Нейроморфні чіпи.

Сама ідея нейроморфних чіпів досить стара. Професор Каліфорнійського університету Карвер Мід (Carver Mead) ввів цей термін в 1990 році, відзначаючи, що аналогові чіпи, в відмінності від бінарних, зможуть імітувати мозкову активність, але

реалізувати ідею в життя і створити такий чип йому не вдалося. Однак сьогодні кілька компаній активно займаються витісненням цієї архітектури в кремінії.

В 2008 році за замовленням організації DARPA компанія IBM Research розпочала роботу над нейроморфним чипом. І через 6 років, у 2014 році, учені представили публіку систему TrueNorth, що складається з 1 мільйона цифрових нейронів і 256 мільйонів синапсів, влаштованих в 4096 синапсних ядер. TrueNorth - це модульна система, яка складається з декількох чипів, що представляють собою нейрони мозку. З'єднуючи такі чипи між собою, учені формують штучну нейронну мережу. За словами представників компанії, TrueNorth споживає менше електроенергії, ніж його "класичні" збирачі.

Нейрочіпи.

Нейрочіп з 5,4 млрд транзисторів споживає 70 мВт енергії, в той час як процесор Intel, в якому транзистори майже в 4 рази менше, вимагає близько 140 Вт. У планах учених ще сильніше знизити енергоспоживання та розміри наступних версій TrueNorth, щоб вони могли знайти застосування в мобільних пристроях або часах.

«Взаємодія процесора та пам'яті в традиційній архітектурі відбувається послідовно, - говорить провідний дослідник проекту SyNAPSE Дхармендра С. Модха. - Наша архітектура - це комплект кубиків LEGO. Кожна колія має різні функції, і ви просто комбінуєте їх ». Наприклад, така система може бути використана для пошуку людей у групі. Один корлет може шукати певну форму носа, інша - колір одягу та так далі.

Не так давно Qualcomm провели в своєму штаб-квартирі в Сан-Дієво презентацію можливостей нового нейромереологічного чипу. Не великий робот розміром з мозком під назвою Піонер під'їхав до дитячої іграшки, а потім почав штовхати її в бік трьох невисоких колон.

Ведучий інженер Qualcomm Іль У Чанг (Ilwoo Chang) вказав обома руками, куди слід розмістити фігурку, і Pioneer, розпізнавши жест із допомогою вбудованої камери, виконавши завдання. Після чого він відправився за іншою іграшкою і приніс їй ту ж саму колону без всяких підказок.

Робот виявився здатним виконувати завдання, для яких, як правило, потрібні потужні спеціалізовані комп'ютери. Піонер вже вміє розпізнавати нові об'єкти та розташувати їх за подією з іншими предметами, реагуючи на команди-жести.

В компанії Qualcomm відзначають, що нейроморфний чіп, який управляє роботом, є цифровим, а не аналоговим, проте попередньо емулює різні аспекти поведінки людського мозку. Засновники заявили, що їх процесор, розміщений у мобільних пристроях, комп'ютерах і роботах, дозволить машинам самостійно навчатися.

Проект отримав назву Zeroth і, за словами представників компанії, перші подібні чіпи повинні з'явитися в продажі в 2014 році, але це не відбулося. Однак у 2015 році компанія все-таки представила аналогічну розрахункову платформу.

Вплив нейроморфних чіпів на сучасні пристрої.

Як було відзначено вище, подібні чіпи дозволять нашим пристроям самовдосконалюватися. Наприклад, медичні гаджети навчаються розпізнавати життєво важливі показники, щоб превентивно впливати на стан пацієнтів. Смартфони ж навчаються передбачати бажання власників. Однак поки ще залишаються певні перепони, які попередньо перейшли. Все ще не вирішена проблема компонування нейронів - складно зіставляти розміри "мозку" з його можливостями. Труднощі виникають на всіх етапах - збірка, доставка потужності, тепловідвід, управління топологією. Ще один блок трудностей зв'язує з абстрактною натурою нейроверсій. Наскільки близьку копію нашого мозку треба створити, щоб вирішити бажані завдання? І як такі чипи будуть взаємодіяти з класичною обчислювальною технікою?

Практично всі проекти зараз проходять тестування, і до їх використання в смартфонах і часах ще далеко. І як вчені справляються з труднощами, покаже тільки час.

Література:
1.https://www.dailytechinfo.org/ ;
2.https://geektimes.ru;
3.https://hi-tech.ru;
4.https://www.overclockers.ua/;
5.https://habrahabr.ru/

Захарченко Андрей Владимирович
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
г. Киев

СПУТНИКОВЫЙ ИНТЕРНЕТ

Спутниковый Интернет — способ обеспечения доступа к сети Интернет с использованием технологий спутниковой связи. Существует в двух вариациях:

- Односторонний (one-way), так называемый «ассиметричный» — когда для приёма данных используется спутниковый канал, а для передачи — доступные наземные каналы.
- Двухсторонний (two-way), так называемый «симметричный» — когда и для приёма, и для передачи используются спутниковые каналы.

Односторонний спутниковый Интернет

Подразумевает наличие у пользователя какого-нибудь существующего способа подключения к Интернету. Как правило это медленный и/или дорогой канал (GPRS/EDGE, ADSL-подключение там, где услуги доступа в Интернет развиты плохо и ограничены по скорости и т. п.). Через этот канал передаются только запросы в Интернет. Эти запросы поступают на узел оператора (провайдера) одностороннего спутникового доступа (используются различные технологии VPN-подключения или проксирования трафика), а данные, полученные в ответ на эти запросы, передают пользователю через широкополосный спутниковый канал. Поскольку большинство пользователей в основном получает данные из Интернета, то такая технология позволяет получить более скоростной и более дешёвый трафик, чем медленные и дорогие наземные подключения. Объём же исходящего трафика по наземному каналу (а значит и затраты на него) становится достаточно скромным (соотношение исходящий/входящий — примерно от 1/10 при веб-сёрфинге, от 1/100 и лучше при загрузке файлов). Естественно, использовать односторонний спутниковый Интернет имеет смысл тогда, когда доступные наземные каналы слишком дорогие и/или медленные. При наличии недорогого и быстрого «наземного» Интернета — спутниковый Интернет имеет смысл как резервный вариант подключения, на случай пропадания или плохой работы «наземного». Задержки при использовании одностороннего доступа определяются как временем передачи сигнала через спутник (от оператора до абонента — порядка 250 мс), так и задержками в "наземном" (запросном) канале, и при большой загрузке сети могут варьироваться в очень широких пределах — вплоть до секунд.

Двухсторонний спутниковый Интернет

Подразумевает приём данных со спутника и отправку их обратно также через спутник. Этот способ является очень качественным, так как позволяет достигать больших скоростей при передаче и отправке, но он является достаточно дорогим и требует получения разрешения на радиопередающее оборудование (впрочем, последнее провайдер часто берёт на себя). Высокая стоимость двустороннего интернета оказывается полностью оправданной за счёт в первую очередь намного более надёжной связи. В отличие от одностороннего доступа, двусторонний спутниковый интернет не нуждается ни в каких дополнительных ресурсах, кроме электропитания.Особенностью «двустороннего» спутникового доступа в Интернет является достаточно большая задержка на канале связи.

Пока сигнал дойдёт от абонента до спутника и от спутника до Центральной станции спутниковой связи — пройдёт около 250 мс. Столько же нужно на путешествие обратно. Плюс неизбежные задержки сигнала на обработке и на то, чтобы пройти «по Интернету». В результате время пинга на двустороннем спутниковом канале составляет около 600 мс и более. Это накладывает некоторую специфику на работу приложений через спутниковый Интернет. Особенно это относится к сетевым играм в реальном времени и ip телефонии. Ещё одна особенность состоит в том, что оборудование различных производителей практически несовместимо друг с другом. То есть, если вы выбрали одного оператора, работающего на определённом типе оборудования, то перейти вы сможете только к оператору, использующему такое же оборудование. Попытка реализовать совместимость оборудования различных производителей (стандарт DVB-RCS) была поддержана очень небольшим количеством компаний, и на сегодня является скорее ещё одной из «частных» технологий, чем общепринятым стандартом.

Литература:
1.http://www.broadband.org.ua/tekhnologii-bystrogo-interneta/1493-sputnikovyj-internet-kak-eto-rabotaet

Стельмах Тарас Николаевич
Государственный университет телекоммуникаций
Факультет телекоммуникаций
г.Киев

SECURITY OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Widespread use of computer technology in automated information and management systems has led to an aggravation of the problem of protection of information circulating in computer systems from unauthorized access. The protection of information in computer systems has a number of specific features related to the fact that the information is not rigidly associated with the carrier, can be easily and quickly copied and transmitted through communication channels. We know a very large number of threats of information that can be realized both by external perpetrators and by internal perpetrators.

One of the security challenges of telecommunication technology is the security of processing and data transmission. Particularly "defenseless" were the data transmitted in global telecommunication networks. At present, a large number of specialists in practically all economically developed countries of the world are working on the problem of the security of information transmitted by the networks of information. We can say that information security was formed in a separate rapidly developing discipline. However, despite the efforts of many organizations involved in information protection, information security remains an extremely acute problem.

At present, security of information requires not only the development of new mechanisms of protection, but the implementation of an integrated approach that includes a set of necessary measures (use of special software and hardware, organizational measures, regulations, etc.). The complex nature of the protection generates complex actions by intruders who try to obtain the information they need byanymeans.

Classification of possible attacks, representing a set of possible variants of the offender's actions by certain methods of implementation with the use of vulnerabilities that make the attack possible. The purpose of the attack may not coincide with the purpose of realizing the threats and may be aimed at obtaining an intermediate result, necessary to achieve the further realization of the threat.

Sources of information security threats are divided into external and internal.

External sources include:

- Foreign policy of foreign countries in the field of information monitoring, dissemination of information and new information technologies;

- Activities of foreign intelligence and special structures.
- Criminal actions of international groups, groups and individuals.

Internal sources are:

- Anti-legal activities of political, economic and criminal structures.
- Violation of the established rules for the collection, processing and transmission of information;
- Deliberate actions and unintentional errors of personnel of automated systems.
- Failure of hardware and software failures in information and telecommunication systems;

Traditional methods for protecting information from unauthorized access are identification and authentication, password protection. Key concepts in security are identification and authentication. Identification is the assignment of any object or subject of a unique name or image. Authentication is the authentication, that is, verification that the object (subject) is really the one for whom it is issued. The ultimate goal of the identification and authentication procedures of an entity (entity) is to allow it to be used for limited use in the case of a positive check or refusal of admission in the event of a negative result of the verification.

The following areas of theoretical and applied research are of greatest interest today: creation and analysis of the reliability of cryptographic algorithms and protocols; adaptation of algorithms to various hardware and software platforms; use of existing cryptography technologies in new application systems; the possibility of using cryptography technologies to protect intellectual property.

Sources:

http://ua-referat.com/Методи_захисту_інформації_в_телекомунікаційних_мережах
http://lib.detut.edu.ua/files/Nauk_trud_vukladahiv/Fakultet%20Infrastruktur_ruxomuy_sklad%20"/Kafedra_tel_tex n_avtomatuka/nauk_trud_voznenko.pdf
https://www.epravda.com.ua/columns/2017/05/25/625302/

Паламарчук Владислав
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

НАЙПРОСТІШИЙ СПОСІБ СТВОРЕННЯ САЙТІВ

В останні роки ми спостерігаємо стрімкий ріст популярності сервісів для самостійного створення веб-сайтів. Ці сервіси називаються конструкторами сайтів або платформами для створення сайтів.

Конструктор сайтів – це зручний інструмент для простого створення та редагування вашого власного сайту. Використовуючи його, ви отримаєте можливість швидко створити ресурс на базі готового шаблону.

Для того щоб користуватися конструкторів сайтів не треба мати якихось спеціальних знань. Також у вас не буде необхідності встановлювати додаткове програмне забезпечення або обладнання. Основний принцип роботи сайтбілдера – практично моментальне створення сайту, який пізніше можна буде редагувати. Це зручно, просто та ефективно.

Одним з перших конструкторів сайтів був проект Geocities, заснований у 1994 році. Після свого 5- річного існування був проданий компанії Yahoo! За $3.6 млн. На той час це

була досить велика сума. Але після того як проект технічно застарів, він був закритий у 2009 році. З того часу ринок конструкторів веб-сайтів представлений більш,ніж 70 платформами. Ось деякі з них:

Сервіс BmShop за розумну плату надає своїм клієнтам можливість швидко створювати сайти інтернет-магазинів. Якщо вам потрібний потужний інтернет-магазин, ви не знайдете щось краще ніж BmShop.

Wix - широко відомий у всьому світі конструктор сайтів. Функціонал орієнтований, в першу чергу, на потреби початківців з нульовими знаннями сайтобудування.

uKit – конструктор з чітко позначеною сферою використання: створення сайтів для малого та середнього бізнесу.

Jimdo – довгоживучий міжнародний проект. Основною особливістю цього конструктора від інших є велика степінь захисту данних та безпеки сайту.

BigCommerce – один із найпотужніших платформ для онлайн продаж. Головним плюсом цього конструктора є можливість інтеграції з магазинами в Facebook, Google Shopping та торговими майданчиками Amazon, Ebay та інші.

Створення сайту за допомогою конструкторів має цілий ряд переваг в порівнянні із традиційним замовленням у веб-студії:

1) Швидкість розробки. Ви можете за одну годину створити ваш сайт.
2) Низька вартість. Вартість використання таких сервісів відносно не велика і на порядки нижча вартості послуг веб-студії.
3) Широкі функціональні можливості. Хороші конструктори дозволяють створювати сайти всіх типів.
4) Професійний супровід. Ви можете бути впевнені, що ваш сайт буде робити 24 години на добу і 7 днів на тиждень. За це відповідає ваш конструктор.
5) Людський фактор. Ви контролюєте усе, що відбувається з вашим сайтом.

Але також у конструкторів є свої недоліки:

1) Не завжди функціоналу вистачає для вирішення бізнес-завдань
2) Дизайн, як правило, вибирається з готових шаблонів.
3) Якщо бізнес виросте, то перенести сайт на свій хостинг або добавити нові функції буде не просто.

Таким чином, створення сайтів за допомогою конструктора не є раціональним рішенням для використання в комерційних цілях, і тому створення бізнес-сайтів ефективніше здійснювати індивідуально або в професійній студії веб-дизайну.

Але, якщо ви хочете створити свій блог або сайт візитку це буде ідеальним варіантом для вас.

Також створення сайтів за допомогою конструктора буде корисним для тих хто тільки починає освоювати сайтобудування.

Література:

1. *bit.ly/2AMcQwc*
2. *bit.ly/2Aoaao0*

Рівнячок Дар'я Леонідівна
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

СВІТ КРОКУЄ ДО 5G

На сьогоднішній день багато уваги приділяється питанню реалізації нового протоколу 5G для мобільних мереж зв'язку. На Всесвітньому мобільному конгресі президент Ericsson Борье Екхольм заявив що технології стандарту 5G готові до використання. Які можливості надаватиме 5G? Які переваги має цей стандарт?

Строго кажучи терміну "5G" не існує - це просто маркетингове найменування стандартів мобільного зв'язку більш сучасних поколінь, ніж ті, які використовуються зараз. Більшість людей вважають що: 2G – це повільно, 3G – швидко, 4G – дуже швидко. За фактом, 5G матиме ту саму швидкість, що й 4G.

Важливою відмінністю 5G являтиметься дуже маленька затримка (тобто час, який витрачається на передачу інформації; рахунок тут йде на мілісекунди) і можливість передавати дані між пристроями безпосередньо.

Його ключовою особливістю буде побудова самої мережі: можна буде виділяти захищені канали зв'язку, які матимуть виділену швидкість для надання критично важливих послуг.

Інформація в нових мережах буде передаватися в 100 разів швидше, ніж в 4G - в теорії швидкості можуть досягати десятків Гб/с.

Наприклад, 8-гігабайтний фільм в HD-якості через мережу 5G скачуватиметься за 6 секунд, а не за кілька хвилин, як це відбувається через 4G.

Звичайно мережа мережа п'ятого покоління надаватиме ширші можливості, ніж швидке скачування фільмів або перегляд відео в прямому ефірі. 5G дозволить безпілотним автомобілям майже миттєво отримувати інформацію про аварії на дорозі - як тільки щось станеться, сенсори на дорогах передадуть інформацію найближчим машинам, і ті зможуть загальмувати або змінити маршрут. Багато компаній активно працюють над розробкою 5G, адже це одна з ключових технологій, яка лежить в основі безпілотних автомобілів. Суть у тому, що потрібно зробити оптимальний маршрут без затримки зв'язку для автомобіля, щоб він зміг їздити автономно. Це дуже трендова тема, і поки що не існує єдиного стандарту.

Отже, можна з упевненістю сказати, що це не тільки швидкий інтернет, це та технологічна платформа, яка буде глибоко впливати на наше життя і наш бізнес. Ера "Гіга-швидкостей" почнеться з 5G.

Література:

1.https://nv.ua/ukr/techno/it-industry/
2.https://techtoday.in.ua/news/5g-dali-start-z-yavivsya-ofitsiyniy-standart-86545.html
3.http://nv.ua/ukr/science/lectures/lektorij-shcho-take-internet-rechej-i-navishcho-vin-potriben-1326653.html.

Стадник Денис Олександрович
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ В ТЕЛЕКОМУНІКАЦІЯХ ТА ПОВСЯКДЕННОМУ ЖИТТІ

На сьогоднішній день людство володіє надзвичайно величезними інформаційними ресурсами. Інформація виступає найважливішою складовою інформаційного суспільства і її роль сьогодні важко переоцінити.Вдосконалення засобів обчислювальної техніки, систем телекомунікацій та інформаційних технологій не лише повною мірою виявляє свою виробничу, технологічну й соціальну корисність, а й поліпшує умови нашої праці і побуту.Технологія Bluetooth – як сучасний спосіб контролю над периферійною технікою та аксесуарами. Near field communication, NFC- як основа сучасного банкінгу. Приклад застосування технології в смартфонах та смарт-годинниках. Надання послуг засобами єдиної мультисервісної мережі, яка отримала назву NGN (Next Generation Network). Це мережа наступного покоління. Без швидкісного мобільного інтернету доступного зараз – неможливо. 5G- стандарт зв’язку наступного покоління, що буде підтримувати інтернет-речей (розумні автомобілі, будинки) та іншу техніку. Стандарт 5G вимагає більш досконалого обладнання, антен, а також розширеного спектру частот. Комплекс технічних

і програмних засобів сучасних телекомунікаційних і мережних технологій забезпечує роботу фахівця у єдиному інформаційному просторі. Сьогодні світ перейшов на новий етап життя де головну роль диктують новітні технології, а мобільні додатки реалізуються у формі одержання найважливішої інформації прямо з екрану смартфону. Поява нових послуг, а також зростаючі вимоги користувачів змушує власників телекомунікаційних мереж модернізувати своє обладнання. Основною ціллю міжнародного союзу електрозв'язку є забезпечення і розширення міжнародного товариства на регіональному рівні використовуючи всі види зв'язку, покращення технічних засобів та ефективної експлуатації. Сучасні технології в сфері технологічного процесу сприяють поліпшеним характеристикам (розміри, енергоефективність, робочі частоти та вартість). Основною ціллю найменшого технічного процесу є більш швидка обробка інформації за рахунок зменшення енерговитрат. Інтернет-речей - це глобальна мережа підключених до інтернету фізичних пристроїв оснащених сенсорами, датчиками передачі інформації. В найблищому майбутньому концепція об'єднання телефонів, пральних машин, чайників, навушників, світильників і всього іншого – нікого не здивує. В світі вже підключених до інтернету пристроїв більше ніж людей на землі. Розвиток ринку буде залежати від безлічі факторів, але абсолютно точно, всім учасникам цього процесу доведеться змінюватися набагато швидше, ніж це відбувається сьогодні. Розвиток інформаційних технологій - шлях до майбутнього. IT і зв'язок стануть основою глобального суспільства, що повинно підняти його на новий ступінь розвитку.

Література:
1.journals.dut.edu.ua/index.php/communication/article/.../
2.http://poradu.pp.ua/internet/32672-merezha-5g-oglyad-opis-ta-shvidkst-merezha-novogo-pokolnnya-5g.html
3.http://axon.partners/uk/blog/what-is-a-blockchain-and-how-cryptocurrency-will-help-to-defeat-corruption-in-ukraine/
4. http://startuplife.by/fintech-startups.html

Ніколаєнко Валерія Ігорівна
Державний університет телекомунікацій
Факультет Телекомунікацій
м.Київ

ПЕРСПЕКТИВИ СВІТЛОГО МАЙБУТНЬОГО З Li-Fi

Li-Fi (Light Fidelity) – високошвидкісна технологія безпровідних оптичних мереж, що використовує світлодіоди для передачі даних. Вона відноситься до класу комунікацій видимого спектру світла (Visible Light Communication), що дозволяє не лише випромінювати світло, а й передавати інформацію. Світлодіодні лампи, що використовуються в освітлювальних приладах, випускають тисячі імпульсів щосекунди. Змінюючи довжину таких імпульсів у них можна кодувати цифрову інформацію.

Засновником інноваційної технології вважається Харальд Хаас, завідувач кафедри мобільного зв'язку Університету Єдинбурга. Вперше технологія Li-Fi була продемонстрована на конференції TED Global, у Єдинбурзі, чим викликала неабиякий ажіотаж та захоплення публіки.

У першу чергу, варто зазначити головні переваги технології Li-Fi, як системи.

Однією з основних переваг по праву вважається ефективність її використання: усюди лампи слугують для освітлення приміщень чи вулиць, але ніхто б не відмовився, щоб за допомогою цього ж світла можна було передавати інформацію, тим самим економити

енергію. Так, адже саме енергоефективність набуває чи не пріоритетного значення у розробці новітніх технологій.

Наступна перевага полягає у доступності. LED-лампи ми можемо зустріти майже скрізь: у офісах, квартирах, машинах чи навіть літаках. Якщо кожну з цих ламп перетворити на засіб для передачі даних, то ми зможемо отримати інтернет без кордонів. До того ж, враховуючи рівень розвитку виробництва світлодіодних ламп та їх собівартість, дана технологія має усі перспективи стати значно дешевшою у повсякденному використанні.

За рахунок меншої відстані, світлом можна передавати дані на значно більшій швидкості, ніж за допомогою радіохвиль. Передача сигналу збільшиться у десять разів у порівнянні зі швидкістю передачі Wi-Fi.

Використання Li-Fi значною мірою вирішить питання перевантаженості мережі: навіть при використанні в перенаселених містах, подібні точки доступу не будуть забитими і не почнуть «конфліктувати» одне з одним, оскільки вони використовують більш широкий діапазон частот, який не є надто перенавантаженим іншими сигналами та мають більш високу пропускну здатність; до того ж, датчики прийому та передачі інформації можуть бути встановленими будь-де. Важливою особливістю технології Li-Fi є відсутність недоліків, яких неможливо позбутись використовуючи стандартні радіочастотні діапазони, що спричиняють значні незручності у використанні, такі як перешкоди для чутливого електронного обладнання (використовується в медичних установах і в навігаційних системах літаків) та забивання частотних діапазонів, про що згадувалось вище.

Безпечність даної мережі обумовлена тим, що технологія працює лиш у короткому діапазоні, отже треба знаходитися близько до джерела сигналу, тому інформація, з якою працює користувач, буде доступна лиш у межах дії світлового потоку. Для того, щоб перехопити інформацію, що передається через Li-Fi, хакеру доведеться стояти напрочуд близько до джерела світла, що зменшує вірогідність зберегти власну анонімність. Також, це робить дану технологію напрочуд раціональною з точки зору інформаційної безпеки, тому її буде доцільно використовувати в державних установах, стратегічно важливих об’єктах, масштабних фірмах, офісах та інших закладах, що потребують максимального інформаційного захисту. До того ж, технологія може використовуватися у місцях, де заборонено використання техніки, що випромінює сторонні радіохвилі, які можуть порушити роботу критичного обладнання.

В даний час ядром VLC-систем є джерела світла на базі світлодіодів, в яких використовуються сполуки фосфору, які перетворюють частину випромінюваного синього світла в червоне і зелене світло. Коли синє, зелене і червоне світло змішуються, то виходить біле світло, яке використовується і для освітлення, і для передачі даних. Але такий підхід має певні обмеження. VLC-системи, що використовують "синтетичне" біле світло, мають обмеження пропускної здатності на рівні 100 мільйонів біт в секунду. Подальше підвищення швидкості комунікацій можливо лише за рахунок збільшень кількості паралельних каналів, що наочно продемонстрували вчені з університету Вірджинії, які домоглися швидкості 300 Mbps, компанії Siemens, які отримали швидкість 500 Mbps, і Пенсільванського університету, які отримали швидкість 1.6 Gbps за допомогою невидимого інфрачервоного світла.

А от одним із найсуттєвіших недоліків виступає взаємодія даного виду оптичної мережі із денним сонячним світлом: Li-Fi погано працює на відкритому просторі, до того ж, якщо кожна лампа буде виступати в ролі роутера, то засвіченість буде надто сильною. Але так як технологія поки знаходиться у стані розробки, то не можна заперечувати, що дані недоліки неодноразово будуть модифікуватися, а система буде вдосконалюватися новими можливостями.

Незважаючи на сучасну обмеженість світлової передачі даних, якщо звернути увагу на швидкість розвитку та нові перспективи і методи застосування, що відкриваються для

даної технології, а також її енергоефективність та зацікавленість публіки, стає зрозумілим те, що за цим майбутнє. Відкритим залишається лише питання часу.

Варто також розуміти, що технологія Li-Fi, не буде заміною звичних засобів передачі даних, принаймні на початковому етапі свого впровадження. Тим більше, Wi-Fi буде дуже складно та дорого враз замінити на єдиний бездротовий стандарт.

Скоріше за все, слід очікувати гібридну систему, у якій співпрацюватимуть Wi-Fi та Li-Fi, в якій у свою чергу нова мережа буде базуватися на комбінації технологій Li-Fi та міліметрових хвиль (5G). Мінімальна затримка також дозволить використовувати її для дистанційного керування машинами та роботами через інтернет. Це може стати дешевим та енергоефективним методом передачі даних.

Отже, нам слід очікувати симбіоз систем та виходу на світовий ринок нових девайсів, що будуть здатні підтримувати комунікацію за допомогою світла.

Література:

1. *Пролетарский А. В. Беспроводные сети Wi-Fi / Пролетарский А. В., Баскаков И. В., Чирков Д. Н. — М.: Интернет-Университет Информационных технологий; БИНОМ; Лаборатория знаний, 2007–216 с.*
2. *Алексеев Д. А., Ермолаева В. В. Li-Fi — прорыв в науке или бесполезная игрушка? Преимущества и недостатки Li-Fi перед Wi-Fi // Молодой ученый. — 2015. — №11. — С. 161-164. — URL https://moluch.ru/archive/91/19744/*
3. *Serafimovski Dr. Nikola. Facts of Li-Fi // Lighting Journal. 2014. № 16*

Мантула Роман Анатолійович
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

РОЗВИТОК СФЕРИ ТЕЛЕКОМУНІКАЦІЙ ТА МЕРЕЖІ НОВОГО ПОКОЛІННЯ

Ринок телекомунікацій є одним з найбільш перспективних та найбільш динамічних напрямків галузі зв’язку як у цілому світі, так і в України. На даний час система телекомунікацій в Україні знаходиться на шляху прискореного розвитку і орієнтована на інтеграцію української системи зв'язку в світову. Однією з галузей зв'язку, яка займає перше місце на даний час, є мобільний зв'язок. Мобільний зв'язок сьогодні є однією з найбільш могутніх рушійних сил в індустрії телекомунікацій. Прибутки від мобільного зв'язку вже зараз значно перевищують прибутки від зв'язку в стаціонарних телефонних мережах, а в майбутньому прогнозується зростання цієї різниці. Тому тема дослідження українського ринку мобільного зв’язку є актуальною.

Однією з основних тенденцій розвитку операторів мобільного зв’язку, яка збережеться найближчими роками, можна вважати вихід операторів на ринок широкосмугового та мобільного Інтернету. Причиною такої стратегії, перш за все, є насичення ринку мобільного зв’язку та перспективи значного зростання ринку Інтернет-послуг в Україні. Можна відзначити, що активний розвиток онлайн-додатків і онлайн-торгівлі – це основні фактори, які забезпечують зростання ринку широкосмугового доступу до Інтернету (далі – ШСД). Розумний інтернет речей – постійна підтримка людини предметами, які його оточують.

У населення найбільшим попитом користуються послуги широкосмугового доступу до мережі Інтернет, доходи від надання яких мережами мобільного зв’язку зросли в 2011 році більше ніж удвічі, а виділеними каналами зв’язку – майже в 1,5 раза. Найпомітніше доходи збільшилися порівняно із січнем – жовтнем 2010 р. на ринку послуг мобільного зв’язку – на 1,6 млрд грн, а також від передачі даних та забезпечення доступу до мережі Інтернет – майже на 0,5 млрд грн. Якщо розглядати ринок ШСД України порівняно зі світовими ринками, то рівень проникнення ШСД в Україну становить, за різними оцінками,

від 15 до 19%, тоді як у Східній Європі він коливається від 34 до 54%, а в країнах Західної Європи – 61–69%. Показники Східної Європи можна вважати підставою для припущення, що Україна має непоганий потенціал до зростання ринку ШСД.

Як мережі 5 покоління змінять світ?

Весь світ нині змагається у розробці 5G, п'ятого покоління мобільної мережі. Хоча 5G наслідуватиме 4G і 3G, науковці покладають на цю мережу значно більше сподівань. Вони очікують, що вона буде інакшою – принципово інакшою.Якщо ви думаєте: "Прекрасно! Мої програми більше не гальмуватимуть, відео не зависатиме, і я зможу забути про вічні паузи в очікуванні завантаження сторінок", – ви праві. Але це ще не все."5G – принципово нова технологія, що гармонізує радіоспектр", – каже професор Рахім Тафазоллі, голова Центру 5G-інновацій, який був заснований при Університеті Саррею й отримує багатомільйонне фінансування від британського уряду.5G обіцяє уможливити "розумні міста" з постійним зв'язком між усіма сферами міського життя, дистанційні хірургічні операції, безпілотні автомобілі і "інтернет речей".

Література:

1.http://ena.lp.edu.ua/bitstream/ntb/16806/1/164-Mamchyn-267-269.pdf
2.http://www.bbc.com/ukrainian/science/2014/12/141204_5g_technology_it

Корольов Дмитро Валерійович
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

ІСТОРІЯ ТЕЛЕКОМУНІКАЦІЙ

Термін телекомунікація складається з грецького теле (τηλε)*, що означає далекий, далеко, або здалеку та латинського комунікація* (communicare)*, що означає ділитись. Його сучасне використання адаптовано у французькій мові, перше письмове використання було зафіксовано у 1904 році французьким інженером і письменником Едуардом Естаньє.*

Взагалі, історію можна розділити на 4 етапів, зараз ми знаходимося в епоху телекомунікацій.

Маяки та Голуби

Свійські голуби використовували в протягом століть різними культурами. Голубина пошта має перське коріння і використовувалися римлянами у військових цілях. Греки пересилали повідомлення з іменами переможців Олімпійських ігор до різних міст використовуючи свійських голубів.

У 1792 році, французький інженер Клод Шапе створив першу фіксовану систему телеграфу (або оптичний телеграф) між Ліллем та Парижем. Однак, недоліком оптичний телеграфів була необхідність у кваліфікованих операторах та дорогих вежах на відстані до 30 кілометрів одна від одної. В результаті конкуренції з електричним телеграфом, остання комерційна лінія була покинута у 1880 році.

Телеграф та телефон

Сір Чарльз Вітсон та сір Вільям Кук винайшли електричний телеграф у 1837 році. Також, перший комерційний електричний телеграф мабуть, був побудований Вітстоном та Куком та відкритий 9 квітня 1839 році. Обидва винахідника розглядали їхній пристрій, як "поліпшення електромагнітного телеграфу", а не як новий пристрій.

Стаціонарний телефон був винайдений незалежно один від одного Алекстандром Беллом та Елішем Грей у 1876. Антоніо Меуччі винайшов перший пристрій, який дозволяв електричну передачу голосу кабелем у 1849 році. Однак його пристрій мав мале практичне значення, оскільки він був оснований на електрофонічному ефекті і тому вимагав, щоб користувачі розміщували приймач у своєму роті, щоб "чути" те, що було сказано. Перший

комерційні телефонні послуги були встановлені у 1878 та 1879 по обидва боки Атлантики в містах Нью-Хейвей та Лондон.

Радіо та телебачення

У 1832 році джеймс Ліндсі продемонстрував бездротовий телеграф його студентам. До 1854 року, він зміг продемонструвати передачу через Ферт Тай з Данді, Шотландія до Вудхейвен, що на відстані 3 кілометрів, використовуючи воду як джерело передачі. У грудні 1901 року, Гульєльмо Марконі встановив бездротове з'єднання між Сент-Джонсон та Полдху, за що отримав у 1909 році Нобелівську премію у фізиці. Проте, невеликий радіозв'язок вже продемонстрував в 1893 році Нікола Тесла на презентації Національна асоціації електричного світла.

25 березня 1925 року, Джон Бейрд зумів продемонструвати передачу рухомого зображення у лондонському універмазі Селфреджез. Притстрій Бейрда був заснований на диску Ніпкова і став відомим як механічне телебачення. Він став основою експериментальних трансляції, зроблених Британською телерадіомовною корпорацією починаючи з 30 вересня 1929 року. Проте у більшості телевізорів 20-го століття використовувалась електронно-променева трубка, яку винайшов Карл Браун. Першу версію такого телевізора було зроблено Філом Фарнсуртом, який показав його сім'ї 7 вересня 1927 року.

Комп'ютери та інтернет

11 вересня 1940 року Джордж Стібіц передав задачу для свого калькулятора комплексних чисел у Нью-Йорку за допомогою телетайпу та отримав результат обчислень у Дартмутському коледжі в Нью-Геймпширі. Така конфігурація централізованого комп'ютера (мейнфрейму) з терміналами віддаленого доступу залишалася популярною і в 1970-х. Проте вже в 1960-х роках дослідники почали розробляти пакетну передачу, технологію, яка посилає повідомлення асинхронно і по частинах до місця призначення, не передаючи його через централізований мейнфрейм. Мережа, яка складається з чотирьох вузлів, виникла 5 грудня 1969 року, що є датою початку роботи ARPANET, яка до 1981 року зросла до 213 вузлів. APRANET зрештою об'єднався з іншими мережами для формування Інтернету. Хоча завдання розробки Інтернету було зосереджено на Робочій Групі Інженерної Мережі Інтернету (IETF), яка опублікувала серію документів для запиту коментарів, інші розробки мережі відбувалися в промислових лабораторіях, такі як розробка локальної мережі (LAN) Ethernet (1983 р.) та протоколу token ring (1984 р.).

Короткі висновки

Телекомунікації мають значний соціальний, культурний та економічний вплив на сучасне суспільство. Телекомунікації пройшли довгий шлях розвитку, щоб розвитися до тих технологій, які ми використовуємо в нашому житті.

Література:

1.https://uk.wikipedia.org/wiki/Телекомунікації#%D0%9C%D0%B0%D1%8F%D0%BA%D0%B8_%D1%82%D0%B0_%D0%B3%D0%BE%D0%BB%D1%83%D0%B1%D0%B8

Калінін Денис Павлович
Державний університет телекомунікацій
Факультет телекомунікацій
м.Київ

5 ТЕХНОЛОГІЙ МАЙБУТНЬОГО, ЯКІ ЗМІНЯТЬ ЖИТТЯ ВЖЕ У 2018

Особливі надії покладаю на 2018 рік, коли ефект, який зроблять нові технології, проявляться з небаченою силою. Уже 30 років люди підключаються до мережі, але сьогодні цим нікого не здивуєш. У 2018 році ми переходимо на новий рівень зв'язку. Тепер люди зможуть ще ефективніше використовувати свої дані, підключаючись до інтелектуальних помічників і до будь-якої хмари за своїм вибором. Отже, представляємо п'ять тенденцій в області високих технологій, які можна розглядати як сферу найбільш перспективних інвестицій в 2018 році.

Дані починають працювати

Зараз організації накопичують стільки даних, скільки людський мозок не зможе обробити протягом усього життя. Для аналізу цієї інформації використовуються штучний інтелект і машинне навчання. Мета цього процесу - допомогти компаніям приймати більш обґрунтовані рішення.

Лікарні стежать, чи вчасно лікарі і медсестри роблять процедури. Банки шукають і усувають проблеми ще до дзвінків від клієнтів. Музеї бачать, які експонати привертають більше відвідувачів. У 2018 році з'явиться безліч прикладів того, як людська уява розсоває межі можливого.

Нові принципи роботи мереж Протягом 30 років в роботі мереж мало що змінювалося. Для ручного управління мережевою конфігурацією була потрібна ціла армія IT-персоналу. У 2018 році настають зміни. Світ переходить до цілей і намірів.Уявіть, що ваша мережа - це автомобіль. До сих пір хтось повинен був сидіти за кермом. Нова мережа, що діє на основі намірів, - це безпілотний автомобіль. Ви говорите, куди потрібно потрапити, і він їде сам.

Точно так же мережа зможе автоматично зконфігурувати пристрої і встановити підключення. Все це відбудеться протягом мілісекунд, а не кількох годин, які були потрібні при ручному конфігуруванні.

Автоматизація віртуальних помічників

Сьогодні люди просять віртуальних помічників дізнатися погоду або показати на мапі напрямок руху. У 2018 році віртуальні помічники настільки "порозумнішають", що зможуть передбачати бажання людей.

Уявіть: ви входите в "розумну" переговорну, розраховану на кілька людей. Зв'язавшись з вашим телефоном, кімната визначить, що ви вже на місці. Устаткування для відеоконференцій поспілкується з вашим календарем і дізнається, що зустріч повинна початися через дві хвилини, і набере потрібний номер.

Кімната також побачить, що ви один, і на кілька градусів підвищить температуру повітря, щоб ви відчували себе комфортно.

Все це доступно автоматизованим помічникам. Всі ваші програми спілкуються один з одним у фоновому режимі і роблять ті чи інші дії. Наукова фантастика? Ні, вже реальність. У 2018 році вона стане ще ближче.

Увійти в будь-яку хмару

Мова вже йде не про підключення до хмари, а про розміщення даних і додатків там, де вони працюють з більшою віддачею, про їх переміщення за бажанням людини, не забуваючи, звичайно, про повну безпеку.

У 2018 року люди зможуть зберігати дані в будь-якому місці: в приватній хмарі, в публічних хмарах Microsoft, Amazon, Google або у всіх перерахованих. Чим більше - тим краще, тому що дані будуть ефективно захищені і структуровані, незалежно від того, скільки хмар людина використовує.

Інформаційна безпека в усьому

Зауважте, я не сказав "інформаційна безпека для всього" або "інформаційна безпека всюди". Всього два слова, але вони багато значать.

У 2018 році люди зможуть вбудовувати засоби інформаційної безпеки в усе, що роблять. Вони побачать, як діють речі та інші люди, зможуть виявити закономірності і отримувати повідомлення при будь-яких змінах.

Уявіть звичайний день одного із співробітників. Кожен день він перевіряє пошту і відвідує певні сайти. Раптом він завантажує файли на сервер, яким не користувався два роки. Це може означати, що він зібрався покинути компанію. Мало того - ще й прихопити з собою дані компанії.

Коли засоби інформаційної безпеки вбудовані в усе, система може швидко виявити відхилення, блокувати передачу файлів і послати керівнику повідомлення. Таким чином можна запобігти проблемам безпеки або, принаймні, швидше на них відреагувати.

Література:
1.http://www.telesphera.net/blog/5-technologies-of-the-future.html
2.https://www.epravda.com.ua/columns/2017/12/27

Панченко Владислав Ігорович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м.Київ

ЗАХИСТ У МЕРЕЖАХ WI-FI

Методи шифрування

WEP-шифрування(*Wired Equivalent Privacy*):
Аналог шифрування трафіку в провідних мережах. Використовується симетричний потоковий шифр RC4 (англ. Rivest Cipher 4), який досить швидко функціонує. На сьогоднішній день WEP і RC4 не вважаються криптостійкими.
Є два основних протоколи WEP:
40-бітний WEP (довжина ключа 64 біта, 24 з яких — це вектор ініціалізації, який передається відкритим текстом);
104-бітний WEP (довжина ключа 128 біт, 24 з яких — це теж вектор ініціалізації); Вектор ініціалізації використовується алгоритмом RC4. Збільшення довжини ключа не призводить до збільшення надійності алгоритму.
TKIP-шифрування(*Temporal Key Integrity Protocol*):
Використовується той же симетричний потоковий шифр RC4, але є більш криптостійким. Вектор ініціалізації становить 48 біт. Враховані основні атаки на WEP. Використовується протокол Message Integrity Check для перевірки цілісності повідомлень, який блокує станцію на 60 секунд, якщо послані протягом 60 секунд два повідомлення не пройшли перевірку цілісності. З урахуванням всіх доопрацювань і удосконалень TKIP все одно не вважається криптостійким.

CKIP-шифрування(*Cisco Key Integrity Protocol*):
Має подібності з протоколом TKIP. Створений компанією Cisco. Використовується протокол CMIC (*Cisco Message Integrity Check*) для перевірки цілісності повідомлень.

WPA-шифрування:
Замість уразливого RC4, використовується криптостійкий алгоритм шифрування AES (*Advanced Encryption Standard*). Можливе використання EAP (англ. Extensible Authentication Protocol, розширюваний протокол автентифікації). Є два режими: Pre-Shared Key (WPA-PSK) - кожен вузол вводить пароль для доступу до мережі; Enterprise - перевірка здійснюється серверами RADIUS;

WPA2-шифрування(IEEE 802.11i):
Прийнятий у 2004 році, з 2006 року WPA2 повинна підтримувати все вироблене Wi-Fi обладнання. В даному протоколі застосовується RSN (англ. Robust Security Network, мережа з підвищеною безпекою). Спочатку в WPA2 використовувався протокол CCMP (англ. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, протокол блочного шифрування з кодом автентичності повідомлення і режимом зчеплення блоків і лічильника). Основою є алгоритм AES. Для сумісності зі старим обладнанням є підтримка TKIP і EAP (*Extensible Authentication Protocol*) з деякими його доповненнями. Як і в WPA є два режими роботи: Pre-Shared Key і Enterprise[1]. Для виходу в інтернет переважна більшість користувачів домашньої мережі використовує Wi-Fi роутери. Коли

мережа незахищена, її можуть використати зловмисники, вважають у Департаменті кіберполіції України. Саме тому, для захисту домашньої мережі від шахрайських дій кіберполіція склала рекомендації. Що варто знати і зробити – у рекомендаціях нижче:

1) Зміна налаштувань DNS серверу. Будь-яке доменне ім'я, наприклад, google.com.ua відповідає індивідуальній IP-адресі, тобто сайт google.com.ua відповідає IP-адресі 74.125.232.255. Якщо ввести у браузері замість сайту google.com.ua IP-адресу 74.125.232.255, завдяки DNS-серверу буде здійснено перехід на веб-сайт google.com.ua. Так, зловмнисник може змінити DNS-сервер на свій власний і налаштувати, наприклад, щоб браузер при введенні сайту google.com.ua переходив на його особисту IP-адресу. Внаслідок цього буде здійснено перехоплення веб-трафіку або зараження вашого особистого ПК, чи будь-якого пристрою, який отримує доступ до мережі з вашого роутера.

2)Наступне, що може здійснити зловмисник – це перехоплення вашої особистої інформації шляхом атаки men-in-the-middle. В такому випадку ваш веб-трафік, який за замовчуванням відправляється до Wi-Fi роутера, буде відправлений спочатку зловмиснику, а потім від нього до роутера. При цьому роутер не помітить змін. Така атака дозволяє хакеру викрасти ваші особисті дані (логіни, паролі), продивитись ваш веб-трафік – сайти, на які ви заходили.

3) Зловмисник, перебуваючи у вашій особистій Wi-Fi мережі, може здійснювати хакерські атаки (взломи сайтів, DDOS-атаки, додати ваші пристрої до бот-мережі, скачувати дитячу порнографію), тобто будь-які незаконні дії від вашого імені, оскільки Wi-Fi роутер має IP-адресу, яку вам надає ваш провайдер при сплаті інтернет-послуг: всі пристрої, підключені до вашого роутера або точки доступу в інтернет, будуть ідентифікуватись за вашою IP-адресою.

Література:

1. *https://uk.wikipedia.org/wiki*
2. *http://watcher.com.ua/2016/09/20/yak-zahystyty-domashnyu-wi-fi-merezhu-vid-hakeriv/*

Панченко Владислав Ігорович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м.Київ

ТЕЛЕКОМУКАЦІЙНА МЕРЕЖА

Телекомунікаційна мережа — комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

За географічним розташуванням:

1.Локальна мережа (Local Area Network — LAN) — звичайно розташована в межах будинку.

2.Глобальна мережа (Wide Area Network — WAN) — охоплює географічний регіон (країну або континент).

3.Міська мережа (Metropolitain Area Network — MAN) — застосовується для об'єднання мереж в місті в одну велику мережу.

4.Internet — індивідуальні комп'ютери під'єднані до інших мереж у світі через публічну мережу(мережу загального користування).

5.Intranet — індивідуальні комп'ютери під'єднані до інших мереж через приватну мережу.

6.Віртуальна приватна мережа (Virtual Private Network — VPN) — індивідуальні комп'ютери під'єднані до інших мереж через сегмент публічної мережі.

За структурою взаємозв'язків (топологією):

a)Пункт-пункт (фізична або логічна).

b)Кільце (фізичне або логічне).

c)Шина (фізична).
d)Широкомовна (логічна).
f)Сітка (фізична або логічна).
g)Комутована або з габами (фізична або логічна).

За режимом комунікації:

1)режим «пункт-пункт»: кожна пара вузлів має взаємозв'язок; цей зв'язок не використовується іншими вузлами;

2)комутований режим: у мережі «пункт-пункт» необхідна кількість зв'язків зменшена за допомогою комутаторів;

3)багатопунктовий (широкомовний) режим: спільний комунікаційний канал використовується всіма вузлами мережі.

За швидкістю мережі:

a)низькошвидкісна: швидкості від кбіт/с до Мбіт/с.

b)високошвидкісна: швидкості від сотень Мбіт/с до Гбіт/с.

Література:
1.https://uk.wikipedia.org/wiki

Панченко Владислав Ігорович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м.Київ

ОПТОВОЛОКНО

Оптоволокно́ або оптичне волокно — це технічний виріб, що складається з оптичного світловоду і захисних покриттів та маркуючої кольорової оболонки.

Оптичний світловод — є фізичним середовищем транспортування оптичного сигналу і складається із серцевини та оболонки, що мають різні величини показників заломлення. Завдяки явищу повного внутрішнього відбиття, надається змога транспортувати оптичні сигнали (світло), що генеруються обладнанням, до якого підключене оптичне волокно.Повний опис процесу розповсюдження світла по оптичному волоконному світловоду (ВС) дає хвильова електромагнітна теорія. Вона показує, що розповсюджуватись по волоконному світловоду можуть лише ті типи хвиль, що формують у поперечному перетині ВС резонансну хвилю. Такі типи хвиль утворюють моди хвилеводу. Режим роботи ВС (одно — чи багатомодовий) визначається величиною нормованої частоти V.

Згідно режиму роботи оптичні волокна (ОВ) поділяються на два основні типи:

1)Одномодові
2)Багатомодові

Багатомодове оптичне волокно — оптичне волокно, яке має зазвичай більшу товщину від одномодового волокна та за рахунок цього може нести декілька мод повного внутрішнього відбиття, направленого під різними кутами до внутрішньої поверхні. Багатомодовий оптичний кабель є різновидом оптоволоконного кабелю, що має великий діаметр серцевини і проводить промені світла за допомогою ефекту внутрішнього відображення. Багатомодовий оптичний кабель загального призначення завдяки своїй конструкції має низку важливих користувацьких властивостей, які дають можливість однаково ефективно використовувати його як виріб внутрішньої, так і зовнішньої прокладки. Кабель має однотрубкове модульне виконання, його світлопроводи знаходяться в центральній трубці, що заповнена гідрофобним гелем і ефективно захищає волокна від коливань температури навколишнього середовища і від механічних впливів. Трубка зі світловодами забезпечена плетенням із склотканини, яка додатково захищає волокна від

механічних впливів і пошкоджень гризунами. Зовнішня негорюча захисна оболонка має рівень LSZH (малодимна, з нульовим вмістом галогенів), тобто в процесі горіння не виділяє задушливих газів, а також додатково оберігає елементи сердечника від впливу ультрафіолетового випромінювання.

Література:
1.https://uk.wikipedia.org/wiki

Файдюк Олександр Володимирович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м.Київ

СОНЯЧНА ЕНЕРГЕТИКА

Сонячна енергетика — використання сонячної енергії для отримання енергії в будь-якому зручному для її використання вигляді. Сонячна енергетика використовує поновлюване джерело енергії і в перспективі може стати екологічно чистою, тобто такою, що не виробляє шкідливих відходів.

На сьогодні сонячна енергетика широко застосовується у випадках, коли малодоступність інших джерел енергії в сукупності з достатньою кількістю сонячного випромінювання виправдовує її економічно.

Сонячна енергія, на поверхні Землі

Потік сонячного випромінювання, що проходить через площу 1 м², розташовану перпендикулярно потоку випромінювання на відстані однієї астрономічної одиниці від центру Сонця (тобто зовні атмосфери) Землі, дорівнює 1367 Вт/м² (сонячна постійна).

Способи отримання електрики і тепла з сонячного випромінювання:

- Отримання електроенргії за допомогою фотоелементів. Для цієї мети застосовують кремнієві сонячні батареї, ККД яких доходить до 20 %. Але вартість отримання чистого кремнію досить велика. Кремній, в якому на 10 кг продукту припадає не більше 1 грама домішок коштує стільки ж, скільки збагачений уран для електростанцій, хоча запаси останнього в 100 000 разів менше запасів кремнію. У той же час, «хорошого» кремнію у світі добувають в 6 разів менше, ніж такого ж урану.

- Геліотермальна енергетика — нагрівання поверхні, що поглинає сонячні промені і подальший розподіл і використання тепла (фокусування сонячного випромінювання на ємності з водою для подальшого використання нагрітої води в опалюванні або в парових електрогенераторах).
- «Сонячне вітрило» може в безповітряному просторі перетворювати сонячні промені в кінетичну енергію.
- Термоповітряні електростанції (перетворення сонячної енергії в енергію повітряного потоку, що направляється на турбогенератор).
- Сонячні аеростатні електростанції (генерація водяної пари усередині балона аеростата за рахунок нагрівання сонячним випромінюванням поверхні аеростата, покритої селективно-поглинаючим покриттям). Перевага — запасу пари в балоні достатньо для роботи електростанції в темний час доби і хмарну погоду.

Переваги сонячної енергетики:

- Загальнодоступність і невичерпність джерела.
- Теоретично, повна безпека для навколишнього середовища (проте в наш час у виробництві фотоелементів і в них самих використовуються шкідливі речовини).

Недоліки сонячної енергетики:

- Потік сонячної енергії на поверхні Землі сильно залежить від широти і клімату.

- Сонячна електростанція не працює вночі і недостатньо ефективно працює у ранкових і вечірніх сутінках.
- Висока ціна сонячних фотоелементів.
- Недостатній ККД сонячних елементів
- Поверхню фотопанелей потрібно очищати від пилу і інших забруднень.
- Ефективність фотоелектричних елементів помітно падає при їх нагріванні, тому виникає необхідність в установці систем охолоджування, зазвичай водяних.
- З кожним роком експлуатації ефективність фотоелектричних елементів знижується.
- Незважаючи на екологічну чистоту отримуваної енергії, самі фотоелементи містять отруйні речовини

Сонячна енергетика розвивається з кожним днем, і в майбутньому сонячна енергія зможе забезпечувати мало не всю земну кулю.

Література:

1.*https://uk.wikipedia.org/wiki/Сонячна_енергетика*
2.*https://proektozbereshennya.io.ua*
3.*http://1sovetnik.net/kak-gde-pochemu/item/48-solnechnaya-energiya-reshenie-buduschego4 solnechnye-elektrostancii.html*

Яременко Виктор Вячеславович
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
г. ***Киев***

БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ

Беспроводные технологии *— подкласс информационных технологий, служат для передачи информации между двумя и более точками на расстоянии, не требуя проводной связи. Для передачи информации могут использоваться радиоволны, а также инфракрасное, оптическое или лазерное излучение. Существует множество беспроводных технологий, наиболее часто известных по маркетинговым названиям, таким как Wi-Fi, WiMAX, Bluetooth. Каждая технология обладает определёнными характеристиками, которые определяются её областью применения.*

История

История беспроводных технологий берет свое начало в конце **XIX**века, когда получил свое развитие телеграф Маркони. Запатентованная в 1896 году в Англии, эта технология обеспечивала передачу радиоволн без проводов на большие расстояния. Однако телеграф Маркони мог передавать только точки и тире азбуки Морзе, а не живой голос. В 1920 году такие компании, как General Electric (GE), AT&T и вновь созданная Radio Corporation of America (RCA) включились в создание беспроводной индустрии — AM-радио. С ростом радио континента росла и потребность в радиопередачах у слушателей. К 1929 году в США было более 6 млн. радиоприемников, которые стали новым средством получения информации. Беспроводные технологии распространялись, даже несмотря на глобальную депрессию 1930-х годов и появление таких новшеств, как радио с частотной модуляцией (FM) и телевидение. Вторая мировая война только ускорила развитие беспроводной связи, поскольку военные вкладывали в это значительные ресурсы. Первые беспроводные телефонные системы появились в США в 1970-е годы. Основанные на технологии, разработанной в лабораториях Белла компании AT&T, эти системы были аналоговыми, работали в ограниченном диапазоне частот и могли одновременно обрабатывать только небольшое число вызовов. Их использовали в основном для

обеспечения безопасности и усиления силовых структур. В течение 1990-х годов беспроводные технологии наконец-то завоевали достойное место на рынке. Вдобавок к расширяющимся сетям, которые передают голос, в 90-е годы появились многочисленные беспроводные сети, ориентированные только на передачу текстовых данных, в частности пейджинговые системы. Они существовали с 60-х годов, но их использование ограничивалось некоторыми вертикальными рынками, например в областях охраны правопорядка и медицины. Подобные системы были односторонними и могли посылать только сигнал типа звонка. Начиная с начала 90-х годов операторы стали активно совершенствовать такие сети, расширять их функциональность, обеспечивая возможность двусторонней связи и передачу буквенных и цифровых сообщений. В самом разгаре революции беспроводной связи вышла на сцену еще одна технология, «подрывающая традиции», — World Wide Web, Всемирная паутина. На первом этапе своего коммерческого развития Паутина управлялась компанией Netscape Communication Corp. среди пользователей разгорелись такие страсти, каких еще не видела история. Обитатели Internet были в восторге от того, что можно получать доступ к необъятным хранилищам информации и устанавливать связь с другими людьми по всей планете — впрочем, только при наличии очень мощного компьютера.

Влияние на здоровье

В настоящее время в мировой научной литературе опубликовано огромное число исследований по теме влияния излучения беспроводных приборов на здоровье. Среди них самое масштабное международное эпидемиологическое исследование INTERPHONE (в 2002—2011) под эгидой Всемирной организации здравоохранения, которое должно было показать, может ли глобальное использование приборов беспроводной связи приводить к развитию различных видов малигнизации (развитию онкологических болезней). В 2005 году китайские исследователи пришли к выводу, что излучение мобильного телефона приводит к повреждению ДНК. В некоторых странах существуют нормы, ограничивающие использование аппаратов, имеющих слишком высокий уровень излучения. В 2007 году шведские учёные сделали вывод по результатам обработки 11 исследований, что при использовании сотового телефона в течение 10 лет вероятность возникновения опухоли слухового нерва увеличивается в два раза. При этом отмечается, что дети подвержены этому риску больше, так как имеют более тонкие костные ткани, чем взрослые. Но руководитель исследования Кьелл Мильд заявил, что ещё рано делать окончательные выводы о вреде радиоволн для человека и необходимы более длительные исследования

Классификация беспроводных технологий

По дальности действия:

- Беспроводные персональные сети (WPAN — Wireless Personal Area Networks). Примеры технологий — Bluetooth.
- Беспроводные локальные сети (WLAN — Wireless Local Area Networks). Примеры технологий — Wi-Fi.
- Беспроводные сети масштаба города (WMAN — Wireless Metropolitan Area Networks). Примеры технологий — WiMAX.
- Беспроводные глобальные сети (WWAN — Wireless Wide Area Network). Примеры технологий — CSD, GPRS, EDGE, EV-DO, HSPA, UMTS, LTE, LTE-A.

По топологии:

- «Точка-точка».
- «Точка-многоточка».

По области применения:

- Корпоративные (ведомственные) беспроводные сети — создаваемые компаниями для собственных нужд.

- Операторские беспроводные сети — создаваемые операторами связи для возмездного оказания услуг.

Литература:

1.https://ru.wikipedia.org/wiki/Беспроводные_технологии

Михайлов Олексій
КПІ ім. Ігоря Сікорського
Факультет електроніки
м.Київ

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ CWDM У ВОЛОКОННО-ОПТИЧНИХ ЛІНІЯХ ЗВ'ЯЗКУ СЕГМЕНТУ УКРАЇНСЬКОЇ НАУКОВО-ОСВІТНЬОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ "УРАН" В МІСТІ ХМЕЛЬНИЦЬКОМУ

Технологія спектрального ущільнення каналів CWDM (Coarse Wavelength Division Multiplexing) з поділом по довжинах хвиль з'явившись на початку 80-х років минулого сторіччя, 10 років поспіль стала широко застосовуватися в міських і регіональних мережах. Ця технологія дозволила збільшити пропускну здатність оптичних ліній зв'язку, за рахунок методу мультиплексування с розподілом по довжині хвилі. Розвиток систем CWDM став можливим завдяки поліпшенню технології виготовлення оптичного волокна, що дало можливість на порядок розширити його робочу смугу пропускання, зменшити загасання сигналу в смузі пропускання, що у свою чергу дозволило значно (в 10-50 разів) збільшити крок несучих хвиль, істотно спростити фільтрацію несучих хвиль на приймальній стороні, знизити витрати на побудову мереж зв'язку за рахунок виключення дорогих елементів і на покупку та прокладку оптичного волокна [1, с.359].

В рамках роботи було досліджено та запропоновано варіант модернізації мережі «УРАН» в м. Хмельницькому за рахунок переведення її на технологію CWDM.

Мережа «УРАН» має 2 вузлових комутатора, які розміщенні в Хмельницькому обласному центрі науково-технічної творчості учнівської молоді (вул. Проскурівська 83) та в Хмельницькому національному університеті (вул. Кам'янецька 110/1) і на даний час з'єднанні між собою оптичним волокном та використовують STP протокол для усунення петель. З метою модернізації зазначеної мережі було запропоновано на стороні кожного абонента встановити MUX/DEMUX на приймаючій та передаваючій сторонах, а також встановити нове обладнання CWDM паралельно існуючому для здійснення безперебійної передачі даних.

У разі реалізації запропонованого варіанту модернізації мережі «УРАН» можливо підвищити її надійність, збільшити кількість каналів для підключення більшої кількості абонентів, не витрачаючи кошти на прокладку нового оптичного волокна.

Література:

1.Слепов Н. Н. Современные технологии цифровых оптоволоконных сетей связи. – Москва.: Радио и связь, 2000. – 468 с.
2.http://www.konturm.ru/newsprint.php?id=help/stat120310

Елиссави Камал Кхалифа А.
Государственный университет телекоммуникаций
Аспиратн
г. ***Киев***

ЭВОЛЮЦИЯ РАЗВИТИЯ ПЕРВИЧНЫХ ИСТОЧНИКОВ СИНХРОНИЗАЦИИ

Показана эволюция развития первичных источников синхронизации. Рассмотрено назначение и принцип действия первичного опорного генератора шкалы времени в сетях с передачей пакетов и

усовершенствованного первичного эталонного генератора сигналов частоты и времени для мультисервисной макросети мобильного оператора.

Развитие современных сетей связи невозможно без точных часов – прецизионных стандартов частоты. Если десятикратное увеличение точности измерения массы, длины и других физических величин происходит каждые 50 лет, то десятикратное увеличение точности измерения времени и частоты - каждые 20 лет [1]. Современный предел относительной точности измерения частоты и времени оценивают величиной $10^{-14} – 10^{-16}$.
На заре развития сетей синхронизации полагалось, что достаточно одного первичного эталонного генератора (PRC - Primary Reference Clock) на всю сеть и можно было бы мириться с их высокой стоимостью. В современных сетях PRC становится массовым изделием [2]. Поэтому производители квантовых стандартов частоты, желая сохранить позиции на рынке оборудования синхронизации, поставляют первичные источники синхронизации (PRS – Primary Reference Source). Это просто стандарт частоты без резервирования, как правило, снабженный стыками.

Важным моментом в развитии атомных часов (Atomic Clocks) за последнее десятилетие является утверждение новых требований к точности и стабильности, а также появление требований к фазовой синхронизации, фактически к параметру “время” (что особенно важно для сетей мобильной связи 4G – LTE) [1, 2, 3].
На рис. 1 представлена эволюция развития первичных источников синхронизации:

- PRC - первичный эталонный генератор для “классической” сети синхронизации;
- PRTC – первичный опорный генератор шкалы времени в сетях с передачей пакетов;
- ePRTC (enhanced Primary Reference Time Clock - усовершенствованный первичный эталонный генератор сигналов частоты и времени для мультисервисной макросети мобильного оператора.

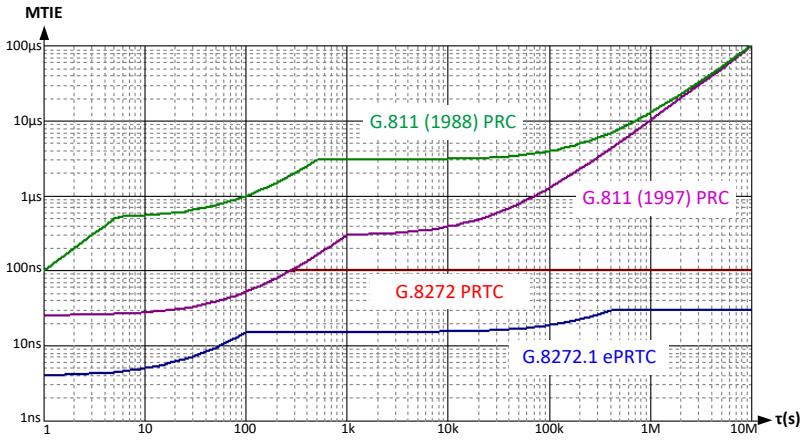


Рис. 1 Эволюция развития первичных источников синхронизации

Повышение требований к точности синхронизации в мультисервисных макросетях ставит новые задачи перед разработчиками специализированного оборудования. Обновляется и международная нормативная база, в частности, требования к генераторному оборудованию различного класса. Примером может служить недавно вышедшая Рекомендация ITU-T G.8272.1/Y.1367.1 [5], определяющая основные характеристики улучшенного первичного эталонного генератора частоты и времени ePRTC. По сравнению с “обычным” PRTC (Рекомендация ITU-T G.8272/Y.1367 [4]), к генераторному оборудованию ePRTC предъявляются более жесткие требования в части уровня фазовых шумов на выходе: расчет максимальной ошибки по временному интервалу (MTIE) и временного отклонения (TDEV):

- в режиме захвата опорного сигнала максимальное отклонение временного интервала (MTIE) не должно превышать 30 нс при $\tau \geq 400\,000$ с (в то время как для “обычного” PRTC значение MTIE не должно превышать 100 нс при $\tau \geq 273$ с);

- в режиме удержания максимальный уход фазы за 14 суток не должен превышать 100 нс.

На рис. 2 показаны показатели временного отклонения TDEV для ePRTC.

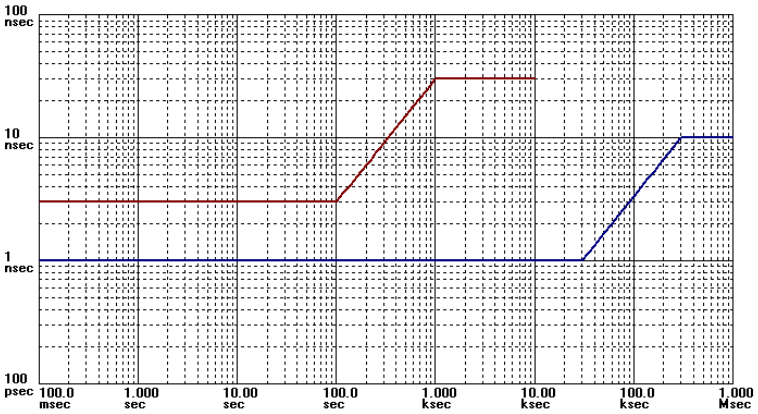


Рис. 2 Показатели временного отклонения TDEV для ePRTC

Эволюция атомных стандартов частоты предполагает изменение параметров стабильности синхронизации и их характеристик. Меняется сама концепция построения первичных источников сигналов синхронизации – [5] (ePRTC). В процессе развертывания и эксплуатации сети синхронизации на транспортной сети IP/MPLS возникает необходимость в создании системы мониторинга сигналов синхронизации.

Внедрение подсетей синхронизации на транспортной сети IP/MPLS в настоящее время является практической необходимостью. За последние годы было реализовано несколько проектов на основе протоколов PTP. Интеграция Atomic Clock в транспортную среду IP/MPLS на основе протокола PTP позволяет реализовать полноценный ePRTC с использованием всех преимуществ новейших технологий.

Литература:

1. C. Audoin, B. Guinot. The Measurement of Time. Time, Frequency and the Atomic Clock. Cambridge University Press, 1998.

2. S. Bregni. Synchronization of Digital Telecommunication Networks. John Willey & Sons, Inc. 2001.

3. D.L. Mills. Computer network time synchronization: the network time protocol. CRC Press, 2006.

4. ITU-T Recommendation G.8272/Y.1367 (01/2015) Timing characteristics of primary reference time clocks.

5. ITU-T Recommendation G.8272.1/Y.1367.1 (11/2016) Timing characteristics of enhanced primary reference time clocks.

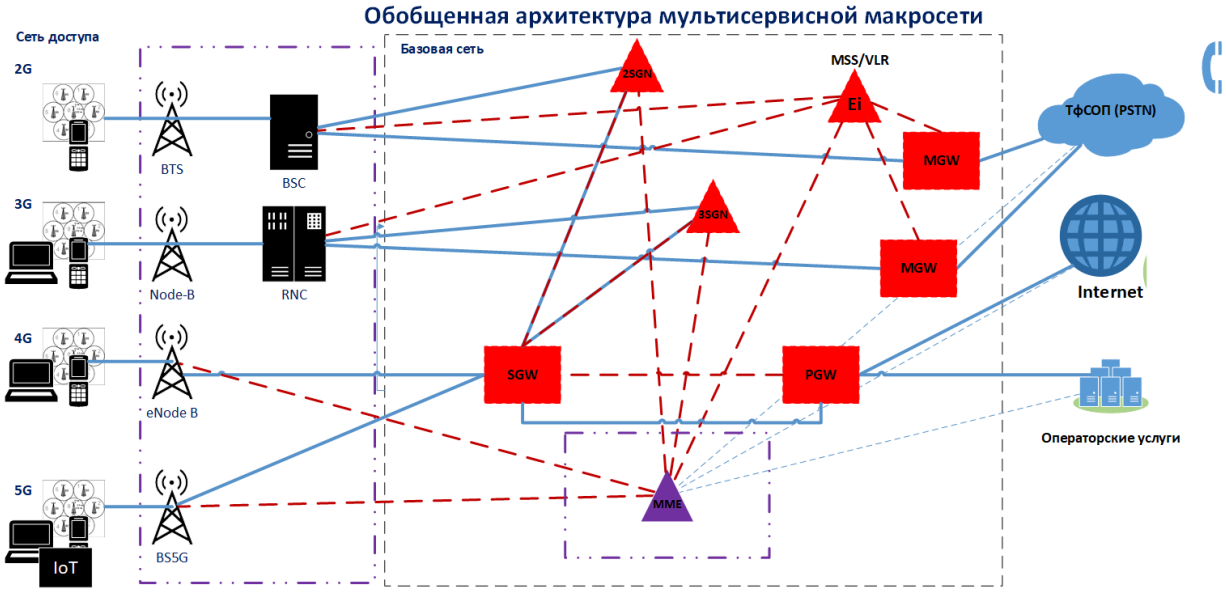
Федорова Н. В.
Елиссави Камал Кхалифа А.
Государственный университет телекоммуникаций
Аспирант
г.Киев

СИНХРОНИЗАЦИИ ЧАСТОТЫ И ВРЕМЕНИ В МУЛЬТИСЕРВИСНЫХ МАКРОСЕТЯХ

Приведена архитектура мультисервисной макросети мобильного оператора и схема сетевой синхронизации. Отмечены актуальные вопросы сетевой синхронизации в мультисервисной макросети. Рассмотрена необходимость в обеспечении сигналами точного времени мультисервисной макросети. Приведены основные методы обеспечения сетевой синхронизацией.

Сегодня, как никогда на рынке мобильных услуг наблюдается тенденция постоянного увеличения количества пользователей, так, только в третьем квартале 2017 года количество подключений к сети 4G увеличилось на 160 млн., достигнув общемирового показателя в 1,5 млрд. Согласно прогнозам, к 2022 году на планете будет 29 млрд. подключенных устройств, 18 млрд. с которых — это устройства интернет вещей.

Активное эволюционное развитие технологий в ближайшей перспективе приведет к созданию мультисервисных макросетей, целью которых будет решение принципиально новых задач. Согласно концепции «неразрушимого» перехода от традиционных сетей с коммутацией каналов к сетям с коммутацией пакетов, подобные решения должны позволять частично переводить отдельные сегменты на новые технологии без кардинальных изменений всей сетевой структуры [1, 2]. На рис. 1 приведена общая архитектура мультисервисной макросети мобильного оператора.



Примечание: 2G, 3G, 4G, 5G – технологии мобильных сетей; BTS – базовая станция 2G; NodeB – базовая станция 3G; eNodeB – базовая станция 4G; BS5G – базовая станция 5G; BSC – контроллер сети радиодоступа 2G; RNC - контроллер сети радиодоступа 3G; MSC - телефонная станция; MSS – MSC сервер (управление служебными данными); MGW – медиашлюз (управление абонентскими данными); SGSN - компонент системы по реализации всех функций обработки пакетной информации; SGW – шлюз обслуживания; PGW - пакетный шлюз; MME – узел управления сетью.

Рис. 1. Архитектура мультисервисной макросети мобильного оператора

При увеличение количества устройств (например, базовых станций мобильной связи), которые подключаются по IP-сети, проблемы синхронизации должны рассматриваться системно. С этим связана некоторая локальная революция в подходе: появление некоторой "критической массы" потребителей сигналов синхронизации в мультисервисной макросети ведет к необходимости рассматривать систему синхронизации как отдельную составную часть системы электросвязи. При дальнейшем увеличении количества цифровых устройств начинает изменяться концепция построения сетевой синхронизации и принципы управления ею. В зависимости от актуальных телекоммуникационных технологий мультисервисной макросети изменяется и содержание [3]:

- задач синхронизации - выбора методов синхронизации и способов распространения сигналов в распределительной сети синхронизации;
- набора нормируемых параметров и методов их измерений;
- объемов контроля параметров синхронизации.

К основным методам обеспечения сетевой синхронизацией в мультисервисной макросети относятся [4, 5]:

- функционирующий на физическом уровне механизм Sync-E, независимый от загрузки сети и позволяющий передавать сигнал синхронизации через транзитные устройства. Но механизм Sync-E обеспечивает только частотную синхронизацию. Кроме того, переход на технологию Sync-E предусматривает полную замену сетевого оборудования или его существенное обновление;

- протокол PTP (Precision Time Protocol) работает на канальном уровне передачи данных и обеспечивает как частотную, так и временную синхронизацию, но стабильность распространяемого сигнала зависит от уровня загруженности сети, а также от расстояния между сетевыми узлами и количества переприемов;

- протокол NTP (Network Time Protocol) работает на прикладном уровне и широко используется, как правило, для временной синхронизации в пакетных сетях. Но в ряде решений разных производителей оборудования (например, базовых станций производства Ericsson), протокол NTP может быть использован также и для частотной синхронизации.
На данном этапе также является актуальным вопрос проведения измерений параметров

Протокол PTP является на сегодняшний день наиболее оптимальным методом синхронизации в мультисервисной макросети. Протокол PTP обеспечивает как частотную, так и временную синхронизацию при высоком качестве параметров стабильности.
Привлекательными сторонами частотно-временного обеспечения сетей связи с использованием PTP являются:

- удовлетворение потребностей всех существующих служб;
- простота решения и минимальные затраты.
- «клиенты» PTP могут быть дополнены серверами NTP, распределяющими сигналы времени по IP адресам от «клиента» PTP до любого компьютера. Технология распределения по протоколу NTP (компьютерная сеть) отработана и заложена в имеющееся оборудование сетей электросвязи.

Литература:

1.Технологии мобильной связи пятого поколения (5G). - http"//ericsson.com/kz/news/130919_wp_5g_254740124.

2. Терещук Сергей Когда Украине ждать 4G и 5G связи. - https://delo.ua/tech/kogda-ukraine-zdat-4g-i-5g-svjazi-325879#

3. Миллс Д. Сличение времени в компьютерных сетях: протокол сетевого времени на Земле и в космосе. / Миллс Д. [пер. с англ. под ред. А.В. Савчука,] – К.: WIRCOM. – 2011. – 464 с.

4. Савчук А.В. Синхронизация текущего времени: Протокол сетевого времени / А.В. Савчук, В.Н. Шапошников, И.П. Черняк // Зв'язок №6. – 2007. - С. 10 – 15.

5. Федорова Н.В. Методы обеспечения синхронизацией базових станций от разных иерархических уровней сети с коммутацией пакетов / В. И. Вакась, Н. В. Федорова // Вісник ДУІКТ. – 2012. – Т. 10, №4. – С.91-96.

Тімченко Артем
Державний університет телекомунікацій
Факультет Інформаційних технолоігй
м. Київ

USING AMAZON WEB SERVICES FOR CLOUD COMPUTING

This article discusses the history and prospects of cloud services from Amazon Web Services. The various services provided by Amazon are provided, general information on cloud computing is provided. The perspectives of using these services are shown.

Amazon Web Services (AWS) is a subsidiary of Amazon.com that provides on-demand cloud computing platforms to individuals, companies and governments, on a paid subscription basis. The technology allows subscribers to have at their disposal a full-fledged virtual cluster of computers, available all the time, through the Internet. AWS's version of virtual computers have most of the attributes of a real computer including hardware (CPU(s) & GPU(s) for processing,

local/RAM memory, hard-disk/SSD storage); a choice of operating systems; networking; and pre-loaded application software such as web servers, databases, CRM, etc. Each AWS system also virtualizes its console I/O (keyboard, display, and mouse), allowing AWS subscribers to connect to their AWS system using a modern browser. The browser acts as a window into the virtual computer, letting subscribers log-in, configure and use their virtual systems just as they would a real physical computer. They can choose to deploy their AWS systems to provide internet-based services for their own and their customers' benefit.

The AWS technology is implemented at server farms throughout the world, and maintained by the Amazon subsidiary. Fees are based on a combination of usage, the hardware/OS/software/networking features chosen by the subscriber, required availability, redundancy, security, and service options. Based on what the subscriber needs and pays for, they can reserve a single virtual AWS computer, a cluster of virtual computers, a physical (real) computer dedicated for their exclusive use, or even a cluster of dedicated physical computers. As part of the subscription agreement, Amazon manages, upgrades, and provides industry-standard security to each subscriber's system. AWS operates from many global geographical regions including 6 in North America.

Literature:

1. *Getting Started with AWS - USA.: Amazon Digital Services LLC, 2012.- 162 p.*
2. *Practice Questions - AWS Certified Solutions Architect Exam/ Zohaib Jabbar – USA.: Amazon Digital Services LLC, 2017.- 178 p.*

Каграманова Юлія

Державний університет телекомунікацій

Факультет Телекомунікацій

м. Київ

СИСТЕМА ЗВ'ЯЗКУ END-TO-END

Мене часто питають, навіщо ховати електронне листування, мені нема чого приховувати. Що ж можливо вам і насправді немає чого ховати, проте безпека персональних даних це щось значно більше. Уявіть, що вийде, якщо ваше листування буде доступне кому завгодно, і кожен зможе знати, що ви робите, куди йдете, у що вірите, кого любите,або навпаки, кого не полюбляєте. Такий світ стане всього на крок від тоталітарної системи описаній в книзі Оруела - 1984. Також існує і фактор технічної безпеки -усе наше життя сьогодні в мережі. Ми користуємось послугами банків, ми укладаємо угоди, висилаємо персональну інформацію, і усе це в електронному вигляді. Уся світова економіка стала електронною і без шифрування сьогодні просто не обійтись.

Базуючись на принципах end-to-end шифрування ми можемо в значному степені запобігти потенційним інформаційним ризикам. Так, як в цьому разі прочитати данні і скористатись ними можуть тільки кінцеві користувачі. Володарі ж проміжних серверів, через який проходить інформація зчитати данні не зможуть. Наша персональна безпека у мережі являється передумовою нашої персональної безпеки.

В 2013 році Едвард Сноуден повідомив. що могутні спецслужби по всьому світі займаються шпигунством за громадянами і їх листуванням. Інформація сьогодні це актив, який став дорожче грошей. Подивіться на такі мережі, як Facebook, чи Google. Їхнє золото це інформація. Інформаційна безпека у 21 столітті стане, чи не головним питанням.

Шифрування це спосіб уберегти данні від несанкціонованого доступу. Уявимо собі двох користувачів, які спілкуються між собою будь якою мовою, до прикладу англійською. Для них інша розмова, який проходить до прикладу на швейцарському діалекті німецької мови буде зашифрований, і вони нічого не зрозуміють не володіючи ключем. В даному випадку знанням швейцарського діалекту.

Історія створення

Сама ідея end-to-end не нова. У 1991-му році Філом Зіммерманом було розроблено програмне забезпечення для шифрування повідомлень і інших даних PGP (Pretty Good Privacy). У наступні роки алгоритм і відповідне ПО вдосконалили і додали додаткові механізми.

У 1997-му році компанія PGP Inc. запропонувала ініціативу OpenPGP, а в 1999-му учасниками руху вільного програмного забезпечення на основі відкритого стандарту була створена вільна реалізація PGP - GnuPG.

Це все до того, що, так як злом PGP ще не був зафіксований, на основі відкритого PGP (адже вихідні коди є) можна створювати механізми шифрування, ніж, швидше за все, і займаються розробники месенджерів. Чи не писати адже з нуля.

Передумови

Колишній агент ЦРУ Едвард Сноуден представив усьому світові докази того, що американська розвідка використовує в роботі незаконні методи. Він опублікував кілька сотень секретних документів, у тому числі накази американського президент Барака Обами про підготовку кібер атак по всьому світу, про прослуховування телефонних розмов. Завдяки Едварду Сноудену стало відомо про глобальне стеження за громадянами США та інших країн за допомогою соціальних мереж, телефонних операторів, комп'ютерних програм («Skype» і інші). Зі спецслужбами пов'язані корпорації «Microsoft», «Apple», «Yahoo», «Google», «Facebook», «AOL» та інші. Агент розповів також про прослуховування телефонних розмов лідерів країн, що входять в велику двадцятку.

Ефект метелика - розгромний доповідь Сноудена зобов'язав усіх захищатися і шифруватися. Підштовхнувши інформаційну індустрію до кроків у бік безпеки.

Особливості

>>Технологія шифрування end-to-end робить повідомлення доступними тільки для співрозмовників.

>>Переважна більшість фахівців з інформаційної безпеки визнають наскрізне (end-to-end) шифрування найбільш стійким методом захисту інформації.

>>При end-to-end шифруванні ключі, які використовуються для шифрування та розшифрування інформації, генеруються і зберігаються тільки на кінцевих вузлах листування, тобто, у її учасників.

>>Серверна сторона не бере ніякої участі в створенні ключів, а, отже, не має до них доступу, в результаті чого, бачить тільки закодовані дані, що передаються між учасниками. Тільки останні можуть розкодувати і прочитати інформацію.

Як працює?

Технологія шифрування end-to-end це доволі складна технологія шифрування, яку можливо пояснити буквально на пальцях. Спілкуючись зі своїм другом я відсилаю йому відкритий замок і невелику дорожню скриню. Мій друг кладе у нього свій лист, закриває його на замок своїм відкритим ключем і відсилає його мені. І ніхто, крім нас двох не може прочитати записку, яка лежить у цій скринці тому, що у них не буде закритого ключа, яким володію тільки я, і ніхто більше. Тим самим я зможу майже на 100% захистити своє листування.

Під час початку сеансу зв'язку, на стороні кожного співрозмовника генеруються по 2 ключа: відкритий і закритий. Останній використовується для розшифровки даних, цей ключ не залишає межі локального пристрою.

Відкритий ключ з відкритого каналу зв'язку передається співрозмовнику (одному або всім, в разі, якщо їх декілька). За допомогою відкритого ключа співрозмовник може тільки зашифрувати дані, а розшифрувати їх може тільки власник відповідного закритого ключа. Тому, не важливо, хто перехопить відкритий ключ. В результаті цього, він зможе тільки передавати свої зашифровані дані.

Згенерувавши по парі ключів, співрозмовники обмінюються відкритими ключами, після чого починається захищене спілкування.

Текст, відео, аудіо, файли після шифрування у відправника потрапляють на сервер, де зберігаються, поки одержувач не буде в змозі отримати дані. Після цього, в залежності від стратегії компанії - власника сервера, дані або знищуються, або зберігаються ще на якийсь термін.

Методи шифрування

Симетричне шифрування

Симетричні криптосистеми - спосіб шифрування, в якому для шифрування і розшифрування застосовується один і той же криптографічний ключ. До винаходу схеми асиметричного шифрування єдиним існуючим способом було симетричне шифрування. Ключ алгоритму повинен зберігатися в секреті обома сторонами. Алгоритм шифрування вибирається сторонами до початку обміну повідомленнями.

Асиметричне шифрування

Криптографічний система з відкритим ключем, або асиметричне шифрування - система шифрування і/або електронного підпису, при якій відкритий ключ передається по незахищеному каналу і використовується для перевірки електронного підпису і для шифрування повідомлення. Для генерації електронного ключа і для розшифровки повідомлення використовується закритий ключ..

Повноцінного end-to-end шифрування можна домогтися, використовуючи такі програми як PGP. За допомогою PGP користувачі можуть згенерувати пари відкритих / закритих ключів і використовувати їх для end-to-end з'єднання. Спосіб цей однак вимагає від користувачів досить широкої технічної обізнаності.

PGP

Шифрування в PGP реалізовано за принципом відкритого ключа. Загалом це виглядає наступним чином: ви створюєте файл, що складається з двох частин, одна частина називається приватний ключ, а друга публічний ключ. За допомогою публічного ключа ви можете тільки зашифрувати повідомлення тому, чий це ключ або перевірити підпис власника ключа, а за допомогою приватного ключа ви можете розшифрувати повідомлення зашифровані вашим публічним ключем.

Отже, вам необхідно згенерувати пару ключів. Ключі будуть захищені паролем, публічний ключ можна давати кому завгодно, а за приватним варто наглядати, хоч він і захищений паролем.

«Ну, якщо ці ключі так між собою пов'язані, то невже не можна з Громадської ключа витягнути всю необхідну інформацію для розшифровки будь-якого повідомлення? Адже це як грошова купюра, розірвана навпіл.»

Ви так говорите тільки лише тому, що знаєте, як виглядає ця купюра. Я пришлю вам половину фотографії, спробуйте відновити іншу.

GnuPG

GNU Privacy Guard - вільна програма для шифрування інформації і створення електронних цифрових підписів. Розроблено як альтернатива PGP і випущена під вільною ліцензією GNU General Public License.

Протокол Диффі Геллмана

Це метод обміну криптографічними ключами. Один з перших практичних прикладів обміну ключами, що дозволяє двом учасникам, що не мають жодних попередніх даних один про одного, отримати спільний секретний ключ із використанням незахищеного каналу зв'язку. Цей ключ можна використати для шифрування наступних сеансів зв'язку, що використовують шифр з симетричним ключем.

Сучасне використання

WhatsApp

Месенджер WhatsApp (зараз належить Facebook) вводить повне шифрування всіх своїх сервісів для всіх користувачів. Нововведення актуально для останньої версії програми. Це означає, що месенджер шифрує всі - повідомлення, телефонні дзвінки, фото,

відео, які передають користувачі один одному. І неважливо, спілкується 2 людини або 10 - шифрування в новій версії месенджера дійсно повне. Тепер навіть співробітники WhatsApp не зможуть розшифрувати дані, що передаються користувачами.

Telegram

Меседжер Telegram також має функцію end-to-end повідомлень. Проте шифрування працює лише після включення цієї функції, оскільки меседжер був створений, щоб стати не лише самим захищеним, але й швидким. Ідеєю даного продукту є захист інформації для усіх. Працює на власному протоколі шифрування MTProto.

Signal

Signal - простий меседжер, схожий на telegram і також має відкритий код. Додаток має доступ до вашої телефонної книги і може слати повідомлення людям, які є у вас в контактах, як і популярні меседжери.

Viber

Месенджер Viber з версії 6.0 ввів end-to-end шифрування в групових і приватних чатах для клієнтів сервісу, йдеться в описі з'явилася нова версія програми для Android. Представники сервісу повідомили, що шифрування можливе на всіх платформах - Android, iOS і в десктопних версіях програми. Також користувачі зможуть приховувати свої листування, захистивши їх від несанкціонованого доступу, додали вони.

Protonmail

У цього поштового сервісу є декілька особливостей. Розміщення компанія розробників у Швейцарії. Швейцарія доволі розвинена країна і не підлягає юрисдикції других країн таких, як Росія та США. Тому, навіть під тиском уряду іншої країни ваше листування не буде розсекречене.

Усі повідомлення зберігаються на сервері лише у зашифрованому вигляді. Так само як і в попередніх меседжерах, навіть при бажанні розробників розшифрувати листування буде не можливо.

Уразливості

Людина посередині

End-to-end шифрування гарантує, що дані передаються надійно між кінцевими користувачами. Але, замість того щоб намагатися порушити шифрування, зловмисник видає себе за одержувача, або відправника повідомлення.

Безпека кінцевих користувачів

Комп'ютер користувача може бути зламаний, щоб викрасти його данні, або криптографічний ключ, для читання повідомлень жертви.

Бекдори

Компанії також можуть вільно чи мимоволі ввести бекдор у їхньому програмному забезпеченні, які допомагають скидати узгодження ключів шифрування У 2013 році просочилася інформація, де Сноуден показав, що Skype мав бекдор, який дозволив Microsoft передати повідомлення своїх користувачів до АНБ , незважаючи на те , що ці повідомлення були зашифровані за допомогою end-to-end.

Література:

1. *iphones.ru/iNotes/595634*
2. *geektimes.ru/post/273884*
3. *spark.ru/startup/actor/blog/7905/end-to-end-shifrovanie-ono-togo-stoit*
4. *swissinfo.ch/rus/видео_что-такое-end-to-end-шифрование--i-/42288308*
5. *en.wikipedia.org/wiki/End-to-end_encryption*

Свердлюк Богдан Ігорович

Государственный университет телекоммуникаций

Факультет Телекоммуникаций

г. Киев

OFDM

Что это за зверь такой, ортогональное частотное разделение каналов с мультиплексированием?Если вы не знакомы с этим понятием, или хотите освежить свою пам'ять, добро пожаловать!

WTF?

Изучая теорию технологий беспроводных сетей, или сетей сотовой связи, неизбежно, так или иначе, можно столкнуться с такой аббревиатурой, как OFDM. Обратившись к википедии, мы обнаружим там следующее: "OFDM мультиплексирование с ортогональным частотным разделением каналов, является цифровой схемой модуляции, которая…

Думаю, после прочтения данного объяснения для большинства тема OFDM как была непонятной, так ей и осталась.

Но на данном этапе попрошу запомнить, что прежде всего OFDM – метод цифровой модуляции

Как работает?

Для лучшего понимания данной модуляции приведу пример. Представьте, что нам надо передать из одного пункта в другой стеклянный стекло. Для этого в нашем распоряжении есть некоторый ресурс, допустим 4 тележки (в случае передачи информации в качестве ресурса можно было бы считать доступный для передачи диапазон частот). В случае OFDM мы разбираем наше стекло на некоторое определенное количество частей, для примера пусть их будет 4. Далее каждая тележка перевозит свою часть посылки, при этом тележки катятся одновременно параллельно друг другу. Допустим на пути у нас встречается одна преграда в виде камня (в случае передачи информации – узкополосная помеха). Одна из тележек наезжает на камень, соответственно одна из частей посылки не доходит до пункта приема. Однако большее количество частей стекла все-таки было корректно получено, поэтому с помощью интуиции и волшебства (помехоустойчивого кодирования), есть шанс восстановить недостающую в результате падения одной тележки часть посылки. Как бы все было, не применяя OFDM? При традиционном подходе для наискорейшей передачи всей посылки мы также задействуем все доступные ресурсы, но будем транспортировать стекло целиком на всех 4 тележках (используем высокоскоростной метод модуляции, занимающий всю полосу канала). Допустим, на пути у нас также встречается одна преграда в виде камня. В результате одна из тележек наезжает на камень, стекло падает и разбивается вдребезги. Восстановить такое стекло не представляется возможным, поскольку алгоритм сборки неизвестен. Одной из особенностью OFDM является то, что все тележки могут двигаться параллельно практически вплотную и при этом не мешать друг другу. При передаче информации роль тележек выполняют поднесущие сигналы, т.е. множество несущих колебаний.

Подробнее

Основная концепция OFDM - это ортогональность поднесущих. Так как носителями являются волны вида синус/косинус, мы знаем, что площадь под одним периодом волны синуса или косинуса равна нулю. OFDM является частным случаем FDM. Идея метода OFDM в распараллеливании передаваемого сигнала на N отдельных низкоскоростных подпотоков с большой длительностью передаваемых символов. Каждый подпоток модулируется и передаётся на своей ортогональной поднесущей. Для повышения устойчивости сигнала к разбросу задержки в каждой поднесущей вводится защитный интервалTg (за счёт уменьшения длительности символаOFDM)**.** Защитный интервал является избыточной информацией и в этом смысле снижает полезную скорость передачи, но именно она служит защитой от возникновения межсимвольной интерференции. Межсимвольная интерференция это форма искажения сигнала, которая вызвана воздействием одного символа на другой. В следствие этого эффекта беспроводной сигнал от передатчика достигает приемника через несколько разных путей. Причины этого

отражения (например от зданий) — рефракция (преломление при прохождению через кроны деревьев) и атмосферные эффекты. Еще одним преимуществом является устойчивость к частотно-зависимому затуханию. Такой тип затухания может оказывать очень негативное влияние при многолучевом распространении сигнала, особенно если источник и приемник не находятся в прямой видимости.

Где применимо?

Используемый в сетях связи, таких как WiMAX и LTE, OFDMA обеспечивает воздушные интерфейсы, превосходящие CDMA и TDMA. OFDM используется в ряде других включая DVB и DAB.

Выводы:

OFDM - это форма передачи, которая использует большое количество близко расположенных несущих, которые модулируются данными с низкой скоростью. Обычно эти сигналы мешают друг другу, но, поскольку сигналы ортогональны друг другу, взаимных помех нет. Это достигается за счет того, что интервал несущей равен обратному периоду символа. Это означает, что, когда сигналы демодулируются, они будут иметь целые числа циклов в периоде символа, а их сумма будет равна нулю - другими словами, нет вклада в помехи. Передаваемые данные разбиваются на все несущие, и это означает, что с использованием методов коррекции ошибок, если некоторые из несущих теряются из-за эффектов с несколькими путями, данные могут быть восстановлены.

Литература:

1. itu.int
2. habr.com/company/yota/blog/119319/
3. artizanetworks.com/resources/tutorials/ofdma.html

Каграманова Юлия Константиновна
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
г. Киев

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ

Здесь мы рассмотрим основные принципы и методы надёжной и эффективной передачи данных между двумя машинами, соединёнными каналом. Под каналом следует понимать любую физическую среду передачи данных. Посредством этой физической среды нужно научиться передавать биты так, чтобы они безошибочно принимались получателем точно в той последовательности, в какой они были переданы.

На уровне канала данных решается ряд проблем, присущих только этому уровню:

- реализация сервиса для сетевого уровня,
- разбиение потока бит на кадры,
- управление потоком кадров,
- обработка ошибок передачи.

Основная задача канального уровня — обеспечить сервис сетевому уровню, а это значит помочь передать данные с сетевого уровня одной машины на сетевой уровень другой машины.

Сервис, создаваемый канальным уровнем для сетевого, опирается на сервис, создаваемый физическим уровнем. На физическом уровне протекают потоки битов. Значение посланного бита не обязательно равно принятому, и количество посланных битов не обязательно равно количеству принятых. Всё это требует специальных усилий на канальном уровне по обнаружению и исправлению ошибок. Типичный подход к решению этой проблемы — разбиение потока битов на кадры и подсчёт контрольной суммы для каждого кадра при посылке данных.

Контрольная сумма — это, в общем смысле, функция от содержательной части кадра (слова длины {\displaystyle m} m), область значений которой — слова фиксированной длины {\displaystyle r} r. Эти r бит добавляются обычно в конец кадра. При приёме

контрольная сумма вычисляется заново и сравнивается с той, что хранится в кадре. Если они различаются, то это признак ошибки передачи. Канальный уровень должен принять меры к исправлению ошибки, например, сбросить плохой кадр, послать сообщение об ошибке тому, кто прислал этот кадр. Разбиение потока битов на кадры — задача не простая. Один из способов — делать временную паузу между битами разных кадров. Однако, в сети, где нет единого таймера, нет гарантии, что эта пауза сохранится или, наоборот, не появятся новые. Так как временные методы ненадёжны, то применяются другие. Здесь мы рассмотрим три основных:

- счетчик символов;
- вставка специальных стартовых и конечных символов или последовательностей бит;
- специальная кодировка на физическом уровне.

Первый метод очевиден. В начале каждого кадра указывается сколько символов в кадре. При приёме число принятых символов подсчитывается опять. Однако, этот метод имеет существенный недостаток — счётчик символов может быть искажён при передаче. Тогда принимающая сторона не сможет обнаружить границы кадра. Даже обнаружив несовпадение контрольных сумм, принимающая сторона не сможет сообщить передающей какой кадр надо переслать, сколько символов пропало. Этот метод ныне используется редко.

Второй метод построен на вставке специальных символов. Обычно для этого используют управляющие последовательности. Но нужно избегать появления этих комбинаций внутри самого тела кадра. Это осуществляется дублированием комбинаций, встречающихся внутри тела кадра, и удаление дублей после получения кадра. Недостатком этого метода является зависимость от кодировки (кодозависимость). Очевидный кодонезависимый метод — управляющие последовательности должны быть бит-ориентированными. В частности, в протоколе каждый кадр начинается и заканчивается со специального флаг-байта: 01111110. Посылающая сторона, встретив последовательно 5 единиц внутри тела кадра, обязательно вставит 0. Принимающая сторона, приняв 5 последовательных единиц обязательно удалит следующий за ними 0, если таковой будет. Это называется bit-stuffing. Если принято шесть и за ними следует ноль, то это управляющий сигнал: начало или конец кадра, а в случае, когда подряд идут более шести единиц, — сигнал ожидания или аварийного завершения. Таким образом, кадр легко может быть распознан по флаг-байту. Если граница очередного кадра по какой-то причине была потеряна, то все что надо делать — ловить ближайший флаг-байт. И наконец, последний метод используется там, где конкретизирована физическая среда. Например, в случае проводной связи для передачи одного бита используется два импульса. 1 кодируется как переход высокое-низкое, 0 — как низкое-высокое. Сочетания низкое-низкое или высокое-высокое не используются для передачи данных, и их используют для границ кадра. На практике используют, как правило, комбинацию этих методов. Например, счётчик символов с флаг-байтами. Тогда, если число символов в кадре соответствует кодировке границы кадра, кадр считается переданным правильно. Решив проблему разбиения на кадры, мы приходим к следующей проблеме:

как обеспечить, чтобы кадры, пройдя по физическому каналу с помехами, попадали на сетевой уровень по назначению, в надлежащей последовательности и в надлежащем виде?

Частичное решение этой проблемы осуществляется посредством введения обратной связи между отправителем и получателем в виде кадра подтверждения, а также специального кодирования, позволяющего обнаруживать или даже исправлять ошибки передачи конкретного кадра. Если кадр-подтверждение несет положительную информацию, то считается что переданные кадры прошли нормально, если там сообщение об ошибке, то переданные кадры надо передать заново. Однако, возможны случаи когда из-за ошибок в канале кадр исчезнет целиком. В этом случае получатель не будет реагировать никак, а отправитель будет сколь угодно долго ждать подтверждения. Для решения этой

проблемы на канальном уровне вводят таймеры. Когда передаётся очередной кадр, то одновременно устанавливается таймер на определённое время. Этого времени должно хватать на то, чтобы получатель получил кадр, а отправитель получил подтверждение. Если отправитель не получит подтверждение раньше, чем истечёт время, установленное на таймере то он будет считать, что кадр потерян и повторит его еще раз. Однако, если кадр-подтверждение был утерян, то вполне возможно, что один и тот же кадр получатель получит дважды. Как быть? Для решения этой проблемы каждому кадру присваивают порядковый номер. С помощью этого номера получатель может обнаружить дубли. Итак, таймеры, нумерация кадров, флаг-байты, кодирование и обратная связь — вот основные средства на канальном уровне, обеспечивающие надёжную доставку каждого кадра до сетевого уровня в единственном экземпляре. Но и с помощью этих средств невозможно достигнуть стопроцентной надёжности передачи. Другая важная проблема, которая решается на канальном уровне — управление потоком. Вполне может случиться, что отправитель будет слать кадры столь часто, что получатель не будет успевать их обрабатывать. Для борьбы с такими ситуациями вводят управления потоком. Это управление предполагает обратную связь между отправителем и получателем, которая позволяет им урегулировать такие ситуации.

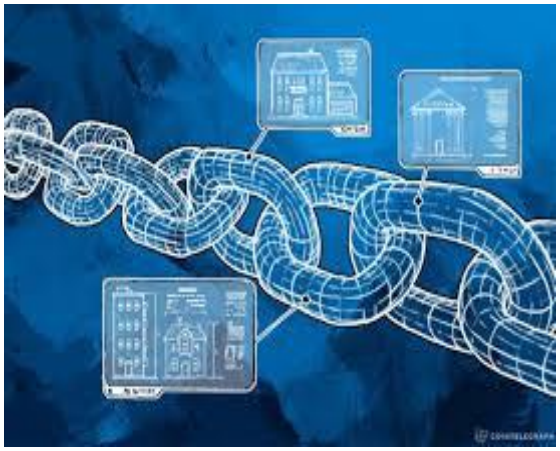
Литература:

1.https://ru.wikibooks.org/wiki
2.https://books.google.com.ua

Roman Bilyk
State University of Telecommunications
Faculty of Telecommunications
Kyiv

BLOCK CHAIN

Block chain - constructed according to certain rules, a continuous series of blocks containing information. Most often, copies of the chain of blocks are stored on a variety of different computers independently of each other.



Implementation in the Bitcoin system.

A transaction block is a special structure for recording a group of transactions in the Bitcoin system and similar ones. A transaction is considered complete and reliable ("confirmed") when its format and signatures are checked, and when the transaction itself is grouped together with several others and written into a special structure - a block. The contents of the blocks can be checked, since each block contains information about the previous block. All the blocks are lined up in a single chain, which contains information about all the operations that have been performed at any time in the database. The very first block in the chain - the primary block - is treated as a separate case, since it does not have a parent block. The block consists of a header and a list of transactions. The block

header includes its hash, hash of the previous block, hash of transactions and additional service information. In the Bitcoin system, the first transaction in the block always indicates the receipt of a commission, which will be a reward to the miner for the created block. Next, there is a list of transactions generated from the transaction queue, not yet recorded in the previous blocks. The selection criterion from the queue is set by the miner independently. It does not have to be a timeline. For example, only transactions with a high commission or with the participation of a given address list can be included. For transactions in the block, a tree hash is used, similar to the generation of a hash for a file in the BitTorrent protocol. Transactions, in addition to charging commission for creating a block, contain a reference to the transaction with the previous state of data within the parameter input (in the Bitcoin system, for example, a reference is made to the transaction where the consumable bitmicons were obtained). Operations to transfer commission for creating a block to the miner do not have "input" transactions, therefore this parameter can indicate any information. The created block will be accepted by other users if the numerical value of the hash of the header is equal to or less than the specified target number, the value of which is periodically adjusted. Since the result of hashing SHA-256 function is considered irreversible, at the moment there is no algorithm for obtaining the desired result, except random enumeration. If the hash does not satisfy the condition, the nonce parameter is changed in the header and the hash is recalculated. Typically, a large number of conversions is required. When a variant is found, the node sends the received block to other connected nodes that check the block. If there are no errors, then the block is considered added to the chain and the next block must include its hash. The value of the target number with which the hash is compared is adjusted in the Bitcoin system every 2016 blocks. It is planned that the whole network of the Bitcoin system should spend about 10 minutes on the generation of one block, about 2016 blocks - about two weeks. If 2016 blocks are formed faster, then the target decreases slightly and it becomes more difficult to reach, otherwise the target increases. The change in the complexity of the calculations does not affect the reliability of the Bitcoin network and is only required for the system to generate blocks at almost constant speed, independent of the computing power of network participants.

Chain of Blocks.

Blocks are simultaneously formed by a set of "miners". Satisfying blocks are sent to the network, including all replicas of the distributed database of blocks. Regular situations arise when several new blocks in different parts of a distributed network call the previous one the same block, that is, a chain of blocks can branch. Specifically or accidentally, it is possible to limit the retransmission of information about new blocks (for example, one of the chains can evolve within the local network). In this case, parallel build-up of different branches is possible. In each of the new blocks, there can be both identical transactions, and different ones, which are included only in one of them. When relaying blocks resumes, the miners start to consider the main chain taking into account the level of complexity of the hash and the length of the chain. If the complexity and length are equal, the preference is given to the chain whose end block appeared earlier. Transactions that have entered only the rejected branch (including payment of compensation), lose

the status of confirmed. If this is a transaction for bitcoins, it will be queued and then included in the next block. Transactions of receiving remuneration for creating cut-off blocks are not duplicated in another branch, that is, the "extra" bitcoins paid for the formation of cut-off blocks do not receive further confirmation and are "lost". Thus, the chain of blocks contains a possession history, which can be found, for example, on specialized sites. Block is formed as a continuously growing chain of blocks with records of all transactions. Copies of the database or its parts are simultaneously stored on a variety of computers and synchronized according to the formal rules for building a chain of blocks. The information in the blocks is not encrypted and is available in clear form, but the absence of changes is certified cryptographically through hash chains (digital signature element). He database publicly stores, in an unencrypted form, information about all transactions signed using asymmetric encryption. To avoid multiple waste of the same amount, timestamps realized by splitting the database into a chain of special blocks are used, each of which, among other things, contains the hash of the previous block and its serial number. Each new block carries out confirmation of transactions, information about which contains and additional confirmation of transactions in all previous blocks of the chain. Changing the information in a block that is already in the chain is not practical, since in this case it would be necessary to edit the information in all subsequent blocks. Thanks to this successful double-spending attack (re-spending previously expended funds) in practice is extremely unlikely. Most often, an intentional change in information in any copy of the database or even in a fairly large number of copies will not be recognized as true, as it will not comply with the rules. Some changes can be made if they are included in all copies of the database (for example, deleting several last blocks due to an error in their formation). To more clearly explain the mechanism of the payment system, Satoshi Nakamoto introduced the concept of "digital coin", defining it as a chain of digital signatures. Unlike the standardized denominations of conventional coins, each "digital coin" has its own denomination. Each bit-address can match any number of "digital coins". With the help of transactions, they can be divided and merged, while the total amount of their denominations minus the commission remains.

Literature:

https://blockgeeks.com/guides/what-is-blockchain-technology/
https://en.wikipedia.org/wiki/Blockchain

Yevhen Pendiur
State University of Telecommunications
Faculty of Telecommunications
Kyiv

IPTV

IP-TV (IPTV - Internet Protocol Television) is commonly referred to as the technology of digital multiprogramming interactive television broadcasting on the Internet using packet video data transmission over IP-protocol (Video over IP) from operator equipment to subscriber equipment.

Side view

In practice this is realized in the following way: the IPTV operator equipment is transmitted, and the user equipment receives streaming video. The term "streaming video" embraces the technology of compression, reduction and buffering of video data, which provide real-time video transmission via the Internet. The main feature of streaming video is that the user does not have to wait for the file to be downloaded in order to start watching it. Streaming video information is sent continuously, in the form of a sequence of IP packets, decoded by subscriber units and displayed on screens as it is received by the equipment. IPTV is a platform that is created and controlled by the provider of telecommunications structures. The consumer interacts directly with the operator. In this sense, the IPTV service operator is almost no different from existing

cable television operators. The entire infrastructure of such a network belongs to the operator and is inaccessible from the Internet. Devices connected to this network are monitored by the operator.

Equipment

To view the programs on IPTV (streaming video) networks, a special set-top box is used, in modern terminology - Set top Box (STB), which is connected to the operator's network (broadcast medium) on one side, and on the other hand it has a connection to a TV or computer . The STB subscriber unit decodes the video data and outputs the decrypted video to the TV screen.

The components of the whole

The IPTV complex as a rule includes the following components:

- complex and service management system or IPTV Middleware - middleware;
- a system of receiving and processing content;
- content protection system;
- system of video servers;
- system of quality control of flows and client equipment.

The functioning of IPTV systems is based on the following protocols:

- UDP - for streaming video.
- HTTP - for the organization of user services.
- RTSP - for managing broadcast streams.
- RTP - for streaming video.
- IGMP - for controlling broadcast streams.

Client part

In addition to its main purpose - television broadcasting, IPTV systems can include a number of additional services, such as video telephony, access to information portals of the operator and to the Internet, network games. In IPTV systems, it is possible to use two or more audio channels within a single video, for example, in Russian and English. As an advantage of IPTV, analogue and cable television can be called higher quality picture and sound: up to HD (high resolution - English High Definition) and 5.1 sound. But the main difference from the services provided by cable or terrestrial television is interactivity, that is, an opportunity for the subscriber to choose and change the composition of services and, if desired, order an additional service, for example, an additional paid viewing of the film.

Литература:

1.https://ru.wikipedia.org/wiki/IPTV
2.https://ku.net.ua/iptv/
3.https://pomogaemkompu.temaretik.com/693248816453781802/chto-takoe-iptv-chto-takoe-iptv-v-routere-instruktsiya-po-nastrojke-iptv/

Chernega Vladyslav
State University of Telecommunications
Faculty of Telecommunications
Kyiv

4G ETHERNE

In the field of mobile communications, a "generation" generally refers to a change in the fundamental nature of the service, non-backwards-compatible transmission technology, higher peak bit rates, new frequency bands, wider channel frequency bandwidth in Hertz, and higher capacity for many simultaneous data transfers (higher system spectral efficiency in bit/second/Hertz/site). New mobile generations have appeared about every ten years since the first move from 1981 analog (1G) to digital (2G) transmission in 1992. This was followed, in 2001, by 3G multi-media support, spread spectrum transmission and, at least, 200 kbit/s peak bit rate, in 2011/2012 to be followed by "real" 4G, which refers to all-Internet

Protocol (IP) packet-switched networks giving mobile ultra-broadband (gigabit speed) access. While the ITU has adopted recommendations for technologies that would be used for future global communications, they do not actually perform the standardization or development work themselves, instead relying on the work of other standard bodies such as IEEE, The Wi MAX Forum, and 3GPP. The fastest 3G-based standard in the UMTS family is the HSPA+ standard, which is commercially available since 2009 and offers 28 Mbit/s downstream (22 Mbit/s upstream) without MIMO, i.e. only with one antenna, and in 2011 accelerated up to 42 Mbit/s peak bit rate downstream using either DC-HSPA+ (simultaneous use of two 5 MHz UMTS carriers)[3] or 2x2 MIMO. In theory speeds up to 672 Mbit/s are possible, but have not been deployed yet. The fastest 3G-based standard in the CDMA2000 family is the EV-DO Rev. B, which is available since 2010 and offers 15.67 Mbit/s downstream. This article refers to 4G using IMT-Advanced (International Mobile Telecommunications Advanced), as defined by ITU-R. An IMT-Advanced cellular system must fulfill the following requirements:
Be based on an all-IP packet switched network.

Have peak data rates of up to approximately 100 Mbit/s for high mobility such as mobile access and up to approximately 1 Gbit/s for low mobility such as nomadic/local wireless access. Be able to dynamically share and use the network resources to support more simultaneous users per cell. Use scalable channel bandwidths of 5–20 MHz, optionally up to 40 MHz. Rumney, Moray (September 2008). "IMT-Advanced: 4G Wireless Takes Shape in an Olympic Year"(PDF). Agilent Measurement Journal. Archived from the original (PDF) on January 17, 2016. Have peak link spectral efficiency of 15-bit/s/Hz in the downlink, and 6.75-bit/s/Hz in the up link (meaning that 1 Gbit/s in the downlink should be possible over less than 67 MHz bandwidth). System spectral efficiency is, in indoor cases, 3-bit/s/Hz/cell for downlink and 2.25-bit/s/Hz/cell for up link. Smooth handovers across heterogeneous networks. 4G-networks provide subscribers with broadband access to the Internet - this means that more people can use the network without "subsidence" of the access speed. For example, at a stadium during a match due to a large number of connections, the 3G network operates either very slowly, or completely disconnected. 4G-network must cope with such loads

In September 2009, the technology proposals were submitted to the International Telecommunication Union (ITU) as 4G candidates. Basically all proposals are based on two technologies.:

- LTE Advanced standardized by the 3GPP
- 802.16m standardized by the IEEE

Implementations of Mobile WiMAX and first-release LTE are largely considered a stopgap solution that will offer a considerable boost until WiMAX 2 (based on the 802.16m spec) and LTE Advanced are deployed. The latter's standard versions were ratified in spring 2011, but are still far from being implemented. The first set of 3GPP requirements on LTE Advanced was approved in June 2008. LTE Advanced was to be standardized in 2010 as part of Release 10 of the 3GPP specification. LTE Advanced will be based on the existing LTE specification Release 10 and will not be defined as a new specification series. A summary of the technologies that have been studied as the basis for LTE Advanced is included in a technical report. Some sources consider first-release LTE and Mobile WiMAX implementations as pre-4G or near-4G, as they do not fully comply with the planned requirements of 1 Gbit/s for stationary reception and 100 Mbit/s for mobile. Confusion has been caused by some mobile carriers who have launched products advertised as 4G but which according to some sources are pre-4G versions, commonly referred to as '3.9G', which do not follow the ITU-R defined principles for 4G standards, but today can be called 4G according to ITU-R. Vodafone NL for example, advertised LTE as '4G', while advertising now LTE Advanced as their '4G+' service which actually is (True) 4G. A common argument for branding 3.9G systems as new-generation is that they use different frequency bands from 3G technologies ; that they are based on a new radio-interface paradigm ; and that the standards are not backwards compatible

with 3G, whilst some of the standards are forwards compatible with IMT-2000 compliant versions of the same standards.

Literature:
1.https://en.wikipedia.org/wiki/4G
2.http://gordonua.com/publications/4g-svyaz-v-ukraine-chto-eto-takoe-i-kogda-zarabotaet-196056.html

Karbovskiy Alexey
State University of Telecommunications
Faculty of Telecommunications
Kyiv

THE NEW G.FAST COMMUNICATION TECHNOLOGY - "WIRELESS + COPPER"

Not every densely populated urban area has an economically (or physically) feasible possibility of laying a fiber optic cable before entering the house (using the "copper" G.fast data transmission technology), and everyone wants broadband Internet access!

At the same time, the "obvious" decision to replace the cable optical channel with a broadband radio channel has also been "prohibitively expensive" up to now. And two Israeli companies - Sckipio Technologies and Siklu - created a combined "wireless-copper" communication technology, which they demonstrated for the first time at the recent MWC-2015 exhibition in Barcelona.

Sckipio Technologies, which manufactures G.fast equipment, has ensured its compatibility with the millimeter-wave ultra-wideband transceiver (70-90 GHz) manufactured by Siklu. This quite economical solution provides office and home users with a communication channel up to 5 km long with a bandwidth of about 2 Gb / s. For the organization of the wireless channel, in addition to transceivers, narrow-directional antennas (developed by Siklu) are installed on the roofs of the building of the telecommunications operator and consumers.

Brand-name developments of the G.fast project

Operators in various regions of the world are looking for cost-effective ways to get 100 Mbps throughput and more in line with national broadband access plans (BBA). Simultaneously, to solve this problem, they choose products with minimal consumption.

Many operators are implementing FTTH solutions "Fiber to the Home", based on scenarios of passive optical networks or active Ethernet. These scenarios, which virtually eliminate restrictions on the bandwidth of the access network, are very expensive and not all operators can afford. There are other limitations.

It is known, for example, that the FTTH network begins to be profitable at a coverage factor (30 ... 50)%, and the implementation time is on average 10 years. So, Verizon - the main "introducer" FTTH in 16 US states, started work on the deployment of this technology in 2004, has not yet completed it.

Particularly difficult is the last section of the FTTH network with a length of 200 meters or less, associated with work inside buildings.

Therefore, the more popular are the cheaper and quicker FTTx solutions: Fiber-to-the-Node (FTTN), Fiber-to-the-Cabinet (FTTC) and Fiber-to-the-Building or Basement (FTTB).

However, the latest technologies also do not fully meet modern requirements. So, they require their own power source, are not economical and cumbersome.

Three key requirements form the basis of the G.fast project

1. If you can not extend the fiber directly to the user's location, you should transfer the ONT optical network device from the user's room to the distributed point (dp) nearest to it.
2. The ONT must be powered remotely from the user equipment.
3. The ONT should be compact and placed almost anywhere.

Naturally, such a long time for the development of the project does not seem to everyone to be optimal. There appeared approximately simultaneously two firm projects practically realizing the key requirements of G.fast.

One of them, Fiber To The Distributed Point (FTTdp), was implemented jointly by Lantiq and Alpha Telecommunications, which developed a new technology, where ONT is the interface node of the optical and copper access line (FTTdp cabinet). This node has a capacity of up to 16 copper lines, consumes no more than 10W and is powered remotely from the user's DSL modem through the existing subscriber line (the so-called reverse power or backpowering power).

The bandwidth of the access network, close to 1 GHz, is expected to be achieved in this project due to improvements in VDSL2 technology, including vectoring, bonding and phantom mode.

Another project is called Ultra Broadband Ethernet - Ultra Broadband Ethernet (UBE) and was proposed by Adtran Inc. In practice, the UBE project is based on G.fast requirements.

The essential difference between this project and the FTTdp project is the use of Ethernet technology instead of DSL. The UBE unit, acting as a node that matches the electrical and optical sections of the access line, is housed in a small-sized casing and contains two key elements:

1. UBE ONT, which converts the optical signal into an electrical signal for 8 ... 16 users.
2. Media Adapter, which matches the electrical signal UBE ONT with the copper section of the access line and through which power is supplied to UBE ONT

***References**:*

1. http://www.lessons-tva.info/edu/tss_tmm_tech/network_tech.html
2. https://professionali.ru/Soobschestva/telekommunikacii/novaja-tehnologija-svjazi--besprovodkamed/
3. https://en.wikipedia.org/wiki/G_fast

Hnatishin Igor
State University of Telecommunications
Faculty of Telecommunications
Kyiv

GREEN TELECOMMUNICATIONS

In work to implement the concepts of green wireless communications, the use of hybrid technologies in the millimeter wave band (MMD) is proposed: optoelectronic methods for the formation of signals and antenna patterns, hybrid network topologies. It is shown that in order to increase the energy efficiency index of MMD networks, new approaches to the modeling of losses and the energy budget of wireless communications are needed, which should be based on the analysis of noise and fundamental physical patterns of propagation and emission of MMD waves.

Development of modern telecommunication communication networks is directed to on an increase the carrying capacity of network and grant of wide spectrum of services : the internet of things, system of safety, videosupervision, sensory systems, television of superhigh clearness (UHD), 3d videos etc. Universal application of such services is included in conception of development of off-wire networks 5g and next generations . Large attention is spared to the increase of spectral efficiency and expansion of radio frequency spectral resource. However, here appear problem of high energy consumption, electromagnetic compatibility (electromagnetic contamination of environment of transmission) and complication of the systems. Most optimizations of off-wire networks on a carrying capacity and spectral efficiency are not energyeffective.

New conceptions of green telecommunications are directed to on support high energy efficiency, reduction of electromagnetic contamination and decline of complication of the systems, for example, such conceptions as joint work of the base stations and plural access with a division at times (TRDMA) as a new chart of access to the off-wire broadbands, and also study of their fundamental theoretical limits

For realization of conceptions of green off-wire telecommunications of millimetric range the use of next hybrid technologies is assumed: optronic methods of forming of radio signals of millimetric range; optronic methods of forming of diagrams of orientation of phase arrays; hybrid to the topology of fiber-aethereal (eng of Radio over Fiber, RoF) and heterogeneous networks (eng of Heterogenic Networks; HetNet), stratospheric communication networks. For the systems of

millimetric range with Gigabit speeds of information transfer a stripe is assumed for one channel to 10 gigacycle with instantly signal processing, that requires the optronic methods of treatment of radio signals.

Literature:

1. *Heejung Yu, Howon Lee, Hongbeom Jeon, "What is 5G? Emerging 5G Mobile Services and Network Requirements," Sustainability, vol. 9, no. 10, 1814, Oct. 2017/*

Rivniachok Daria
State University of Telecommunications
Faculty of Telecommunications
Kyiv

INTERNET OF THINGS CHANGES THE WORLD

Trend of the Internet of Things is gaining much popularity. Smart toasters, smart houses, connected rectal thermometers and dog fitness collars are just some of the everyday items that are connected to the Internet as part of the Internet of Things (IoT). In the broadest sense, the term IoT covers everything related to the Internet, but it is increasingly used to identify objects that "talk" to each other. And what is a smart Internet of things?

How does Internet of Things affect the lives of ordinary citizens?

In people's lives there will be less space for domestic problems, and hence more time will be spent on families, creativity, hobbies. Connected devices on the Internet will also give people more opportunities for rational resource management. Already today, they help to optimally spend heat, water, light and save on payment of utilities.

For today the Internet of things is used in such fields as: manufacture(supply chain), energetics(objects of oil and gas industry,utilities and intelligent power system), transport(aviation, public transport, marine vessels, car roads, cars)

It should be noted that not only the lives of individuals, but the whole industry as a whole. Mobile operators will gradually change their business models from network providers to "smart" service providers and applications.

Is the Internet safe for things?

Of course, there are risks. The main one is security. Experts say that up to 80% of devices will be exposed externally In the industrial Internet of industry, the problem will be resolved by rigid rules and regulations, as well as by special security protocols. For critical devices, as already mentioned, absolute reliability of the network will be necessary, since the slightest failure can lead to injury or death of people.

What technologies are not enough to make internet things a reality today?

In order to implement many IoT scenarios, 5G networks need to be implemented. Networks of the fifth generation will allow to reduce delays, simultaneously maintain a huge number of connections, extend the service of "smart" devices up to 10 years, and also achieve incredible by the current rates of mobile data transmission.

The 5G feature is that within the same network, the work of applications and devices with a wide range of characteristics will be supported at the same time. As they say, from each one according to his abilities, to everyone - according to needs! This is achieved by segmenting the network into fragments, each of which is designed for specific needs.

The appearance of the Internet of things is a rather anticipated step, because laziness is the engine of progress.

Literature:

1.*https://tvrain.ru/articles/internet_veschej-413220/*
2.*https://techtoday.in.ua/news/5g-dali-start-z-yavivsya-ofitsiyniy-standart-86545.html*
3.*http://www.wired.co.uk/*

Pylypenko Mariya
State University of Telecommunications
Faculty of Telecommunications
Kyiv

UNMANNED REPEATER. REALITY AND FUTURE

Project Loon is a pilot project by Google to launch giant balloons into the air that will run in the lower layers of the stratosphere (at a height of 20 kilometers) and distribute wireless Internet.

Aerostats were chosen by Google for the reason that it is the easiest and cheapest way to deploy a wireless network. Instead of creating complex infrastructure and laying wires through mountains, jungles and other inaccessible corners of the Earth, this way you can connect 2/3 of the world's population, who now do not have access to the Internet.

High speed internet is transmitted up to the nearest balloon from our telecommunications partner on the ground, relayed across the balloon network, and then back down to users on the ground. We have demonstrated data transmission between balloons over 100 km apart in the stratosphere and back down to people on the ground with connection speeds of up to 10 Mbps, directly to their LTE phones.

They want to launch and maintain a fleet of balloons to provide on-site access to the Internet, and our rescue teams can safely and consistently launch a new bullet every 30 minutes. Since the start of the project, we have already traveled more than 25 million test flights - with one of our record air balloons, preserved for 190 days in the upper stratosphere.

The Project Loon team tracks the location of every balloon using GPS, coordinating directly with the local air traffic control to bring each one safely to ground targeting sparsely populated areas. When a balloon is ready to be taken out of service, the lift gas keeping the balloon aloft is released and the parachute deploys automatically to bring the balloon to the ground in a controlled descent. Our recovery teams then collect the equipment for reuse and recycling.

Literature:

1. *https://www.google.com.ua/amp/s/hitech.vesti.ru/amp/article/621823*
2. *https://x.company/loon/*

Mikulyak Svitlana
State University of Telecommunications
Faculty of Telecommunications
Kyiv

THE WORLD'S FASTEST HIGH-SPEED LINE

Using the Internet is an integral part of our lives. The amount of information is increasing day by day and therefore the network must meet these requirements. Speed is a major indicator of the global network. Most competing companies are tackling this issue in terms of speed improvements. One of these is the largest telecommunications company in France - Alcatel Lucent.

The 450-km long fiber-optic line connected two cities: Paris and Lyon. Thanks to the new telecommunications system, access to the network in the homes of users of France will now be 4 times faster and more stable, according to local media. A new development, which received the commercial name of "photon engine" makes it possible to transmit data at a speed of 400 gigabits per second. This is an unprecedented global indicator.

The infrastructure was created by Alcatel Lucent, the largest telecommunications company in France, and Orange, which was formed from the national telecom company France Telecom, will provide the service. In France Telecom itself, it is announced that now the French users of the network will have new opportunities: they will be able to watch more movies and live broadcasts online, listen to music, communicate more actively in social networks and use the now popular

cloud technologies. At the same time, the price of Internet access will not increase, the operator promises. Earlier it was reported that Cuba got high-speed Internet, using the connection to the global network via fiber-optic cable.

Literature:

1.Internet and IT: 400 gigabits per second. Journal Correspondent, 2013. Access mode: https://korrespondent.net/business/web/1500626.html, free.

2.News Of France: The world's fastest high-speed communication line. Journal Euromag, 2013. Access mode: https://www.euromag.ru/france/29052.html, free.

Kolodiazhna Anastasia
State University of Telecommunications
Faculty of Telecommunications
Kyiv

WHAT IS TELECOMMUNICATION TECHNOLOGY?

Telecommunication, which can be considered as a science and practice of transmitting information by electromagnetic centres on the problems involved in transmitting large volumes of information over long distances without damaging loss due to noise and interference. The basic components of a modern digital telecommunications system must be capable of transmitting voice, data, radio, and television signals. Digital transmission packets are being employed in order to achieve high reliability. In fact, the cost of digital switching systems is much lower than the cost of analog systems.

Telecommunications, also known as telecom, is the exchange of information over significant distances by electronic means and refers to all types of voice, data and video transmission. It's a broad term that includes a wide range of information, which is being transmitted transmitting such as telephones, microwave communications, fiber optics, satellites, radio and television broadcasting, the internet and telegraphs.

Early telecommunication technologies included different kind of a visual signals and optical heliographs. Pre-modern telecommunications technologies also included some audio messages.

Electrical and electromagnetic telecommunication technologies include:

- telegraph,
- telephone, and teleprinter,
- networks,
- radio,
- microwave transmission,
- fiber optics, communications satellites and
- the Internet.

Telecommunications service providers

Telecommunications systems are being run by telecommunications service providers. These companies historically offered telephone and related services and now offer a variety of internet and WAN services.

In many countries, telecom service providers were primarily government owned and operated in the past times, today many of them have been privatized. The main Telecom Organisation today -International Telecommunication Union - is the United Nations agency that administers telecommunications and regulates broadcast, although most countries also have their own government agencies to set and enforce telecommunications guidelines. For example, in the United States, the Federal Communications Commission is the primary regulatory agency.

Maybe the most important role of telecommunications is fulfilling its most basic purpose of transmitting data. Modern telecom technology includes telephony and video conferencing, facsimile, broadcast and interactive television, instant messaging, email and data transmission. It

transmits and stores your intellectual property and it also comprises the means through which you connect to your partners, suppliers and customers. The technology allows your firm to gather, collate, analyze, share and act on information in a variety of ways that ultimately bear on your bottom line.

Literature:

1. *http://searchtelecom.techtarget.com/definition/telecommunications*
2. *https://www.britannica.com/technology/telecommunication*
3. *http://smallbusiness.chron.com/role-telecommunication-technology-firm-14094.html*

Rogovyy Sergiy
State University of Telecommunications
Faculty of Telecommunications
Kyiv

TELECOMMUNICATION

Telecommunication is a type of communication, a method of transmitting information using electromagnetic signals, for example, through a current through metal cables, radiation in the optical band (in the atmosphere or through a fiber optic cable), radiation in the radio range. The principle of telecommunication is based on the transformation of message signals (sound, text, optical information) into primary electrical signals. In turn, primary electrical signals are converted into secondary electric signals by means of a transmitter, the characteristics of which are in good agreement with the characteristics of the communication line. Further through the communication line, secondary signals are fed to the input of the receiver. In the receiver, the secondary signals are converted back to the message signals in the form of sound, optical or text information.

At the end of the XIX century, with the innovative discoveries of Nikola Tesla and Alexander Popov, the development of wireless communications began. Other pioneers in this field are Charles Whitstone and Samuel Morse (telegraph), Alexander Graham Bell (telephone), Edwin Armstrong and Lee de Forest (radio), John Baird, Vladimir Zvorykin, Semyon Kataev (television).

The amount of information transmitted through bilateral networks is constantly growing. Under the guidance of Martin Gilbert, scientists from the University of Southern California conducted research and analysis of the storage, processing and transmission of information for 1986-2007 [1]. In particular, it was revealed that the total reserves of data of all mankind were estimated at that time approximately 295 exabytes [1]. At present, digital storage of information dominates the analog, although until 2002, mankind has stored information mainly in analog form [1]. In 2007, about 1.9 zettabytes of information were transmitted by radio and television (equivalent to about 174 newspapers per day per person), and the personal communication of people reached about 65 exabytes (corresponding to each person's retelling about 6 newspapers per day)

Literature:

1. Англо-український тлумачний словник з обчислювальної техніки, Інтернету і програмування. – Вид. 1 – К.: Видавничий дім "СофтПрес", 2005. – 552 с.
2. Англо-український тлумачний словник з обчислювальної техніки, Інтернету і програмування. – Вид. 2 – К.: Видавничий дім "СофтПрес", 2006. – 824 с.
3. Бухаркина М.Ю. Телекоммуникации в образовании? Это реально// Распахнутая дверь в мир педагогических и информационных технологий. – М., 1994.
4. Бухаркина М.Ю. Учебные проекты: возможности Интернет. // Сборник докладов научно-практической конференции "Глобальные телекоммуникации в образовании". – М., 1996.

Galushchak Andriy,

Perekupko Mykhailo
State University of Telecommunications
Faculty of Telecommunications
Kyiv

ANALYSIS OF THE PECULIARITIES OF THE LOCATION IN NETWORKS OF MOBILE COMMUNICATION

With the development of the telecommunication industry, the development and implementation of new standards of communication and security, there is a need to provide accurate data on the location of subscriber stations to provide users of mobile networks of navigation services, assistance in the event of accidents, ensuring their safety, and also for operational use in the system. -search activities. This requires high accuracy of determining the geographic coordinates of subscriber stations and their unambiguous binding to a digital terrain map.

Existing positioning technologies in mobile networks give a big error in the positioning of the AS or require significant costs for their implementation. In this regard, most mobile operators in practice use the easiest and cheapest method of positioning based on identifying a cellular network (Cell-ID) in which the AU is located. This method allows you to determine the location of the AU with accuracy, which corresponds to the size of the cell, which is the wanted AU. This accuracy of positioning is not sufficient to provide users of mobile networks of navigation services, assistance in the event of accidents, ensuring their safety, as well as for use in the system of operational-search activities.

The measuring points of the bumping network are located in the positional areas of the base stations (BS) and have in their composition GSM-1800 receivers and antenna devices, which are receiving faded antenna arrays (FAR) with electronic control. The management and processing of the results of the operation of the bumping network is carried out in a special control panel that interacts with the controllers and the switching system of the mobile communication network.

The algorithms of work and procedures for the operation of the mobile network and positioning include the following steps:

Stage 1. Procedure for determining the mobile communications network sector in which the subscriber station is located.

Stage 2. Procedure for determining the list of measuring points, bearing the desired subscriber station.

Stage 3. Algorithm of the transition of the AS into the mode of operation in the standard GSM-1800.

Stage 4. Algorithm for the output of the subscriber station to the maximum transmission power.

Stage 5. Procedure for positioning the subscriber station using the equipment of the belt network.

Considered structure and procedures of functioning of the mobile communication network and positioning promote:

- unification of equipment in the IP and, as a consequence, reduction of its constructive complexity and cost;
- reduction of the signal load on the bell network;
- increasing the electromagnetic availability of the AU by means of the bell network;
- reduction of the "near-far" effect.

Literature:

1. Stepun A.N. Principles of construction and functioning of the superimposed downlinking network / AN Stepun // Natural and technical sciences. - 2011. - №2. - P. 363-375

2. Tikhvinsky, V.O. Management and quality of services in GPRS / UMTS networks EcoTrends, 2007

3. Thomas W. Electronic communication systems. M .: Technosphere, 2007. - 1360 p.

Zavoruev Dmitry
State University of Telecommunications

Faculty of Telecommunications
Kyiv

APPLICATION OF DECT STANDARD RADIO SYSTEMS FOR THE CORPORATE SECTOR

Even the most superficial study of the market for wireless communication systems gives reason to believe that DECT technology today occupies one of the leading places. According to most experts, the pace of development of the world market of DECT-devices is one of the highest. In Russia, a similar situation, however, with some lag. So, in 2005, the sales volume in the Russian market of DECT-devices amounted to about $ 600 million, which is more than 2 times higher than in the previous year. According to the Mobile Marketing Agency (AMM), on average, the annual sales of DECT-devices are increased by 2 - 2.5 times.

Why DECT?

Even the most superficial study of the market for wireless communication systems gives reason to believe that DECT technology today occupies one of the leading places. According to most experts, the pace of development of the world market of DECT-devices is one of the highest. In Russia, a similar situation, however, with some lag. So, in 2005, the sales volume in the Russian market of DECT-devices amounted to about $ 600 million, which is more than 2 times higher than in the previous year. According to the Mobile Marketing Agency (AMM), on average, the annual sales of DECT-devices are increased by 2 - 2.5 times.

Let's try to understand why corporate users prefer this technology.

Cellular communication systems, due to the high cost of subscriber traffic and the unregulated connection time, especially during busy hours, are not advisable to use as an office and technological connection, where a large number of calls take place and an important requirement is the speed of communication. Trunking communication systems are optimal for technological communication, for operative interaction of employees of special services, but are hardly convenient for intra-office communication, where high speech quality and full duplex are needed. In addition, these systems require large investments during the deployment phase, rather long reconciliations and registration in the radio-frequency services, as well as payment for the use of radio air.

Another significant factor is the rather high level of the power of the radiation from subscriber tubes - up to 2 W in cellular communication systems and up to 4 W in trunking communication systems. With adaptive power control, which occurs in most digital radio communication systems, power can be maximized indoors, especially in the lower floors of buildings. And in CHN activity of subscribers (and their irradiation) can reach 0,5 Earl and make 30 - 50% of working time.

Currently, broadband wireless broadband access technologies for Wi-Fi and WiMAX technologies are rapidly developing and are actively being introduced into the corporate sector, but in the overwhelming majority of these systems are fixed access systems oriented to high-speed data transmission. When deploying such systems, coordination with radio frequency services is required, and the cost of equipment, in particular WiMAX base stations, is on average $ 7,000. For the sake of fairness, it should be noted that the technical and functional characteristics of the system, developed on the basis of the IEEE 802.11x family standards and IEEE 802.1.

Literature:

1.http://www.3tel.ru/article_t_061211.html

Vasin Maksim
State University of Telecommunications
Faculty of Telecommunications

Kyiv

VIRTUAL PRIVATE NETWORK

VPN stands for "Virtual Private Network," which is a term used to describe a digital network within another physical computer network. VPNs are used to allow individuals access to protected information stored on a private network by connecting to that network using a public network. VPNs are not only used to provide an extra layer of security, but businesses can also be used by individuals to remotely access a protected network from any Internet connection.

VPNs can be either remote-access (connecting a computer to a network) or site-to-site (connecting two networks). In a corporate setting, remote-access VPNs allow employees to access their company's intranet from home or while travelling outside the office, and site-to-site VPNs allow employees in geographically disparate offices to share one cohesive virtual network. A VPN can also be used to interconnect two similar networks over a dissimilar middle network; for example, two IPv6 networks over an IPv4 network.

Therefore, many personal use VPN providers have been developing technologies to bypass the blocking of proxies.A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.Traditional VPNs are characterized by a point-to-point topology, and they do not tend to support or connect broadcast domains, so services such as Microsoft Windows NetBIOS may not be fully supported or work as they would on a local area network (LAN). Designers have developed VPN variants, such as Virtual Private LAN Service (VPLS), and Layer 2 Tunneling Protocols (L2TP), to overcome this limitation.

VPNs cannot make online connections completely anonymous, but they can usually increase privacy and security. To prevent disclosure of private information, VPNs typically allow only authenticated remote access using tunneling protocols and encryption techniques.

Enterprises generally use either an Internet Protocol security (IPsec) or Multiprotocol Label Switching (MPLS) VPN to connect their remote and mobile employees to data, apps, and other corporate resources. The terms “IPsec” and “MPLS” indicate the way each type of VPN transmits data. The primary differences between IPsec and MPLS are related to the networks they run over. IPsec connects sites using public Internet transport, which is made of interconnected networks run by different carriers. MPLS connects sites using a single carrier’s MPLS network. The carrier has management control of the network, including the ability to enforce quality-of-service policies on traffic flows. MPLS VPNs partition each customer’s traffic from the others to keep it private across the infrastructure.

VPNs work by sending data over tunneling protocols, which are designed to provide an extra layer of encryption and data protection. Tunneling protocols send information in one network protocol through another, providing a second level of security. Tunneling is a lot like sending an addressed package within another larger package through the mail: the person who receives the package at the first address mails the package within the initial package to the second address.

VPN systems may be classified by: The tunneling protocol used to tunnel the traffic, the tunnel's termination point location, e.g., on the customer edge or network-provider edge, the type of topology of connections, such as site-to-site or network-to-network, the levels of security provided, the OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity, the number of simultaneous connections

One major limitation of traditional VPNs is that they are point-to-point, and do not tend to support or connect broadcast domains. Therefore, communication, software, and networking, which are based on layer 2 and broadcast packets, such as NetBIOS used in Windows networking, may not be fully supported or work exactly as they would on a real LAN. Variants on VPN, such as Virtual Private LAN Service (VPLS), and layer 2 tunneling protocols, are designed to overcome this limitation.

Literature:
1.Nemeth UNIX System Administration Handbook_3ed
2.Tanenbaum & Wetherall Computer Networks
3.Olifer Computer networks. Principles, technologies, protocols 5th edition
4.James F. Kurous, Keith V. Ross Computer Networks

Avramenko Oleksiy
State University of Telecommunications
Faculty of Telecommunications
Kyiv

WHAT IS THE DIFFERENCE BETWEEN IT AND TELECOMMUNICATIONS?

This is a simple question that hinders many people. Also, one of the most popular issues on Quora. So, we are going to see what smart people say and finally shed the light on the main difference between IT and Telecommunications..

Definition

Starting with the definition, IT "I"nformation "T"echnology is an acronym to name the procedure of electronic control of information, programming/coding, PC system(hardware) operations, and other information administration. T also means information technology, including software Tech, web Tech, computer Tech, storage Tech, etc.

Telecommunications or media transmission is rather offered to a transmission of signs, signals, messages, compositions, pictures and sounds or knowledge of any nature by wire, radio, optical or other electromagnetic frameworks.

Telecommunication technologies or Information and Communications Technology (ICT) mean communication technology, including wireless access systems (for cell phone communication, satellite communication, etc).

So, there is something in between to combine these two IT+Telecommunications=(ICT)

What's behind

It's hard to imagine modern generation without telecommunication technologies. Sometimes, it's simply impossible. These technologies are so much imprinted into our concept of world and in our private lives that it is simply unrealistic to imagine our existence without them at least for a while. However, there are still people who do not even notice these important modern technologies or simply do not know any details about them. So let's try to figure out what's behind telecommunications definition and why telecommunications are so much-needed in the modern world. What is meant by the term telecommunications? It is simple: under telecommunications we imagine the whole complex of technical means that are intended to transmit information to any distance and its being successfully delivered and processed. This complex of technical equipment can contain: sounds, signals, text, other signs, images and much other stuff allowed by the local laws. All these means are transmitted through both wired and wireless channels, via optical fibers, radio and other electromagnetic systems. The system of technical means by which telecommunications is carried out is called a telecommunication network. The telecommunication network has one of the main characteristics of the entire technology in question: it provides an opportunity to obtain the necessary information or data to support the activities of any telecommunications participants or to meet the personal needs of users and many other things. So, as you see, every thing's simple. Less definitely means more! Feel free to comment, share and do not forget to come over to BSG any time you need cheep and speedy mass SMS messaging.

Literature:
1. *https://www.quora.com/What-is-the-difference-between-ICT-and-telecommunications*
2. *https://medium.com/bsg-sms/what-is-the-difference-between-it-and-telecommunications-c5d250436b3a*

Bogachova Karina

State University of Telecommunications
Faculty of Telecommunications
Kyiv

WHAT IS THE TELECOMMUNICATIONS SECTOR?

Telecommunications systems are generally run by telecommunications service providers, also known as communications service providers. Telecommunications devices include telephones, telegraph, radio, microwave communication arrangements, fiber optics, satellites and the Internet.

What is the telecommunications sector?

Telecommunications is communication using electronic equipment such as telephones, computer modems, satellites and fiber-optic cables.

Telecommunication systems include telecommunication cables from the subscriber to local switches (local lines), switching facilities that provide a communication connection with the subscriber, with lines or channels that transmit calls between the switches and, of course, the subscriber. In the period from the beginning to the middle of the 20th century, such innovations as telephone, electromechanical commutator systems, cables, repeaters, carrier systems, microwave equipment, and then in the industrialized regions of the world telecommunications systems began to spread. From the 1950s to 1984, new technologies continued to develop in this industry. For example, satellite and advanced cable systems, digital and fiber optic technologies and video telephony. The communications industry was completely computerized. All these modifications contributed to the spread of telecommunications systems across the world. In 1984, the monopoly of the American Telegraph and Telephone Corporation (AT & T) was destroyed by a court ruling in the United States. This event coincided with many major changes in the technology of the telecommunications industry itself. Until the 1980s, almost all countries believed that telecommunications services were public services and operate within a legislative framework that provided a monopoly position. Along with the growth of economic activity, the advent of new technologies led to the privatization of the telecommunications industry. This trend reached its culmination when AT & T lost its monopoly position, and the state regulation of the US telecommunications systems ceased. In some other countries, similar privatization processes are taking place. After 1984, as a result of technological progress, telecommunications systems have spread that can provide universal services to people around the world. This happens when telecommunication technologies are combined with other information technologies in related areas, such as electronics and data processing. The introduction of new technologies has had a different impact on employment in this industry. Undoubtedly, the level of employment has decreased, the tasks of the telecommunications industry workers have fundamentally changed, as well as the requirements for their qualifications and experience. Nevertheless, some believe that in the future there will be an increase in employment, and this will happen as a result of new business activity, stimulated by the reduction of state regulation, which will lead to the creation of new jobs requiring high qualification. From the professional point of view, work in the telecommunications industry can be divided into two categories: skilled workers and office workers. The first category includes specialists in connecting cables, installers, technicians for maintenance of complex equipment at external installations, in central offices and in studios. These positions require high qualifications, especially when working on new technological equipment. For example, they should all be well versed in the electrical, electronic and / or mechanical fields that arise when installing, operating and repairing telecommunications devices. Their preparation requires preliminary training and training directly at the workplace.

Literature:

1.Title: Telecommunications. Author: David LeGrande. Section: Section XVII. Services and Trade

German Vitalii

State University of Telecommunications
Faculty of Telecommunications
Kyiv

TOPOLOGY OF DATA TRANSMISSION NETWORKS

Telecommunications refers to the exchange of information by electronic and electrical means over a significant distance. A complete telecommunication arrangement is made up of two or more stations equipped with transmitter and receiver devices. A single co-arrangement of transmitters and receivers, called a transceiver, may also be used in many telecommunication stations.Telecommunications devices include telephones, telegraph, radio, microwave communication arrangements, fiber optics, satellites and the Internet.

The configuration of the network itself, more precisely, the sequence of connection of its objects is called topology. The main types here are:

Star. In this case, the server itself processes all data from the computers connected to it. All data between any workstations passes through the main node in the computer network along separate lines. The throughput in this case is determined by the power of the node itself. Topology "Star" is the fastest.

Ring. Here all workstations are connected among themselves in a circle. All messages in such a topological network circulate in a circle. In this case, it is possible to perform a ring request simultaneously to all stations. The more users, the longer the transfer of information. In this case, each such workstation must participate in the data movement. And if there is at least one failure, the whole process is paralyzed.

Tire. The transmission of information in the bus topological network is represented as a common trunk. It is to it that all workstations are connected. In this case, they can enter into work and among themselves. A feature of this type of network is the fact that its performance does not depend on the status of the stations (workers or not). They can be connected and disconnected at any time without disturbing network processes.

The principle of data transfer in peer-to-peer networks is based on the equality of all participants. In most cases, there may not be a dedicated server. That is why each node of the network can act as a client and the server itself. This organization allows you to keep working with any combination of available nodes.

During the organization and work, special requirements are imposed on the data transmission network. What does this include?

Security.
Reliability.
High performance.
Scalability.
Modernity.
Easy control.
Support for various types of traffic
Transparency.

Literature:

1) *http://www.sviaz-expo.ru/ru/articles/2016/peredacha-dannyh-v-setyah/*

Vadim Kovalchuk
State University of Telecommunications
Faculty of Telecommunications
Kyiv

IMPORTANCE OF DEVELOPMENT OF CONTROLLED TECHNOLOGIES OF THE WIRELLESS COMMUNICATION

In the modern world it is very difficult to imagine us without cellular communication, Wi-Fi technology, contactless data transmission and many other useful aspects of wireless communication. For example, Wi-Fi wireless technology is spreading very fast, especially noticeable in the area of home appliance – in TVs, stereos and other equipment that can be connected to each other and a personal computer, which is quite important. The Wi-Fi standard 802.1 that is currently being used to build informational wireless networks with a range of 300 m. A company that is one of the world's leading manufactures of equipment for local wireless networks of the Wi-Fi standard is Cisco. Another important feature of wireless technology is the wireless transmission network, which ensures the availability of information without being tied to a specific workplace, that is, you can, work anywhere and anytime. The development of wireless communication is accompanied by a continuous variable technology. The most urgent issues will be the speed and reliability of data transfer, especially at present, the continuous development of wireless networks and technology of the new generation. In real-time control systems, in mobile phones, smartphones and communicators, laptops and netbooks. This technology allows you to increase the speed and reliability of data transmission in real time systems. OFDM(Orthogonal Frequency Division Multiplexing Access) and SC-FDMA(Single Carrier FDMA) – Orthogonal Multifunction Multiplexing and Frequency Multiplexing with Single Carrier Frequency. Thanks to these radio access techniques along with QPSK quadrature phase manipulation of 16 QAM and 64 QAM. QAM (Quadrature Amplitude Modulation) is a technology for transmitting a digital information stream in the form of an analog signal. This is achieved by separating the carrier wave into two carrier equal frequencies shifted relative to each other by 90%, each of which is modulated by one for two or more discrete amplitude levels. 16 QAM is a 4x4 matrix in which each cell represents one of 15 possible binary combinations. The vertical and horizontal position of each point corresponds to the I and Q levels of the amplitude of the signal transmitted during one cycle 64 QAM is the 8x8 matrix, respectively. As LTE technology is one of the most promising, there are three main advantages that distinguish LTE from previous generations of communication; high speed data transmission, mass video capture and distribution of Internet products. High speed – this is a completely different level of comfort for the subscriber. Therefore, for everyone, there will be a significant advantage of LTE when using applications requiring high data rates. For example, when watching online videos or using online virtual reality apps or watching high-definition video.

Conclusion

Important advantages of LTE with lower-end networks is that the latter have been periodically confronted with delays and buffering, so, just a few seconds latency, but according to Ericsson, after waiting for 4 second, 10% of users refuse to watch the video, and another 40% closes the application after a 10 second delay. There are dozens of other dozens of well-known wireless technologies, but we are interested in technologies that the users rely on, so we are preparing for change in the near future and do not forget to follow the world of telecommunication.

Literature:

1. *Technologies and standards for building local wireless networks* http://stud.com.ua/20631/informatika/tehnologiyi_standarti_pobudovi_lokalnih_bezdrotovih_merezh
2. *Basics of QAM transmission* https://telcogroup.ru/files/materials-pdf/cab/QAM.pdf
3. *Applications of LTE technologies in real time systems* http://jrnl.nau.edu.ua/index.php/SBT/article/viewFile/5242/5784

Dmytro Malyshenko
State University of Telecommunications
Faculty of Telecommunications
Kyiv

LTE (LONG-TERM EVOLUTION)

4G (LTE) is the fourth generation mobile Internet, the successor to 3G and 2G. This is the standard for mobile ultra-fast data transfer for your devices - smartphones, tablets or modems. 4G-network provides data download speed up to 300 Mbit / s and transmission - up to 55 Mbit / s. There is no LTE in Ukraine. But there is LTE roaming in European countries. It was opened for its subscribers by the lifecell operator (which belongs to the Turkish company Turkcell). In addition to Turkey, LTE-roaming for lifecell subscribers is available in Austria, Belgium, Estonia, Germany, Poland and Russia. Soon they promise to launch LTE-roaming in France, Czech Republic, Bulgaria, Slovenia and Serbia. To use high-speed Internet in roaming in next-generation networks, lifecell subscribers need to exchange a SIM-card for USIM-card in one of the official stores of the company.

In Ukraine, the first tender was held for frequencies suitable for 4G-networks, in the range of 2600 MHz. Three participants - Kyivstar, Vodafone Ukraine and lifecell - announced their price offers and bought frequencies. Lifecell received 30 MHz at the beginning of the range, "Kyivstar" is the same 30 MHz, and Vodafone Ukraine, which initially claimed the first lot, received 20 MHz. Now time for operators to act. Under the terms of the tender, after five years in each region of Ukraine there should be at least one base station: for the development of the first region, the operator is given 6 months from the beginning of the validity of the license and plus two months for each subsequent region.

Today in Ukraine national operators operate in the following conventional frequency bands:

800 MHz - operator CDMA Intertelecom (formerly CDMA-Ukraine), PeopleNet (partial coverage)

900 MHz - GSM operators Vodafone, Kyivstar, Lifsell

1800 MHz - GSM operator Vodafone, Kyivstar, Lifsell

2100 MHz - UMTS / WCDMA operator TriMob

At all these frequencies you can build a network LTE 4G. The only question is the cost of costs, which can vary significantly when you choose different options.

LTE FDD and LTE TDD: what's the difference?

There are two kinds of LTE and the differences between them are quite significant. FDD - Frequency Division Duplex (frequency separation of the incoming and outgoing channel)

TDD - Time Division Duplex (time separation of the incoming and outgoing channel). Roughly speaking, FDD is a parallel LTE and TDD is a serial LTE. For example, with a channel width of 20 MHz in FDD LTE, part of the range (15 MHz) is given for downloading, and part (5 MHz) for uploading. Thus, the channels don't overlap in frequency, which allows working simultaneously and stably for loading and unloading data. In TDD LTE, all the same channel in 20 MHz is completely given both for downloading and for uploading, and the data is transferred to the one and the other side in turn, with priority still being downloaded. In general, FDD LTE is preferable, because it works faster and more stable.The next stage in the development of 4G LTE networks is the LTE-A (LTE-Advanced) standard. Some operators call this technology 4G + for marketing purposes, but this is fundamentally incorrect. In fact, LTE-Advanced is the real 4G. The data rates in the LTE-A network are significantly higher than the usual LTE. The main feature of LTE-Advanced is the aggregation of frequency bands. A LTE-A subscriber unit summarizes the data channels in different frequency bands available to the operator. For example, Megaphone, by combining several frequency bands in the 2600 MHz band, receives a channel at 40 MHz, which gives a speed in the LTE-Advanced network of 300 Mbps. But this is not the limit. If you add another 20 MHz from the 1800 MHz band, you get a 60 MHz channel (band 7 + band 3), which is 450 Mbps! In other matters, these are theoretical or bench velocities. In reality, they are certainly much smaller, but nevertheless, the wireless technology LTE-Advanced is quite close to wire speeds. It is worth noting that all operators can aggreate different channels in different frequency ranges if there are appropriate licenses and network infrastructure. The main task is to expand the frequency range. The wider it is, the higher the maximum speed, i.e. network bandwidth. But of course there must be a subscriber equipment supporting LTE-Advanced.

Literature:
1. http://trushenk.com/standart-4g-lte-v-ukraine.html
2. https://itc.ua/articles/chem-horoshi-seti-lte-i-chto-tormozit-zapusk-4g-v-ukraine/
3. http://kubaninternet.ru/chto-takoe-4g-lte.html

Oleksandr Novik
State University of Telecommunications
Faculty of Telecommunications
Kyiv

UNIVERSAL ZABBIX NETWORK MONITORING SYSTEM

Considered the telecommunication industry in the present, the analysis of modern telecommunication infrastructure. The principle of functioning of modern universal monitoring system of Zabbix networks is shown.

The telecommunication industry is undergoing significant transformations today, its speed is increasing every year, so a modern representative of the telecommunications market in its activity uses monitoring and control systems. At the same time, in the conditions of constant increase of the complexity of information and telecommunication systems, the reliability of the telecommunication network and the quality of the services provided are of particular importance. Modern telecommunication infrastructure is a complex network that includes telecommunication, server and software of different manufacturers, working in different standards and managing various software. The complexity and scale of the network infrastructure result in a high level of automated monitoring and management tools that should be used to ensure the robust operation of the network.

One of the best tools for solving this problem is the free Zabbix system, which consists of three basic components: a server for coordinating inspections, forming verification queries, and stacking statistics; agents for external party inspections; frontend for organization of system management.

Zabbix offers excellent reporting and visualization capabilities based on gathered data, making Zabbix the perfect tool for planning and scaling. A well-designed program can play an important role in monitoring IT infrastructure.

Thus, we can conclude that Zabbix is in vain used by a large number of companies that chose it for its ease of use, high fault tolerance, and reliability at extremely low cost of its use.

Literature:
1. *Zabbix Practical guide/ Andrea Dalle Wacque, 2017.- p. 15.*
2. *www.zabbix.com*
3. *Synopsis of lectures "Monitoring of Telecommunication Networks", State University of Telecommunications, 2017.*

Yurii Kovalets
Yaroslav Mykolaichuck
State University of Telecommunications
Faculty of Telecommunications
Kyiv

USAGE, STANDARDIZATION AND INITIAL STAGE OF DEVELOPMENT OF RFID TECHNOLOGY

The article describes the technology of automatic identification of RFID objects: its features and historical references. It also indicates the international standards developed by ISO and IEC defining RFID as part of the automatic identification technology

RFID (Radio Frequency Identification) is the technology for automatic identification of objects in which data stored in RFID tags is read or written through radio signals. The starting point for the development of this technology can be seen in the invention of Lev Termen in 1945 year device for overlaying audio information on radio waves. The feature of RFID-tag is their ability to overwrite

Classification of radios can be carried out by the power supply on the active, passive and semi-passive, depending on whether the label has a built-in power supply or not. You can meet this technology more often in retail outlets and checkpoints of organizations with restricted access but the true range of their use is much wider. It includes such industries as medicine, transport, agriculture and real-time localization systems.

Signaling between the reader and the tag is done in several different incompatible ways, depending on the frequency band used by the tag. Tags operating on LF and HF bands are, in terms of radio wavelength, very close to the reader antenna because they are only a small percentage of a wavelength away. In this near field region, the tag is closely coupled electrically with the transmitter in the reader.

The tag can modulate the field produced by the reader by changing the electrical loading the tag represents. By switching between lower and higher relative loads, the tag produces a change that the reader can detect. At UHF and higher frequencies, the tag is more than one radio wavelength away from the reader, requiring a different approach. The tag can backscatter a signal. Active tags may contain functionally separated transmitters and receivers, and the tag need not respond on a frequency related to the reader's interrogation signal.

International standards for RFID, as part of automatic identification technology, are developed and adopted by the international organization ISO in conjunction with IEC.

Preparation of projects (development) of standards is carried out in close cooperation with initiative organizations and companies.

Literature:

1. Lewan, Todd. Chip Implants Linked to Animal Tumors.- Washington Post. - 2007.- p.50.
2. RFID News Roundup. - New York.- 2018.- Available at:
3.http://www.rfidjournal.com/articles/view?17384

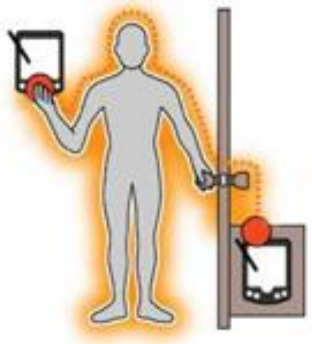
Димарчук Дмитрій Сергійович
Державний університет телекомунікацій
Факультет телекомунікацій
м.Київ

ТЕХНОЛОГІЯ REDTACTON

Куди рухатиметься науковий прогрес, що буде зі світовим телекомунікаційним ринком надалі, які технології стануть доступними пересічним Інтернет-користувачам, наскільки можуть збільшитися швидкості інтернет-доступу в найближчі 5-10 років? На сьогоднішній день це експериментальна розробки, але через кілька років вона може щільно увійти в наше повсякденне життя.

Технологія RedTacton використовує найбільший біологічний канал передачі даних - шкіру людини. Чи бувало з вами таке, що ви дивилися фільм про шпигунів з їх високотехнологічними штучками і теж хотіли одним дотиком руки отримувати інформацію на свій телефон, обмінюватися електронними візитками і будь-якими іншими даними за допомогою рукостискання або роздруковувати документи, просто провівши рукою по

принтеру? Все це і ще багато іншого може стати реальністю, якщо технологія RedTacton отримає розвиток.



Суть технології: технологія побудована на тому, що кожна людина має електромагнітним полем, а його шкіра може виступати каналом передачі сигналу між декількома електронними пристроями. В основі технології лежить використання електрооптичних кристалів, властивості яких змінюються під дією електромагнітного поля людини. А вже з кристалів за допомогою лазера зчитуються зміни і переводяться в більш-менш прийнятний формат.Причому система RedTacton може працювати не тільки в звичайних умовах, але і під водою, у вакуумі, в космосі.

Застосування: сьогодні нам доводиться часто користуватися різними кабелями, перехідниками та ін. для того, щоб, наприклад, підключити телефон до ноутбука або принтер до ПК. Якщо технологія RedTacton буде розвиватися, то незабаром всі ці дроти стануть непотрібними. Досить буде взяти в одну руку один гаджет, а іншою рукою торкатися другого пристрою. І з'єднання між ними відбудеться через наш шкірний покрив. Уже сьогодні більшість смартфонів оснащені екранами, які працюють від електромагнітних імпульсів на кінчиках наших пальців.

І це тільки перші кроки в популяризації даної технології. Вона може застосовуватися в медицині (всі ваші медичні дані можна записати на спеціальний чіп, який попередить лікаря про алергіях і непереносимості того чи іншого препарату після дотику до вас), збройних силах (можна зробити зброю, яке зреагує тільки на руки власника, і ваші діти ніколи не зможуть зашкодити собі, якщо знайдуть вдома ваш пістолет або мисливську рушницю), в побуті (ключі до вхідних дверей більше не потрібні, можна просто доторкнутися до замку і він спрацює від електромагнітного імпульсу), на виробництві (на заводах будуть встановлені датчики, які попередять вас про небезпечні зони і поломки, ви зможете швидко залагодити несправність, просто доторкнувшись до приладу) та інше.

Недоліки: технологія поки не вивчена достатньо, щоб точно сказати, що вона є абсолютно нешкідливою для організму людини. Впроваджувати RedTacton в маси можна буде тільки після того, як буде проведено безліч дослідів і досліджень. Небезпеки, перш за все, можуть піддаватися люди з підвищеною чутливістю і деякими медичними проблемами (особливо з серцевими захворюваннями). Крім того, хакери через якийсь час знайдуть спосіб красти дані людей або запускати комп'ютерні віруси, торкаючись до них в транспорті або на вулиці. Але основною проблемою цієї технології може стати психологія людей - багато сьогодні бояться комп'ютерів, Wi-Fi мереж і мікрохвильових печей, а можете собі уявити, що з ними буде, якщо їх власне тіло стане передавачем інформації?

Наука і технології рухаються вперед. А Інтернет-технології розвиваються чи не швидше за всіх інших. Щороку вчені винаходять все нові способи обмінюватися інформацією, спілкуватися на відстані, збирати, зберігати і передавати різні дані. Пройде ще десяток років, і ми будемо користуватися кожен день тими пристроями і можливостями, про які сьогодні можемо тільки мріяти.

Література:

2 . https://studwood.ru/1610039/informatika/internet_tehnologiyi_maybutnogo

Cherednichenko Volodymyr
State University of Telecommunications
Faculty of Telecommunications
Kyiv

HOW DOES MOBILE VOIP WORK?

In the work the solved the main advantages are revealed: Mobile VoIP uses an internet connection to offer significantly cheaper calls that with a traditional mobile phone line. With the Vonage Extensions mobile VoIP app, you can call cheaply or even for free as long as you have an internet connection.

Voice over IP, VoIP or IP telephony is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN)

Mobile VoIP or simply mVoI**P** is an extension of mobility to a Voice over IP network. Two types of communication are generally supported: cordless/DECT/PCS protocols for short range or campus communications where all base stations are linked into the same LAN, and wider area communications using 3G/4G protocols.

Mobile VoIP works with a cell phone's 3G, 4G, GSM, or other Internet service to send voice calls as digital signals over the Internet using voice over IP technology. Mobile VoIP phones can also take advantage of WiFi hotspots to eliminate the calling costs of a cellular voice or data plan..

By using VoIP, mobile VoIP phone users — especially smartphone users — can benefit from lower costs when calling, texting, or other common smartphone activities. Digital data transmission using VoIP is also typically faster, as the data is spread out over multiple packets, each taking the fastest route to its intended destination.

Using a mobile VoIP phone with WiFi hotspot access can also reduce a mobile VoIP phone user's costs by sidestepping the carrier's expensive 3G service altogether. For instance, with a cellular carrier's monthly data plan, callers can easily exceed bandwidth maximums, incurring overage charges. Tapping into WiFi hotspots with mobile VoIP software reduces that risk and extends the lifespan of the monthly data allotment.

A mobile VoIP phone service can eliminate the need for a basic voice plan, as well as optional (and costly) text add-ons. With a mobile VoIP phone, cell phone users can enjoy more flexibility in calling times than a cellular voice plan provides, with fewer restrictions. VoIP mobile phone service means that a mobile VoIP user can make unlimited inexpensive or free calls using voice over IP technology at any time.

Accessing Mobile VoIP

Cell phone users can use mobile VoIP service on their phone with the addition of mobile VoIP software. These are apps offered by VoIP phone service providers customers may already be using at home or at work, such as Vonage, or standalone mobile VoIP apps such as Skype, Vyke, or Truphone.

Some services, such as Truphone, also offer an entire mobile VoIP network by combining a SIM (Subscriber Identity Module) card and an app together. (The SIM card contains all the information needed to identify network subscribers.) One functions where the other doesn't, depending on the circumstance, to offer a comprehensive mobile VoIP network service.

To use this kind of mobile VoIP function, along with other similar services, you need an unlocked handset. Most mobile VoIP apps, however, piggyback onto your existing data plan and do not require unlocking.

Benefits of Mobile VoIP

Mobile VoIP phone users can benefit from voice over IP services to lower their monthly phone bills. Some cell phone users will take advantage of mobile VoIP phone service to eliminate

their voice plans. Using mobile VoIP can result in a simple, data-plan-only relationship with your cell phone carrier. Choosing a data-only plan can result in significant savings.

Five Best Mobile

VoIP AppsIf you want to save some money on your wireless bill, ditch your minutes and use a mobile VoIP app to make your calls. It's not difficult, and many are either free or low-cost depending on who you call. Here are five of the best VoIP apps for your smartphone, based on your nominations.Earlier in the week we asked you for your favorite mobile VoIP appswe asked you for your favorite mobile VoIP apps. You weighed in with tons of great options, way more than we have room to highlight here, so make sure you head back to the call for contenders if you don't see your favorite listed here. With that aside, here are the five that got the most nominations and made it to this round, in no particular order

1 Viber
2 Google Hangouts
3 Skype
4 MagicAp
5 Vonage Mobile

Literature:

1.Mobile Voice over IP (MVOIP): An Application-level Protocol for Call Hand-off in Real Time Applications, G. Ayorkor Mills-Tettey and David Kotz, Proc. Of 21st IEEE Int. Perf, Comp. and Comm. Conf,

Lytvun Glib
State University of Telecommunications
Faculty of Telecommunications
Kyiv

MODERN INFORMATION TECHNOLOGIES

*The development of IT-technologies helps to increase the efficiency of social production in all spheres***.**

The ability to search, manage, process and exchange information opens up new horizons, it is possible to automate as much as possible any production processes, improve labor performance and simplify business management.

Modern information technologies should be as accessible to consumers as possible so that they can conduct various operations without the expense of time and effort.

The organization of quick access to all the information resources necessary for work guarantees the improvement of the economic performance of enterprises of any sector and the improvement of working conditions for personnel.

According to the type of information processed, IT technologies can be conditionally divided into the following types:

- Data (algorithmic languages, tabular processors);
- Text (word processors and hypertext);
- Graphics (graphics processors);
- Knowledge (expert systems);
- Objects of the real world (multimedia).

All modern technologies allow the use of several types of information processing. For example, in text editors it is possible to compile tables for calculating data, charts can be used in tables, etc.

Nevertheless, each method allows to create new technologies, which at the moment are used by narrow-profile enterprises, factories, factories and companies.

Providing information technology (IT)

This type of IT provides the solution of specific tasks of different complexity level by using certain components and software. Providing information technologies can be combined on a

subject basis, but in such conditions all systems should have a single standard interface for the convenience of their use.

Functional Information Technology (FIT)

This kind of IT is a modification of the providing technologies for the directed solution of specific problems. The transition of ICU to FIT is carried out by converting the commonly used tools into a special one. For example, employees of technical departments can be provided with their own supporting technologies and functional technologies of other departments.

Modern information technology can also be classified according to the types of user interface. The application interface allows you to implement functional IT, and the system interface contains a set of techniques for interacting with the computer. This set can be implemented by the operating system or its add-ons.

The following requirements are imposed on information technologies:

- Differentiation - the ability to break the whole process into separate phases, stages and actions;
- Completeness - the presence of a whole set of tools that are necessary to achieve certain goals;
- Regular character - standardization and unification of all stages for the most effective management of information processes.

Informatization of society

The introduction of IT in all spheres of human activity is the process of informatization of society. During this process, specialists from different areas are trained to use all information tools to achieve specific goals. Knowledge of the information, the ability to process and exchange it helps significantly reduce financial costs, time and effort to perform certain operations.Modern society, information has become the same value as education, cadres, money and other material values, so its free flow can lead to a significant improvement in the standard of living of every person. Quick access to all necessary data can be obtained both by employees of different spheres of production, and by doctors, students, scientists and other specialists. New discoveries, wireless control of space vehicles, the restoration of the appearance of prehistoric inhabitants of the planet is not a complete list of broad opportunities that people have already learned to use in practice with the help of IT.

Literature:

1.https://ru.wikipedia.org
2. http://www.sviaz-expo.ru

Oleksandr Novik,
Denis Kozhemyakin,
Student of the group TSD-41
State University of Telecommunication

UNIVERSAL ZABBIX NETWORK MONITORING SYSTEM

Considered the telecommunication industry in the present, the analysis of modern telecommunication infrastructure. The principle of functioning of modern universal monitoring system of Zabbix networks is shown.

The telecommunication industry is undergoing significant transformations today, its speed is increasing every year, so a modern representative of the telecommunications market in its activity uses monitoring and control systems. At the same time, in the conditions of constant increase of the complexity of information and telecommunication systems, the reliability of the telecommunication network and the quality of the services provided are of particular importance.

Modern telecommunication infrastructure is a complex network that includes telecommunication, server and software of different manufacturers, working in different standards and managing various software. The complexity and scale of the network infrastructure result in a high level of automated monitoring and management tools that should be used to ensure the robust operation of the network.

One of the best tools for solving this problem is the free Zabbix system, which consists of three basic components: a server for coordinating inspections, forming verification queries, and stacking statistics; agents for external party inspections; frontend for organization of system management. Zabbix offers excellent reporting and visualization capabilities based on gathered data, making Zabbix the perfect tool for planning and scaling. A well-designed program can play an important role in monitoring IT infrastructure.

Thus, we can conclude that Zabbix is in vain used by a large number of companies that chose it for its ease of use, high fault tolerance, and reliability at extremely low cost of its use.

Literature:

4. *Zabbix Practical guide/ Andrea Dalle Wacque, 2017.- p. 15.*
5. *www.zabbix.com*
6. *Synopsis of lectures "Monitoring of Telecommunication Networks", State University of Telecommunications, 2017.*

Скнарь І. М., Кожем`якін Д. В.
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Телекомунікацій
м. Київ

ШТУЧНИЙ ІНТЕЛЕКТ ДЛЯ КОМП'ЮТЕРНИХ ІГОР

Дослідники з Корнуельського університету зробили те, що зможе кардинально змінити процес розробки нових відеоігор. Вони створили пару змагающихся нейронних мереж (Generative Adversarial Network, GAN) і навчили їх на прикладі самої першої гри-Шуттер, DOOM-а. В процесі навчання нейронні мережі визначили основні принципи побудови рівнів цієї гри і після цього вони стали здатні генерувати нові рівні без найменшої допомоги з боку людей.

GAN-мережі, досліджуючи рівні DOOM-а, становили свою власну карту, на яку наносилися не тільки топографічні особливості віртуального простору, а й місця розташування різних активних об'єктів, включаючи і інших ігрових персонажів, противників і монстрів в даному випадку.

Одна мережа навчалася тільки на основі потоку переданих їй відеоданих, а іншій мережі передавалися ці ж дані, забезпечені додатковою інформацією, отриманою в ході попереднього аналізу. І після того, як мережі "проковтнули" всі рівні DOOM-а, вони стали здатні генерувати свої власні рівні. При цьому, якість і складність нових рівнів були вельми і вельми високими, але система штучного інтелекту буквально за секунди часу робило те, що зайняло б багато годин роботи цілого колективу, що складається з дизайнерів, художників і програмістів.

І на закінчення слід зазначити, що дослідники з Корнуела не переслідували мету створення нових рівнів саме для застарілого DOOM-а або іншого Шуттер від першої особи. Ця технологія може бути успішно використана і по відношенню до комп'ютерної гри будь-якого іншого жанру, в чому можна переконатися, заглянувши на сторінку проекту "Video Game Level Corpus", розташованого на відомому сервісі Github.

Інформаційні ресурси:

1. https://www.slashgear.com/video-game-maps-made-by-ai-more-doom-08529997/

СЕКЦІЯ №2. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Солопова Д.О.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ЦЕНТРАЛІЗОВАНА ОБРОБКА ІНФОРМАЦІЇ НА ЕОМ

Сучасне матеріальне виробництво та інші сфери діяльності все більше потребують інформаційного обслуговування, переробки величезної кількості інформації. Універсальним технічним засобом обробки будь-якої інформації є комп'ютер, який грає роль підсилювача інтелектуальних можливостей людини і суспільства в цілому, а комунікаційні засоби, які використовують комп'ютери, служать для зв'язку і передачі інформації. Поява і розвиток комп'ютерів - це необхідна складова процесу інформатизації суспільства.

При впровадженні нової інформаційної технології в організації необхідно оцінити ризик відставання від конкурентів у результаті її неминучого старіння з часом, тому що інформаційні продукти, як ніякі інші види матеріальних товарів, мають надзвичайно високу швидкість змінюваності новими видами або версіями.

Централізована обробка інформації на ЕОМ обчислювальних центрів була першою історично сформованою технологією. Створювалися великі обчислювальні центри колективного користування, оснащені великими ЕОМ . Застосування таких ЕОМ дозволяло обробляти великі масиви вхідної інформації й одержати на цій основі різні види інформаційної продукції, яка потім передавалася користувачам.

Переваги методології централізованої технології:

- Можливість звернення користувача до великих масивів інформації у вигляді баз даних і до інформаційної продукції широкої номенклатури;

- Порівняльна легкість впровадження методологічних рішень по розвитку й удосконаленню інформаційної технології завдяки централізованому прийняттю

Недоліки такої методології:

- Обмежена відповідальність нижчого персоналу, який не сприяє оперативному одержанню інформації користувачем, тим самим, перешкоджаючи правильності виробітку управлінських рішень;
- Обмеження можливостей користувача в процесі одержання і використання інформації.

Децентралізована обробка інформації пов'язана з появою персональних комп'ютерів і розвитком засобів телекомунікацій. Вона дуже істотно потіснила попередню технологію, оскільки дає користувачу широкі можливості в роботі з інформацією і не обмежує його ініціатив.

Перевагами є:

- Зменшення потреби в користуванні центральним комп'ютером і відповідно контролі з боку обчислювального центру;
- Більш повна реалізація творчого потенціалу користувача завдяки використанню засобів комп'ютерного зв'язку.

Недоліки:

- Складність стандартизації через велику кількість унікальних розробок;
- Психологічне неприйняття користувачами рекомендованих обчислювальним центром стандартів готових програмних продуктів;

Описані переваги і недоліки централізованої і децентралізованої інформаційної технології призвели до підходу,який назвемо раціональною методологією ,у цьому випадку будуть розподілятися обов'язки так:

- ✓ Обчислювальний центр повинен відповідати за вироблення загальної стратегії використання інформаційної технології;
- ✓ Персонал, який використовує інформаційну технологію, повинен дотримуватися вказівок обчислювального центру, здійснювати розробку своїх локальних систем і технологій відповідно до загального плану організації.

Раціональна методологія використання інформаційної технології дозволить досягти більшої гнучкості, підтримувати загальні стандарти, здійснити сумісність інформаційних локальних продуктів, знизити дублювання діяльності та ін.

Сучасні інформаційні технології міцно увійшли в наше життя. Вони відкрили нові можливості для роботи і відпочинку, дозволили багато в чому полегшити працю людини.

ературою, освітленням та іншими периферфйними пристроями.

Чухра М.І.
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ДОПОМОГА СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В БОРОТЬБІ З НАДЗВИЧАЙНИМИ СИТУАЦІЯМИ

У сучасному суспільстві інформатизація є важливим засобом організації й регулювання приватної і суспільної життєдіяльності. Тому роль інформації у вирішенні будь-яких проблем є однією з основних. Одною з проблем для людини, підприємства, держави є надзвичайна ситуація (НС).

Впровадження інформаційно-комунікаційних технологій у підрозділи реагування, рятувальних служб мінімізує час на вивчення особливостей НС. Інформатизація забезпечує мобільність, оперативність та ефективність дій керівництва, знижуючи ймовірність смертності людей, адже прагнення керівника до прийняття рішення з меншим ступенем

ризику призводить до збільшення витрат часу на підготовку та вибір оптимального варіанту.

Аналіз управління та розробки управлінських рішень свідчить про потребу розв'язання управлінських проблем особливо на основі використання засобів комп'ютерної техніки. Побудова ІС на базі засобів обчислювальної техніки приводить до зміни й удосконалення методів збирання, опрацювання, зберігання і використання у процесі прийняття управлінських рішень.

Своєчасно отримана інформація дозволяє заздалегідь підготуватись і організувати заходи щодо збереження людського життя та захисту життєво важливих даних для підприємства, держави. Також інформування та оповіщення є невід'ємним елементом системи заходів проти НС цю інформацію становлять відомості про характер НС, класифікацію, межі поширення, наслідки.

Сучасні засоби передачі та зв'язку полегшують евакуацію населення та інформування про безпечні зони для людей, повідомлення про потребу медичної допомоги та вказують на точне місце знаходження потерпілого. Технічні засоби дозволяють своєчасне виявлення чинників біологічного, радіаційного та хімічного зараження.

Інформаційні технології є перспективними напрямками розвитку суспільства. Основним напрямком котрих є прискорення процесу отримання нових знань та навичок. Не варто забувати, інформаційні технології несуть негативний характер в тому, що люди не помічають наскільки сильно залежать від сучасних технологій і при відмові тих же систем оповіщення і реагування на які покладається керівництво можуть постраждати люди.

Література:

1. *Реферат на тему: «Управлінська діяльність підрозділів МНС: впровадження інформаційних технологій.» http://ru.osvita.ua/vnz/reports/management/15228/*

Маленюк А.О.
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ДОПОВНЕНА РЕАЛЬНІСТЬ У СУЧАСНОМУ СВІТІ

У наш час, коли темп розвитку технологій дивує все більше і більше, кожна людина стає частиною інформаційного простору і потребує певних навичок для використання всіх можливостями, що відкриваються перед нею. Побудова зручного інтерфейсу користувача – одна з основних проблем розробки апаратного та програмного забезпечення сьогодення.

Наразі найбільш перспективною моделлю інтерфейсу вважають саме середовище з доповненням фізичного світу цифровими даними в режимі реального часу – доповнену реальність, що вже зарекомендувала себе з позитивного боку у таких галузях як медицина, архітектура, навігація та дизайн. Технології доповненої реальності вже зараз використовують пілоти військових літаків та вертольотів.

Доповнена реальність проникає до наших смартфонів. Значна кількість додатків навіть сьогодні здатна використовувати зображення з камери та змінювати його для користувача. Наприклад, технологія потокового перекладу від корпорації Google здатна перекладати друкований текст, що знаходиться перед камерою у режимі реального часу або гра Pokemon GO, що нещодавно з'явилася і миттєво набула популярності серед молоді.

Розробники програмного забезпечення ще нещодавно вважали, що такі технології стануть можливими лише через 10 років, але вже зараз, після появи доволі примітивних прикладів використання доповненої реальності стає зрозуміло, що це тільки початок. Така технологія дозволить робити 3D-фотографії. Наприклад, 3D-фотографія кімнати. Це означає, що фотографію можна розглядати під будь-яким кутом, змінювати світ, предмети

на ній будуть змінюватися залежно від кута огляду. З такими знімками можна експериментувати: затопити кімнату, вимкнути/увімкнути в ній світло.

За словами голови Apple Тіма Кука, технологія доповненої реальності - також відома як AR (з англ. - augmented reality) - це настільки ж "велика ідея", здатна змінити світ, як свого часу - смартфон.

Ринкова вартість всіх засобів доповненої реальності, разом з ігровими, автомобільними, рекламними, освітніми та геолокаційними додатками в 2016-у році була оцінена як $5 155,92 млн., і зараз продовжує свій ріст. Такі гіганти інноваційного руху як Google та Microsoft вже мають свої варіанти реалізації доповненої реальності для простих користувачів – окуляри Google Glass та Microsoft HoloLens, що вже зовсім скоро з'являться на поличках магазинів комп'ютерно' техніки.

Таким чином, доповнена реальність вже зараз стає частиною людського життя та однією з найперспективніших напрямів для розробки програмного забезпечення.

Скаба С.М.
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

INTERNET OF THINGS. ВАРІАНТИ ПІДКЛЮЧЕННЯ IOT

Спочатку Інтернет був мережею взаємодії між людьми за допомогою комп'ютерів. Згодом він став використовуватися для взаємодії пристроїв між собою, даний метод згодом отримав назву Інтернет речей. Технології взаємодії суворо пристроїв з пристроями отримали назву M2M (machine to machine). Концепція IoT має не лише об'єднати ці два підходи («Інтернет машин» та «Інтернет людей»), а й вивести їх на новий глобальний рівень взаємодії та можливостей. Ідея Internet of Things охвачує всі сфери сучасного життя – побут, освіта, бізнес, медицина, транспорт, промисловість, екологія тощо. Список можна продовжувати нескінченно. Недивно, що говорячи про ринок Internet of Things аналітичні компанії оперують сумами в трильйон доларів.

Безпроводові технології - інформаційні технології, призначені для безпроводової передачі інформації на відстань між двома й більше об'єктами. Для передачі інформації може використовуватися інфрачервоне випромінювання, радіохвилі, оптичне або лазерне випромінювання. На сьогодні існує безліч безпроводових технологій, відомих користувачам по їхніх маркетингових назвах, таким як Wi-Fi, WiMAX, Bluetooth, ZigBee, LTE та інші. Кожна технологія має певні характеристики, які визначають її область застосування.

Найновішою областю застосування безпроводових технологій є IoT (Internet of Things). В даний час розроблюються безпроводові технології під егідою робочої групи 802.11, в тому числі 802.11ah, також відомої як HaLow – стандарт для більш низької частоти для великих територій, призначений виступати в якості комірчастої мережі саме для Інтернету речей.

На сьогодні можна зустріти різні визначення як концепції IoT, так і різноманітні точки зору на те, які основні сфери вона охвачує. Найбільш показовим є розділення, запропоноване Harward Business Review, в рамках якого розвиток Інтернету речей проводиться в п'яти напрямках: портативні пристрої, «розумний будинок», підключені автомобілі, «розумне» місто, промисловий Інтернет.

Є безліч варіантів підключення IoT і кожен з них має певні плюси і мінуси. Основні параметри з'єднання, які використовуються в загальному випадку, це Wi-Fi, Bluetooth та стільникового бездротовий зв'язок (4G). Але у кожного з них є недоліки: Wi-Fi

використовує багато енергії; Bluetooth має обмежений діапазон; 4G також енергоємний та може бути дорогим, особливо для передачі великих об'ємів даних.

Мережеві інновації зосереджені на вирішенні проблем підключення пристроїв на великій відстані та задоволення потреб з низьким енергоспоживанням, наприклад, для пристроїв, що працюють на батареях. Цілий ряд нових мережевих IoT-опцій існують, серед них:

- Sigfox - У 2009 році Sigfox, французький стартап, представив малопотужну мережу, з ультра-вузькою смугою пропускання, що працює на неліцензованій частині спектру. Базується на моделі обслуговування операторів безпроводового зв'язку. Sigfox доступний тільки в певних частинах Європи, великих містах США та вибірково в Латинській Америці.
- LoRA - Lora Alliance – це група індустріальний партнерів, що займаються розробкою протоколу з низьким енергоспоживанням, що називається LoRaWAN. Даний протокол працює на неліцензованих частотах.
- Стільниковий IoT – Це кілька стандартів, що базуються на специфікації 3GPP, такі як LTE-M, NB LTE-M, і NB-IoT. Ці стандарти мережі змінені і оптимізовані для пристроїв IoT.

У найближчому майбутньому більшість наших електронних або квантових пристроїв будуть підключені до Інтернету через унікальну IP-адресу (в полі IPv6-адрес, оскільки IPv4 уже скоро стане елементом минулого) і, таким чином, його можна буде контролювати власником з будь-якого місця в будь-який час.

В деяких країнах плануються проекти розумних міст, створених на основі смарт-інфраструктури в поєднанні з використанням технології IoT. Що стосується людей, то портативні пристрої і розумні будинки стануть ключем до розумного і сталого майбутнього.

IoT також допоможе урядам і великим підприємствам в моніторингу, збору, аналізу і прийнятті рішення щодо будь-якої ситуації протягом короткого часу.

Проте слід пам'ятати, що постійний розвиток технології означатиме більше електронних відходів, проблема охорони навколишнього середовища з розвитком IoT набуде особливого значення.

Дві причини підштовхують українців до реалізації IoT-проектів, здатних підкорити місцевий ринок і весь світ. Перша - спроба заощадити внутрішні ресурси: електроенергію, час, воду, сили людини. Друга - бажання опинитися біля витоків багатомільйонного бізнесу.

Internet of Things - це підключення до Інтернету всіляких пристроїв, за винятком смартфонів, планшетів і комп'ютерів. Це можуть бути датчики світла і тепла, спеціальні пристрої в автомобілях, медичні прилади й просто будь-які інші звичні предмети. Дані, які вони збирають про людину і навколишній світ, пропускаються згодом через складні програми, які перетворюють хаотичний набір показників корисну інформацію і рекомендації.

IoT є відносно безпечним - ви навряд чи зіткнеться з серйозною втратою або пошкодження через смарт-датчики, принаймні, не більше, ніж через свій домашній комп'ютер. Тим не менше, немає ніякої гарантії і досі робиться не достатньо для забезпечення захисту IoT від злому.

З кожним днем збільшується необхідність в додатковому обладнанні, яке дозволило б збирати і обробляти більший масив даних. Оскільки речей, здатних робити це, незліченна кількість, це відкриває новий необмежений ринок. За прогнозами, він буде стрімко зростати: з 656 млрд дол в 2014 році до 1,7 трлн дол в 2020 році.

Цапро Ігор
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій

м. Київ

ЧИ МОЖЛИВЕ ЗАСТОСУВАННЯ КВАНТОВОЇ ЗАПЛУТАНОСТІ В КОМУНІКАЦІЯХ?

Теорія квантової механіки забороняє передачу інформацію з надсвітловою швидкістю. Це пояснюється принципово ймовірнісним характером вимірювань і теоремою про заборону клонування. Уявіть собі дві монети, кожна з яких може випасти орлом або решкою. Одна монета у вас, інша у мене, а ми знаходимося надзвичайно далеко один від одного. Ми підкидаємо свої монетки в повітря, ловимо їх і шльопаємо на стіл. Перед тим як поглянути на монету, ми очікуємо, що решка випаде з ймовірністю в 50/50, і орел, звичайно, також. У звичайному, незаплутаному Всесвіті, ваш і мій результати будуть незалежні один від одного. Якщо у вас випаде решка, моя монета з ймовірністю у 50% впаде орлом або решкою. Але за певних умов ці результати можуть бути заплутані: якщо ви проводите цей експеримент і отримуєте решку, ви будете знати, що моя монета з ймовірністю в 100% покаже орла, ще до того, як я вам про це повідомлю. Ви дізнаєтеся про це миттєво, навіть якщо ми будемо розділені світловими роками і не пройде жодної секунди.

У квантовій фізиці ми зазвичай заплутуємо НЕ монети, а окремі частинки, накшталт електронів і фотонів, де, наприклад, кожен фотон може мати спін +1 або -1. Якщо виміряти спін одного фотона, ви миттєво дізнаєтеся спін іншого. Поки ви не виміряли спін одного фотона, вони обидва існують в невизначеному стані; але як тільки виміряли один, ви відразу ж довідаєтеся про інший. На Землі проводили такий експеримент, розділивши два заплутаних фотона багатьма кілометрами і вимірявши їх спіни протягом наносекунди. Виявилося, що якщо ми вимірюємо спін одного і він виявляється +1, ми дізнаємося про те, що спін іншого -1 в 10000 разів швидше, ніж могла б дозволити нам швидкість світла.

І ось питання: чи могли б ми використовувати це властивість - квантової заплутаністі - щоб зв'язатися з далекою зоряною системою? Відповідь: так, якщо вважати проведення вимірювання у віддаленому місці формою зв'язку. Але є проблема: заплутаність працює, тільки якщо ви питаєте частинку: в якому вона стані? Якщо ви ставите заплутану частинку в певний стан, ви руйнуєте заплутаність. Крім проблеми «суперпозиції» заплутаних часток залишається невирішеною проблема **декогеренції**, тобто втрати частинками заплутаності згодом через взаємодію з навколишнім середовищем. Але з розвитком науки, цілком можливе використання квантової заплутаності у комунікаціях.

Зайченко Є.А.
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

МОЖЛИВОСТІ WI-FI РАДІОХВИЛЬ

В данній статті ведеться мова про використання Wi-Fi сигналу в методиках створення голографічних зображень та сканування різних об'єктів з метою побудови тривимірних зображень .

Тотальне поширення Wi-Fi пристроїв привело до того, що ми і все, що нас оточує, буквально оповите невидимою мережою випромінюваних сигналів. Дослідники з Мюнхенського технічного університету вирішили, що таке «добро» не повинно дарма пропадати, оскільки його можна з успіхом використовувати для створення тривимірних образів простору.

У той час, як оптичні голограми вимагають складних лазерних технологій, створення голограми з мікрохвильовим випромінюванням для Wi-Fi-передавача вимагає тільки однієї фіксованої і однієї рухомої антени.

Подібні технології вже застосовувалися при створенні пристроїв, які «бачать крізь стіни», здатних розрізняти фігури людей і визначати їх кількість. Вчені з Мюнхена пішли далі, навчившись формувати повне тривимірне зображення простору кімнати або навіть будівлі за допомогою Wi-Fi і стільникових сигналів.

Подальше теоретичне моделювання показало, що схожим чином можна відновити обстановку більш великої площі, у тому числі складу розміром 20x17x12 метрів з металевими стелажами. Причому роутер як джерело «освітлення» в цьому випадку може перебувати за міжповерховим перекриттям.

Замість використання рухомої антени, яка вимірює зображення точки на точку, можна використовувати більшу кількість антен, щоб отримати відео — як кадрування зображення. В майбутньому Wi-Fi-частоти, як пропонований стандарт 60 гігагерц і IEEE 802.11 дозволять резолюції аж до міліметрового діапазону.

Дослідники сподіваються, що подальше вдосконалення технології може допомогти в знаходженні жертв, похованих під лавиною або у зруйнованій будівлі. У той час, як звичайні методи дозволяють тільки відслідкувати точки локалізації жертв, голографічна обробка сигналів може забезпечити просторове уявлення зруйнованих структур, що дозволяє екстрено реагувати, щоб обійти навколо важкі предмети і використовувати порожнини в завалах, щоб системно висвітлити найпростіший підхід, щоб швидко дістатися до жертви.

Література:

1. *Philipp M. Holl and Friedemann Reinhard Holography of Wi-fi Radiation.\ Philipp M. Holl and Friedemann Reinhard\\ Physical Review Letters. — 05.05.2017. – DOI: 10.1103 — PhysRevLett.118.183901*
2. *Physical Review Letters, 05.05.2017 – DOI: 10.1103/PhysRevLett.118.18390*

Остапенко Г.А.

Державний Університет Телекомунікацій

Навчально-науковий інститут Телекомунікацій та інформатизації

Факультет Інформаційних технологій

м. Київ

«ЛУЧ ТЕМНОТЫ».

Идея проекта не сложная : изображение, передающееся в наши глаза, есть не что иное, как отражение света от объекта. Если отражения не будет — не будет информации о состоянии объекта, то есть можно будет заявить о его «невидимости».

Несмотря на всю нереальность вышесказанного , технология полноценно работает: “луч тьмы” создаёт трёхмерный участок невидимости, так называемую, “пустую световую капсулу”. В этом участке можно скрывать макроскопические объекты.

Сингапурские исследователи добавив известные всем факты, с помощью системы линз сумели создать такой участок пространства, в котором интенсивность света близка к нулю. Это пространство учёные назвали «антиразрешением», так как она является противоположностью суперразрешению.

Система, применяемая для создания таких участков, довольно проста: в неё входят лазер, специальные линзы с диэлектрическими пазами и проецирующий аппарат.

ГЛАВНАЯ ИДЕЯ ПРОЕКТА

Главная идея в том, что когда объект находится в фокусе, он воспринимается четко и с определенными границами. Вне фокуса резкость границ уменьшается, а середина остается яркой. Исследователи взяли за основу технику суперразрешения и с помощью

системы линз сумели создать участок пространства, в котором интенсивность света близка к нулю – а если нет света, то в этой точке невозможно что-либо увидеть.

Вместе с тем, когда этот самый объект находится в фокусе, наши глаза воспринимают чёткие очертания с хорошо различимыми границами. Вне фокуса резкость границ объекта значительно уменьшается, а яркой остаётся только середина.

РЕЗУЛЬТАТЫ

В ходе экспериментов учёным удалось спрятать 40-микрометровый трёхмерный объект от одной конкретной длины волны (630 нм — красный лазер).

В ходе испытаний учёные успешно сокрыли 40-микрометровый трёхмерный объект от одной конкретной длины волны.

В результате у них получается пустая световая “капсула невидимости”. Система, применяемая для создания таких участков, удивительно проста, и состоит из лазера, специальных линз с диэлектрическими пазами, и проецирующего аппарата.

Плюс в том, что линза, модифицирующая излучение лазера, проста в изготовлении и, по сути, является прозрачной пластинкой с концентрическими кругами стандартных диэлектриков.

Это явление называют функцией точечного рассеивания (point spread function, PSF)

В перспективе исследователи обещают создание полноценной “пушки невидимости”, которая позволит нацелиться на любой произвольный объект и сделать его невидимым.

ЧТО ОЖИДАТЬ ОТ ПРОЕКТА?

В перспективе исследователи обещают создание полноценной “пушки невидимости”, которая позволит нацелиться на любой произвольный объект и сделать его невидимым.

Раньше исследование были в области мета материалов, позволяющих изгибать волны вокруг объектов и искажать или скрывать тем самым изображение.

ВЫВОД

Здесь видно различие- первая в мире демонстрация нового метода создания невидимости.

Если посмотреть на темпы развития исследования лазеров, в будущем новое средство разрешит создать устройство, которое будет способно спрятать более крупные предметы от наших глаз.

Не смотря на то что шаги продвижения этого проекта не велики ,я вижу перспективу в будущем, ведь это абсолютно новый подход.

Я была крайне впечатлена и с удовольствием искала информацию по поводу этого проекта, и я уверенна что в будущем мы сможем лицезреть его.

Література:

1. *http://www.extremetech.com/extreme/172797-anti-resolution-darkness-ray-can-make-objects-invisible-from-a-distance*

Адаменко А.Н.
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ДЕЦЕНТРАЛИЗОВАННЫЕ ЦИФРОВЫЕ УДОСТОВЕРЕНИЯ ЛИЧНОСТИ И БЛОКЧЕЙН

Рассмотрены принципы и концепции по децентрализованным удостоверениям личности, где целью есть представить разнообразие интерфейсов, найти механизмы повышения доверия и

сократить разногласия, чтобы каждый человек мог иметь собственное цифровое удостоверение личности и распоряжаться им.

Мир находится в процессе глобальной цифровой трансформации, где цифровая и физическая реальность сливаются в единый интегрированный современный стиль жизни, и многие из вас наблюдают это каждый день. Вместо того чтобы давать доступ к своей персональной информации бесчисленному множеству приложений и сервисов и делиться своими данными с огромным количеством провайдеров, людям необходимо создать надежный зашифрованный цифровой хаб, где они смогут хранить свои идентификационные данные и без труда контролировать доступ к ним.

Каждому из нас необходимо цифровое удостоверение личности, находящееся в нашем полном распоряжении, где с соблюдением надежности и конфиденциальности хранятся все элементы наших персональных данных. Это удостоверение должно быть простым в использовании, и у каждого человека должна быть возможность выбирать, кто может получить доступ к его персональным данным, и как их можно использовать.

Блокче́йн — выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию. Чаще всего копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга.

Блоки – это данные о транзакциях, сделках и контрактах внутри системы, представленные в криптографической форме. Они все выстроены в цепочку, то есть связаны между собой. Для записи нового блока, необходимо последовательное считывание информации о старых блоках. Все данные в блокчейн накапливаются и формируют постоянно дополняемую базу данных. С этой базы данных невозможно ничего удалить или провести замену/подмену блока. И она «безгранична» - туда может быть записано бесконечное количество транзакций. Это одна из главных особенностей блокчейна.

Работу блокчейн можно сравнить с Torrent. Функционирование торрентов происходит в режиме P2P (peer to peer – компьютерная сеть, где все участники равноправны). Когда мы скачиваем какой-то файл с трекера, то мы не используем центральный сервер или хранилище. Файл напрямую скачивается у такого же участника торрента, как и вы. Если в пиринговой сети не будет участников, то и файлы скачивать вы не сможете. Аналогично и в блокчейн. Все операции проводятся между субъектами напрямую. А осуществляются они за счет того, что все участники подключены к одной сети – Blockchain.

Семь основных концепций децентрализованного удостоверения личности :

- Владейте своим удостоверением личности и распоряжайтесь им.
  С учетом того, что утечки данных и кражи персональной информации происходят всё чаще и становятся всё более изощренными, пользователям необходим способ, который позволит им взять на себя ответственность за свои персональные данные. Технология блокчейна и протоколы смогут стать хорошей основой для децентрализованных удостоверений личности
- Изначально предусмотренная, «встроенная» конфиденциальность.
  Сегодня приложения, сервисы и организации создают удобные, предсказуемые, адаптированные интерфейсы, которые зависят от контроля персональных данных. Необходим безопасный зашифрованный цифровой хаб (ID-хаб), который может взаимодействовать с пользовательскими данными, сохраняя конфиденциальность и контроль.
- Доверие, полученное человеком и сформированное сообществом.
  Традиционные системы идентификации, как правило, включают в себя аутентификацию и управление доступом. В то время как контролируемая пользователем система идентификации фокусируется на аутентичности и формировании доверия сообществом, в децентрализованной системе доверие базируется на удостоверениях подлинности, то есть на утверждениях, которые

поддерживают другие пользователи, что помогает подтвердить отдельные фрагменты персональных данных.

- Приложения и сервисы, в центре которых находится пользователь.
  DID и ID-хабы могут позволить разработчикам получить доступ к более четкому набору удостоверений подлинности, снижая юридические риски и риски соответствия, за счет обработки такой информации вместо контроля над ней от имени пользователя.
- Открытая, совместимая основа.
  Чтобы создать устойчивую экосистему децентрализованных удостоверений личности, доступную для всех, необходимы стандартные технологии, технологии с открытым кодом, протоколы и эталонная реализация.
- Готовность к мировому масштабу.
  Чтобы обеспечить поддержку различного рода организаций, пользователей и устройств, технология, лежащая в основе, должна быть масштабируемой наравне с традиционными системами. Некоторые публичные блокчейн-платформы предоставляют прочную основу для встраивания DID, записи операций децентрализованной инфраструктуры открытых ключей (DPKI) и привязки удостоверений подлинности. В то время как некоторые блокчейн-сообщества увеличили объем транзакций, этот подход обычно снижает децентрализованное состояние сети и не позволяет достичь миллионов транзакций в секунду, которые система должна генерировать в мировом масштабе.
- Доступность для каждого.
  Сегодня блокчейн-экосистема включает в себя в основном первых адептов, которые готовы тратить время, усилия и энергию на управление ключами и обеспечение безопасности устройств. Необходимо решить задачи, связанные с управлением ключами, такие как восстановление, ротация и безопасный доступ, сделав их интуитивно понятными и защищенными от неумелого обращения.

Непосредственно, компания Microsoft, в сотрудничестве с Accenture и Avanade, уже разработала прототип на базе блокчейн на Microsoft Azure. Они вместе провели эту работу в поддержку организации ID2020 Alliance – глобального частно-государственного партнерства, помогающего 1,1 миллиарда человек на Земле, у которых отсутствуют какие-либо официальные идентификационные документы. По замыслу проекта до 2030 года планируется обеспечить всех людей на планете цифровым ID

Итог

Закрытие «идентификационного пробела» – сложнейшая задача. Необходима слаженная работа множества людей и организаций из разных стран, представляющих разные секторы экономики и технологии. Но так приятно мечтать о мире, где появятся безопасные и надежные цифровые удостоверения личности, и где они становятся основой для реализации всех прав и перспектив, которых заслуживают все люди на Земле.

Литература:

1. *Блокчейн. - Режим доступа:* https://ru.wikipedia.org/wiki/Блокчейн
2. *Децентрализованные цифровые удостоверения личности и блокчейн: будущее, как мы его видим. - Режим доступа:* https://news.microsoft.com/ru-ru/decentralized-did/
3. *Partnering for a path to digital identity. - Режим доступа:* https://blogs.microsoft.com/blog/2018/01/22/partnering-for-a-path-to-digital-identity/

Труш І.Е.
Державний Університет Телекомунікацій

Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

АВАРИЙНЫЕ РОБОТЫ ПОДДЕРЖКИ ДЛЯ УСТРАНЕНИЯ СЛОЖНЫХ ПОЛОМОК В РАЗЛИЧНЫХ СРЕДСТВАХ ПЕРЕДВИЖЕНИЯ

В докладе рассмотрено перспективы использования специализированных роботов по ремонту и обнаружения сложных поломок и неисправностях в системах транспорта. Сделан анализ наиболее вероятных возникавших проблем в системах транспорта. Обозначены необходимые требования по соответствию программного кода для роботов, который войдёт в основу функционирования техники поддержки.

Обозначены и проработаны первейшие необходимые «навыки» как: умение быстро диагностировать простейшие неполадки в системах транспорта, набор действий для ликвидаций критичных проблем:

- проведён анализ и выделены разъяснения касательно умения диагностировать. Обозначены конкретные пункты для достижения требуемого уровня машинам путём многоразовых тестов, работы над простейшими механизмами транспортных систем, возможность функционирования в недоступных для человека местах, как следствие снижение риска аварийных поломок;
- проведён анализ и разработаны теоретические основы касательно связи между ботами поддержки путём проводного соединения, сетевого (с использованием технологии Wi-Fi, Bluetooth) и скоординированной их работы в транспортных системах.
- проведён анализ и разработка единой базы данных для улучшения диагностики проблем транспорта и способы бесперебойного доступа роботам к ним.
- выделены и проанализированы условия при которых активируются данные боты и функционирование системы ручного их активирования в случае сбоя аварийной системы.

Труш І.Е.
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

СОЗДАНИЕ СПЕЦИАЛИЗИРОВАННОЙ БАЗЫ ДАННЫХ ДЛЯ КОМПАНИЙ

В докладе сделано анализ специализированных баз данных для компаний, распространённые требования различных компаний, касательно их реализации, дизайна, информации, которую будут они содержать и функциональность.

- Обозначены и проработаны первейшие необходимые навыки студента или частного подрядчика по реализации: умение работы с данными, знание английского языка, знания по специальности:
- проведён анализ и выделены разъяснения касательно умения работать с информацией. Обозначены конкретные пункты для достижения требуемого уровня студентом по знанию теоретического материала, путём тренингов осваивать на практике полученную теорию, саморазвитием в области создания баз данных;
- проведён анализ и выделены разъяснения касательно знания английского языка. Обозначены конкретные пункты для достижения требуемого уровня студентом по данному пункту образование в университете, чтение профильной литературы, выбор интересных источников и развивающих тренингов;

- проведён анализ и выделены разъяснения касательно знания по направлению, тренировок и практик, включение в задания лабораторных работ, работ, которые давались студентам компаниями во время проведения практик. Обозначены конкретные пункты для достижения требуемого уровня студентом (сертификация.

Сахарова София Владиславовна
Лобченко Надежда Юрьевна
Государственный университет телекоммуникаций
Учебно-научный институт телекоммуникаций и информатизации
г. Киев

ПЕРСПЕКТИВЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ БЛИЖАЙШЕГО БУДУЩЕГО: ИНТЕРНЕТ ВЕЩЕЙ, РОБОТИЗАЦИЯ И БЛОКЧЕЙН

На сегодняшний день Информатизация и Информационные технологии занимают в жизни людей очень важное место и становятся фундаментом новых качественных изменений в мире. Актуальным в наше время есть исследование информационных и коммуникационных технологий в национальной экономике Украины. Среди главных тенденций IT-сферы хочется отметить бурное развитие онлайн-платформ, которые фактически тут же создали новую бизнес-модель. Искусственный интеллект и машинное обучение, внедрение чат-ботов, а также технология blockchain — те точки, на которые ориентируются украинские стартапы. В данном тезисе будут рассмотрены перспективы IT ближайшего будущего.

Блокчейн: перспективы развития

Блокчейн (от англ. block и chain, «цепочка блоков») – распределенная база данных, потенциально доступная каждому. В блокчейне нет централизованного элемента, который мог бы управлять им и каким-либо образом вмешиваться в его работу.

Возможности Блокчейн:

- ✓ Хранение различных данных, которые верифицируются специальным оборудованием – майнерами.
- ✓ Механизм взаимодействия с приложениями на базе блокчейна напоминает работу с сервисом Google Docs, когда несколько человек обладают одновременным доступом к документу и могут наблюдать за его изменениями в режиме реального времени.
- ✓ Блокчейн – это общая, постоянно сверяемая, распределенная база данных.
- ✓ Сохранение авторских прав или же персональных данных.(например, применяя ее с биометрической защитой, пользователь может создать персональный ID, который невозможно будет подделать и это может стать заменой паспортных данных в будущем).
- ✓ Использование в торговле активами, и в голосованиях (в некоторых реалиях довольно актуальными являются честные результаты голосований, например, выборы в парламенте или президента).

Перспективы блокчейна в Украине:

Блокчейн – это однозначно прорыв. Но чтобы его внедрить необходимо провести реструктуризацию огромных систем с огромным количеством учасников. Таким образом, до регулирования блокчейна еще очень далеко.

Краткие выводы:

Сам по себе блокчейн – не панацея от бед украинского государства, а лишь способ более надежного хранения информации. Это, к слову, очень полезно, если речь шла бы о госреестре собственности.

Интернет вещей

Что такое Интернет вещей?

Интернет вещей (англ. «Internet of Things», IoT) – это группа устройств, взаимодействующих не только с пользователями, но и друг с другом.

IOT — концепция пространства, в котором все из аналогового и цифрового миров может быть совмещено – это переопределит наши отношения с объектами, а также свойства и суть самих объектов. © Роб Ван Краненбург.

Данная концепция зародилась относительно недавно – в 1999 году, но с тех пор изменилось многое. За относительно небольшой промежуток времени развитие IoT проделало путь от концепции, до практического применения в самых различных сферах жизнедеятельности человека.

Появление **интернета вещей** — это довольно ожидаемый шаг, ведь лень — двигатель прогресса. Зачем подходить к телевизору для переключения каналов, если можно придумать дистанционный пульт управления.

Согласно определению Глобального института McKinsey:

«Интернет вещей представляет собой класс устройств, которые могут контролировать окружающую их обстановку, сообщать о своем статусе, получать инструкции и действовать, опираясь на полученную информацию».

Краткие выводы:

Таким образом, IoT открывает по-настоящему широкие возможности, как для автоматизации бытовых и повседневных задач, так и для систем поддержки принятия решений и роботизации высокотехнологичных производств.

Роботизация

Машины теперь способны решать все больше процессов, за которые раньше отвечали люди. Кроме того, делают это качественнее и во многих случаях дешевле. Основным драйвером процесса автоматиции является применение искусственного интеллекта, работающего с большими данными, как более эффективной замены человеку.

Роботизация охватывает ту часть этой практики, когда на замену людям приходят физические механизмы.

Преимущества:

- ✓ одна из ключевых информационных технологий будущего
- ✓ наиболее успешное направление искусственного интеллекта, вытеснившее экспертные системы и инженерию знаний
- ✓ проведение функции через заданные точки в сложно устроенных пространствах
- ✓ математическое моделирование, когда данных много, знаний мало
- ✓ тысячи эффективно выполненных алгоритмов

Краткие выводы:

Работизация не только заберет у людей работу – благодаря ней также появятся новые профессии и даже индустрии. Из-за распространения роботов увеличится ценность во взаимодействии с людьми.

Литература:

Блокчейн:

1. https://newsone.ua/news/tekhnolohija-blokchejn-chto-eto-takoe-i-kak-ispolzuetsja-v-ukraine.html
2. https://forklog.com/blokchejn-i-iot-perspektivy-vzaimodejstviya-i-problemy-na-puti-razvitiya/

Интернет вещей:

1. https://geektimes.ru/post/149593/
2. https://forklog.com/blokchejn-i-iot-perspektivy-vzaimodejstviya-i-problemy-na-puti-razvitiya/

Роботизация:

1. https://habrahabr.ru/post/337870/
2. https://ain.ua/special/robots-vs-humans/

Бабій Д.

Державний Університет Телекомунікацій

Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ДОПОЛНЕННАЯ РЕАЛЬНОСТЬ

Технологии дополненной реальности сейчас активно развиваются. Сама по себе дополненная реальность (augmented reality, AR) представляет собой наложение виртуальных слоев, которые создал компьютер, на реальность обычную, в которой мы существуем. Самый показательный (и один из самых ранних) примеров дополненной реальности — «картинка», которую видел Терминатор из «Терминатора-2».

Сам термин был предложен в 1990 году сотрудником корпорации Boeing Томом Коделом. Идея дополненной реальности сейчас развивается даже более активно, чем идея виртуальной реальности.

Корпорация Apple провозгласила дополненную реальность трендом ближайшего и более отдаленного будущего. Компания встроила возможности AR в свою мобильную операционную систему, заявив, что отныне мобильные устройства неразрывно связаны с AR. Не исключено, что так и будет.

Сфер применения дополненной реальности очень много. Это и проектирование в дизайне, и спорт, и военное дело, медицина, и, конечно же, игры (как и вся сфера развлечения). По прогнозам объем рынка дополненной и виртуальной реальности вместе взятых увеличится до $150 млрд к 2020 году. Можно думать, что больше всего денег будет инвестировано в развлечения.

Сироткін Владислав Вікторович
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ІНТЕРНЕТ РЕЧЕЙ (IoT): МОДЕЛІ ВИКОРИСТАННЯ ОБМЕЖЕНОГО РАДІОЧАСТОТНОГО РЕСУРСУ

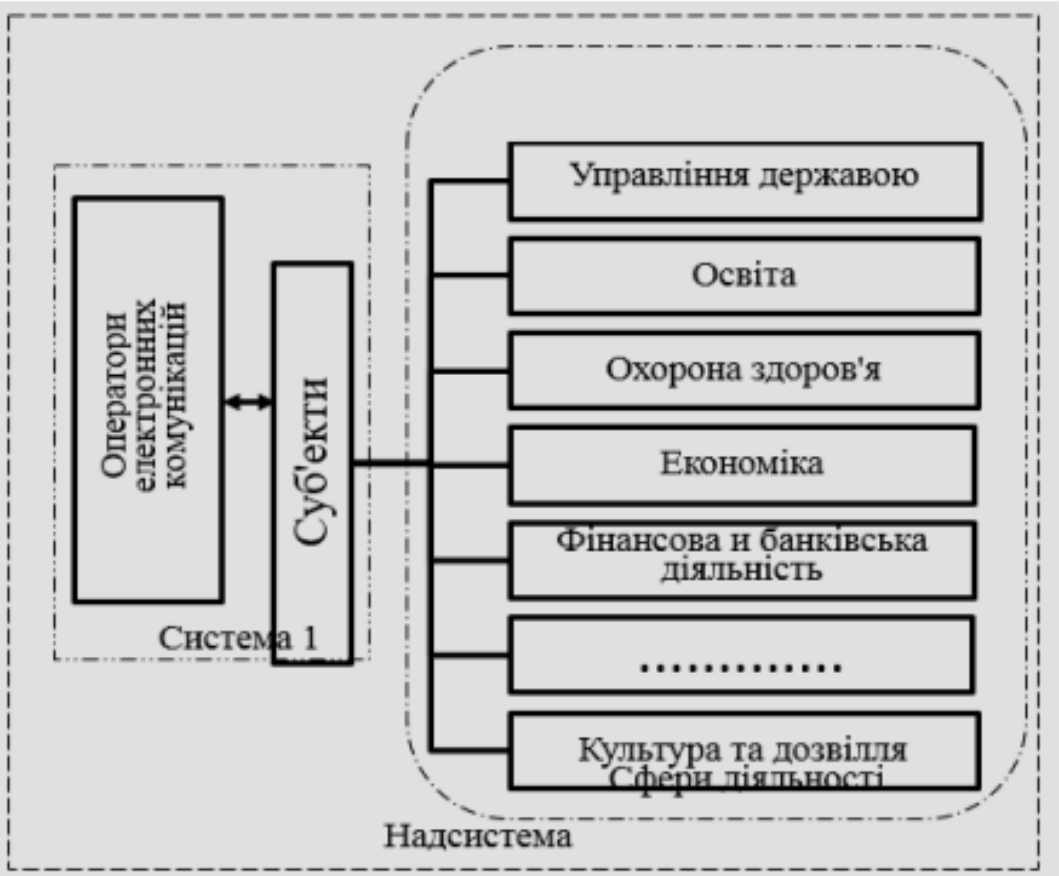
Аналізується генезис регулювання використання радіочастотного ресурсу для надання послуг електронних комунікацій. Досліджуються теоретико- методологічні засади формування моделей використання обмеженого радіочастотного ресурсу в умовах інтернету речей на основі вивчення соціальної моделі сфер діяльності суб'єктів з використанням послуг електронних комунікацій та соціальної моделі системи надання послуг електронних комунікацій.

В умовах широкого поширення технологій Інтернету речей (IP, Internet of Things, IoT), на думку експертів, кількість об'єктів, підключених до мережі Інтернет, до 2025 року може досягти 100 млрд, при цьому значна їх частина буде генерувати великий обсяг даних, що будуть передаватись за допомогою бездротових телекомунікацій. При цьому прогнозується, що трафік передачі даних мобільних операторів зросте на три порядки (в 1000 разів) отже, значно збільшиться навантаження на різні діапазони радіочастотного ресурсу (далі – РЧР), що призведе до різкого зростання актуальності вирішення проблеми ефективного користування обмеженим.

Протягом декількох десятиліть Міжнародний союз телекомунікацій (ITU), Європейський Союз, національні Адміністрації зв'язку та Національні регуляторні органи в сфері телекомунікацій (електронних комунікацій) докладають значних зусиль з пошуку шляхів вирішення проблеми забезпечення гармонізованого ефективного користування окремими діапазонами радіочастотного ресурсу. Як правило, раніше ці зусилля зводилися до проведення регуляторних (правових), організаційних, інженерних та інженерно-технічних заходів. Звичайно, перш за все пошук підвищення ефективності користування радіочастотним ресурсом спрямовується в технічному напрямі. Операторами електронних

комунікацій стали інтенсивно впроваджуватися нові радіотехнології, які мали кращі характеристики радіосигналів, що дозволяло передавати значні обсяги даних на одиницю спектра та надало потенційні можливості для обслуговування більшої кількості користувачів. Але задіяння технічного потенціалу не дозволило повною мірою вирішити проблему підвищення використання РЧР. Тому зростання протягом трьох останніх десятиліть споживчих очікувань і вимог до обсягу, переліку та якості послуг електронних комунікацій, що базуються на радіотехнологіях, стимулювало появу прогресивних бізнес-моделей діяльності операторів електронних комунікацій (далі – оператор) в частині користування окремими діапазонами РЧР. Результати аналізу наукових публікацій Дослідження в області ефективного використання радіочастотного ресурсу в сучасних умовах знайшли відображення в роботах ряду авторів і організацій: Forge S., Шалагінова А., ITU, Європейськиій парламент, Ofcom, Cisco, Qualcomm та інших.

Для даної теми досліджень соціальна модель, яка потребує вивчення – це соціальна модель системи надання послуг електронних комунікацій, а надсистемою є соціальна система сфер діяльності суб'єктів з використанням послуг електронних комунікацій як сукупність операторів електронних комунікацій, суб'єктів і сфер діяльності цих суб'єктів.



Малюнок 1. Соціальна модель сфер діяльності суб'єктів з користуванням електронних комунікацій

На малюнку 1 зображена соціальна модель сфер діяльності суб'єктів з використанням послуг електронних комунікацій (надсистема) зі складовим елементом – соціальною моделлю системи надання послуг електронних комунікацій (система 1).

У соціальній моделі (Мал. 1): суб'єкти – це будь-які фізичні або юридичні особи, які виявляють свою активність в різних сферах діяльності та можуть бути споживачами послуг електронних комунікацій.

Протягом близько 40 останніх років в рамках соціальної моделі (Мал. 1) діяльність операторів стільникових електронних комунікацій, які користуються РЧР, в основному була зорієнтована на надання послуг суб'єктам, які використовують поодинокі кінцеві пристрої (мобільні термінали). До кінця 90-х років минулого століття світовий ринок загальнодоступних послуг електронних комунікацій, в тому числі, мобільних електронних комунікацій (МЕК), розвивався в основному як ринок надання послуг голосової телефонії. Основною відмінною рисою соціальної моделі системи (Мал. 1) в ці роки була орієнтованість кожного оператора МЕК на власну самостійність (автономність) при наданні послуг своїм абонентам. З урахуванням останнього, бізнес-модель діяльності операторів МЕК відповідну соціальну модель системи 1 умовно назвемо "автономна". Виходячи з загальнодоступності послуг МЕК, «система» є системою масового обслуговування, тобто системою з однаковими номенклатурою, змістом і показниками якості послуг для всіх користувачів або їх окремих груп.

Слід зауважити, що виконання певних функцій в деяких сферах діяльності обумовлювало формування особливих вимог до показників якості послуг голосової телефонії. Але для цих випадків створювалися окремі, спеціальні мережі МЕК, які не належали до мереж загального користування. Під впливом широкого поширення комп'ютерних та Інтернет-технологій з 2000-го року став впроваджуватися розроблений Міжнародним союзом телекомунікацій (ITU) стандарт мобільного зв'язку 3G (3 покоління), який дозволив надавати користувачам набір послуг МЕК, що об'єднують як високошвидкісний мобільний доступ до мережі Інтернет, так і технологію радіозв'язку, яка формує канал передачі даних. Для бізнес-моделі "автономна", в переважній більшості випадків, показники надійності і стійкості роботи мережі мобільних електронних комунікацій не є критичними, як не є критичними випадки тимчасового припинення надання послуг для конкретного користувача або навіть груп користувачів. Також для оператора не є критичною проблема надійного забезпечення географічно суцільного покриття по всій території країни для забезпечення можливості надання послуг.

Кількість можливого кінцевого обладнання (мобільних пристроїв), задіяного в технологіях IP у одного споживача, може обчислюватися сотнями і десятками тисяч. Переривання надання послуг мобільних електронних комунікацій практично повністю виключається тому, що може призвести до зупинки діяльності, наприклад, руху автономного автомобільного транспорту.

Висновки. Аналіз сучасного ринку електронних послуг дає підстави для висновку про те, що вирішення проблеми задоволення кардинальної зміни користувацьких вимог до номенклатури, змісту та якості цих послуг стане можливим тільки за умови переходу від системи масового обслуговування "невимогливих" користувачів до створення "локальних" екосистем електронних комунікацій для окремих суб'єктів або їх груп. Пропонуючи вихід з ситуації, що склалася, коли в умовах вже розподілених діапазонів частот стало явно недостатньо ресурсу РЧР для розгортання перспективних радіотехнологій в інтересах технологій Інтернету речей.

Крім того, в преамбулі цього Рішення, відзначається, що торгівля правами на використання спектру в поєднанні з гнучкими умовами використання може істотно допомогти економічному зростанню, а смуги частот, в яких гнучке використання вже було введено законодавством Євросоюзу, повинні негайно стати предметом торгівлі в тому числі, для цих діапазонів радіочастот права користування могли б передаватися або здаватися в оренду. Тому в якості однієї з цілей політики в області радіочастотного спектру визначено створення бази для забезпечення можливості торгівлі правами на використання спектру, створюючи тим самим можливості для майбутніх цифрових послуг в масштабах всього ЄС.

Таким чином, з кінця нульових років XXI століття як у світі, так і в окремих національних державах, активізуються роботи за трьома основними напрямками

підвищення ефективності використання РЧР: гнучке спільне і гнучке колективне використання РЧР, а також торгівля правами на користування РЧР. При цьому, звичайно, стає актуальним створення правових умов для колективного і спільного використання окремих діапазонів радіоспектру, а також для торгівлі правами на його використування як в рамках законодавства національних держав, так і в міжнародному праві.

Использованая литература

1. Cisco visual networking index: global mobile data traffic forecast update, 2015 – 2020. Cisco White Paper, 2014. – Режим доступу : http://www.cisco.com/c/en/us/solutions/collateral/serviceprovider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf

2. The 1000x mobile data challenge. Qualcomm Presentation, 2013. – Режим доступу : http://www.qualcomm.com/media/documents/fils/1000x-mobile-data-challenge.pdf

3. Forge S. Perspectives on the value of shared spectrum access. Final Report. Support for the preparation of an impact assessment to accompany the Commission's Initiative on the Shared Use of Spectrum. 10 February 2012. – Режим доступу : https://ec.europa.eu/digital-singe-market/sites/digit alagenda/files/scf_study_shared_spectrum_access_20120210.pdf

3. *Constitution of the International Telecommunication Union (ITU). – Режим доступу : http://www.jus.uio.no/english/services/library/treaties/07/7-06/itu_const.xml#treaty-header1-1$; Convention of the International Telecommunication Union (ITU).*
4.

Пінчук Дар'я
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НАЙБЛИЖЧОГО МАЙБУТНЬОГО: БЛОКЧЕЙН, ІНТЕРНЕТ РЕЧЕЙ

За останні роки інформацію стали розглядати як один з основних ресурсів розвитку суспільства, а інформаційні системи та технології – як засіб за допомогою якого можна підвищити продуктивність праці та ефективність роботи окремого індивіда або персоналу в компаніях загалом.

Інформаційні системи та технології увібрали в себе майже всі досягнення електроніки, математики, фізики та економіки. Результат поєднання цих наук ознаменував революційний стрибок в історії інформаційних технологій, яка налічує тисячі років.

Блокчейн - це технологія, своєрідна розподілена база даних, яка підтримує перелік записів, так званих блоків і невпинно зростає, при цьому пристрої зберігання даних не є під'єднаними до спільного сервера . База надійно захищена від підробки та переробки. Кожен блок містить часову мітку та посилання на попередній блок хеш дерева (дерева Меркла).

Блокчейн технологія слугує бухгалтерською книгою для усіх економічних транзакцій електронної криптовалюти Біткоїн, описаної у 2008 році Сатосі Накамото, і представлений ним у 2009 році. Зараз Біткоїн називають "цифрове золото", бо на сьогоднішній день загальна цінність його валюти складає біля $18,8 млрд. Ця технологія передбачає і створення будь-яких інших електронних видів цінностей.

Блоки одночасно формуються безліччю «майнерів», а блоки, які задовольняють перевірочні критерії , відправляються в мережу, включаючись у розподілену базу блоків. Тобто коли є запит на проведення грошової транзакції ця операція передається до peer-to-peer мережі, яка складається з комп'ютерів- вузлів, вони перевіряють статус транзакції та після її підтвердження ця транзакція разом з іншими створює новий блок даних розподіленого журналу після чого цей блок додається до існуючого ланцюга блоків де стає постійним та незмінним.

Регулярно виникають ситуації, коли кілька нових блоків в різних частинах розподіленої мережі називають попереднім один і той же блок, тобто ланцюжок блоків може розгалужуватися. Навмисно чи випадково можна обмежити ретрансляцію інформації про нові блоки (наприклад, один з ланцюжків може розвиватися в рамках локальної мережі). У цьому випадку можливе паралельне нарощування різних гілок.

У кожному з нових блоків можуть траплятися як однакові транзакції, так і різні, що входять тільки в один з них. Коли ретрансляція блоків поновлюється, майнери починають вважати головним ланцюжок з урахуванням рівня складності хешу і довжини ланцюжка. При рівності складності і довжини перевага віддається тому ланцюжку, кінцевий блок якого з'явився раніше. Транзакції, що увійшли тільки у відхилену гілку, втрачають статус підтверджених.

Розподілена база даних Blockchain формується як безперервно зростаючий ланцюжок блоків з записами про всі транзакції. Копія бази даних або її частини одночасно зберігаються на безлічі комп'ютерів та синхронізуються відповідно до формальних правил побудови ланцюжка блоків. Інформація в блоках не шифрована і доступна у відкритому вигляді, однак захищена від змін криптографічно через хеш-ланцюжок.

Безумовною перевагою блокчейн-технології можна вважати те, що вона не може контролюватися кимось одним та не має єдиної точки відмови дій. Ця технологія являю собою вищу ступінь обліку та ідентифікації даних. Дозволяє не пропускати жодної транзакції та уникнути помилок зі сторони людини або змін без згод задіяних сторін.

Цю технологію використовують не лише як фундамент крипто валюти. Вона є досить привабливою для різних компаній працюючих у різних сферах діяльності. Наразі вже існує ряд різних додатків що базуються на блокчейні і які дозволяють: безпечно адмініструвати мережі знижуючи ризик хакерських атак, дозволяють фіксувати документи за часом аби вирішити проблему патентування та авторського права, підтверджувати справжність сертифікатів, документів, свідоцтв а також дозволяють безпечно проводити двосторонні угоди.

Поступово набирають популярності нові стартап-блокчейн проекти які вже через деякий час можуть суттєво змінити наше життя. Вони набирають популярність через те, що допомагають вирішувати ряд задач котрі люди виконують в повсякденному житті. Наприклад: зберігання важливих файлів, обмін валют, обмін документами між різними установами та організаціями, та інше. Ці стартапи використовують ланцюги блоків у якості базової платформи для розробки.

Одну з таких розробок можна частково віднести і до Інтернету речей. Ця розробка носить назву Sia. Головна ідея цього стартапу полягає в тому аби надати користувачу можливість зберігати свої дані повністю конфіденційно і максимально знизити ризик їх утрати, або ж надавати ключ лише тим кому потрібно через деякий час. Дані користувачів у Sia зберігаються у зашифрованому вигляді на великій кількості комп'ютерів на відміну від традиційних сервісів зі збереження даних Google Drive або Amazon S3 які зберігають дані сотень тисяч користувачів на власних серверах.

Варто зауважити що це є не безкоштовним і за зберігання своїх даних потрібно платити але ціна значно нижча ніж в інших хмарних сховищах такого типу.

Кожний новий користувач вступає в певну угоду з власниками Sia. Він надає місце на своєму комп'ютері на якому у зашифрованому вигляді будуть зберігатися дані інших користувачів. А його особисті дані після завантаження їх до розподільної мережі і розбиття на блоки і шифрування будуть таким самим чином зберігатися на комп'ютерах інших користувачів. Інформація котру ви завантажили дублюється і розміщується одразу на декількох комп'ютерах інших користувачів з тією метою якщо один комп'ютер буде не в мережі його завжди міг замінити інший. За надання місця на своєму девайсі кожен отримує плату. Вона залежить від кількості наданого місця та як довго ви зможете його надавати. У Sia є своя власна валюта Siacoin в якій і нараховуються виплати.

Зараз цей проект активно розвивається та має вже розміщений на усіх континентах окрім Африки. У майбутньому планується розширення та розповсюдження його й надалі.

Література:

1. *https://mining-cryptocurrency.ru/blockchain/#i*
2. *https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD*
3. *https://habrahabr.ru/post/330140/*

Гнатюк В.І.
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ

Виртуальная реальность — созданный техническими средствами мир , передаваемый человеку через его ощущения : зрение, слух, обоняние, осязание и другие. Виртуальная реальность имитирует как воздействие, так и реакции на воздействие. Для создания убедительного комплекса ощущений реальности компьютерный синтез свойств и реакций виртуальной реальности производится в реальном времени.

Объекты виртуальной реальности обычно ведут себя близко к поведению аналогичных объектов материальной реальности. Пользователь может воздействовать на эти объекты в согласии с реальными законами физики (гравитация, свойства воды, столкновение с предметами, отражение и т. п.). Однако часто в развлекательных целях пользователям виртуальных миров позволяется больше, чем возможно в реальной жизни (например: летать, создавать любые предметы и т. п.).

Не следует путать виртуальную реальность с дополненной. Их коренное различие в том, что виртуальная конструирует новый искусственный мир, а дополненная реальность лишь вносит отдельные искусственные элементы в восприятие мира реального.

Пінчук Дар'я
Савіцький В.А.
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ПЕРСПЕКТИВЫ МОБИЛЬНОЙ РАЗРАБОТКИ

В 2018 году Apple App Store и Google Play отметят свой 10-летний юбилей. С самого момента запуска этих магазинов мобильные приложения оказывали влияние на общество в невиданных темпах и масштабах. За это десятилетие индустрия приложений развивалась в нескольких направлениях:

На конец октября 2017 года в iOS App Store и Google Play предлагалось более 2 млн приложений и более 3,5 млн приложений соответственно. Кроме того, число новых приложений продолжает расти в геометрической прогрессии. В среднем за месяц в iOS App Store выходит около 50 000 новых приложений, а в Google Play добавляется свыше 150 000.

На зрелых рынках пользователи в среднем проводят по два часа в день— то есть месяц в году — в приложениях.

В 2017 году совокупный показатель потребительских расходов в iOS App Store и Google Play превысит $100 млн долларов в каждой стране со свободным доступом в интернет.

На сегодняшний день мобильные приложения играют ключевую роль практически во всех сферах, включая розничную торговлю , банковскую сферу, путешествия, рестораны и места общественного питания, товары широкого потребления, а также медиаиндустрию.

Кусяк О.В.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НАЙБЛИЖЧОГО МАЙБУТНЬОГО «ІНТЕРНЕТУ РЕЧЕЙ»

«Світ майбутнього, який ми бачимо в кіно неможливе без інтернету речей.»

Інтернет речей – одна з найпопулярніших концепцій в сучасній футурології. І більш того, одна з тих небагатьох, що вже перестають бути концепціями і втілюються в життя.

Концепція передбачає, що інтернет речей здатний серйозно вплинути на розвиток сучасного суспільства, оскільки дозволить багатьом процесам відбуватися без участі людини.

Інтернет речей значно трансформує особисті та соціальні аспекти життя, а також бізнес і навіть цілі галузі. Також ця технологія має потенціал вирішити деякі глобальні проблеми сучасності.

Наприклад, в Австралії вже зараз за допомогою переносних датчиків лікарі можуть віддалено відслідковувати стан здоров'я пацієнтів і реагувати в режимі реального часу. А мобільний оператор AT&T у США розробив систему, яка допомагає вирішити одну з найнебезпечніших проблем для літніх людей - несподівані падіння. Невеликий пристрій автоматично визначає різку зміну положення тіла власника і зв'язується з колл-центром для надання негайної допомоги. Навіть таке «нішеве» IoT-рішення істотно покращує якість життя людей.

За допомогою інтернету речей, життя буде полегшуватися у побутовому плані, тобто ми зможемо економити свій дорогоцінний час, витрачаючи його на щось більш важливе для нас, бо час неможливо придбати, або змінити, час це саме те, чого не вистачає кожному із нас.

Вінт Церф, віце-президент компанії Google, вважає, що різна техніка взаємодіятиме між собою, покращуючи якість нашого повсякденного життя. Але існує ризик того, що зловмисники можуть отримати контроль над технікою і спричинити серйозні проблеми. Великого розвитку досягне штучний інтелект. Приватне життя стане складно залишати закритим. Отже, для розвитку Інтернету речей слід буде вирішити питання стандартизації та інформаційної безпеки. Взаємодія з технікою вийде за межі кнопок та сенсорів і включатиме голос та жести. Комп'ютер буде здатен автоматично аналізувати обстановку: визначати об'єкти у полі зору, будинки, людей та інші об'єкти навколишнього середовища. Безперервний моніторинг буде великою частиною нашого життя: моніторинг показників здоров'я, навколишнього середовища, охорона та захист, рух транспорту, витрати ресурсів.

Пер Ола Крістенсон, лектор університету св. Ендрю, Англія, бачить майбутнє в широкому розвитку функціональності гаджетів, але сумнівається, що буде можливо керувати ними безпосередньо за допомогою мозку. «У 2025р. ми будемо здатні вводити текст в мобільні пристрої так само швидко як зараз вводимо на великій клавіатурі персонального комп'ютера. Сенсори на одязі та можливість гаджету слідкувати за поглядом користувача будуть використовуватись для того, щоб знати, де користувач знаходиться, що він робить і чим можна йому допомогти, якщо потрібно. Звичайно, будуть досконаліші сенсори, досконаліші алгоритми машинного навчання, і як наслідок, краща і зручніша взаємодія із технікою».

Для того, щоб реалізовувати потенціал Інтернету речей потрібна тісна співпраця бізнесу, телеком-операторів, урядів і навіть простих користувачів підключень.

ВИСНОВКИ:

Отже, інтернет речей розвивається з кожним днем, та в результаті відкриє новий світ для людей, у якому будуть слуги-роботи, незамінні гаджети для здоров'я та повсякденного життя, будинки з дистанційним керуванням, та багато іншого, що змінить життя усього людства.

Література :

1. *«Лекторій. Що таке інтернет речей і навіщо він потрібен?» Олексій Бондарев* https://nv.ua/ukr/science/lectures/lektorij-shcho-take-internet-rechej-i-navishcho-vin-potriben-1326653.html
2. *«Інтернет речей перетворює звичні для нас речі у нові пристрої, створюючи як розумні годинники, так і розумні міста.»* http://thefuture.news/iot/
3. *Цитати Пера Ола Крістенсона – лектора університету св. Ендрю.*
4. *Цитати Вінт Церфа – віце-президента компаній Google.*

Кусяк О.В.

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій та інформатизації

Факультет Інформаційних технологій

м. Київ

ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НАЙБЛИЖЧОГО МАЙБУТНЬОГО «РОБОТИЗАЦІЇ»

«Зовсім скоро, головним, а може, і єдиним засобом виконання всіх наших життєвих завдань стануть комп'ютери.»

Багато вчених в цьому свято переконані. Їх аргумент простий: прориви в сфері робототехніки і штучного інтелекту дозволить автоматизувати різні види праці. Безпілотні автомобілі замінять водіїв таксі та вантажівок, програмне забезпечення замінить юристів і бухгалтерів. Людство ударними темпами рухається до того моменту, коли практично всю роботу будуть виконувати за людину машини.

Зростаючий останні кілька років група вчених змушує повірити в неминучість такого сценарію.

Пітер Фрейзе поділився своїм баченням ситуації в книзі «Four Futures: Life After Capitalism». Два пекла, два раю: він вважає, що у людей будуть як два способи, щоб відмінно вдосконалити своє життя, так і два способи, щоб успішними темпами перетворити своє існування в пекло. Причому, і в тому, і в іншому випадку обов'язковим атрибутом кардинальних змін стане повна автоматизація виробництва. Змінюватися буде лише політичний або екологічний фон, іншими словами, хто стане власником роботів і як зміна клімату вплине на ресурси, від яких багато в чому залежить і виробництво технологій.

З кожною новою технологічною революцією, прогрес кидає людству виклики. До 2020 року ринок смарт-роботів досягне $ 7,85 млрд, а його сукупний темп зростання складе 19,22% в період між 2015 і 2020 роками. Дослідники прогнозують, що роботизація призведе до розколу суспільства: по одну сторону виявляться кваліфіковані професіонали - інженери і розробники, а по іншу - низькокваліфікований персонал. Саме про таке суспільство і його проблемах писав Курт Воннегут в романі «Механічне піаніно» ще в 1952 році.

Согласно Воннегуту, рабочие, которые потеряли свою работу из-за автоматизации, не готовы лишь потреблять блага цивилизации, которыми щедро одаривает их прогрессивное общество — роботы отняли у них не только рабочие места, но и возможности самореализации. Бывшие рабочие затевают восстание, которое, правда, ни к чему не приводит.

ВИСНОВКИ :

Роботизація несе за собою велику відповідальність перед суспільством, і якщо все таки роботизація захопить усі світові підприємства разом з робочими місцями, та позбавить людей джерел доходу ще до того, як з'являться нові професії в перспективі, то єдиним вихідом буде швидко навчити людей новим навичкам, поки не стало надто пізно.

Література :

1. *«Какое будущее подарит миру роботизация — 4 сценария»; http://ktovkurse.com/a-vy-kurse/kakoe-budushhee-podarit-miru-robotizatsiya-4-stsenariya .*
2. *Peter Frase «Four Futures: Life After Capitalism»*
3. *«Роботизация 2017: когда машины отберут у людей работу» https://hightech.fm/2017/01/08/robots*
4. *Глава Банка Англии: «Технологическая революция лишает людей работы» https://hightech.fm/2016/12/08/mark_carney*

Кусяк О.В.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НАЙБЛИЖЧОГО МАЙБУТНЬОГО «БЛОКЧЕЙНА»

«Завдяки блокчейну вся економічна діяльність людини може бути перебудована.»

З появою і розвитком технології блокчейн починають швидше еволюціонувати традиційні галузі. Електронна комерція, ринок нерухомості, юридичні послуги - всюди починає з'являтися блокчейн. На основі цієї технології компанія Amazon.com надає послуги логістики, консультування і навіть доставки на наступний день після замовлення.

Можливості блокчейна в сучасному світі практично не обмежені. Повсюдне впровадження цієї технології призведе до перебудови економіки та суспільства. Розробники отримують зараз карт-бланш, оскільки саме вони будуть створювати прикладні рішення, експериментуючи з блокчейном.

Наприклад, електронний нотаріус Stampery запевняє угоди за допомогою блокчейна. Сервіс Ascribe допомагає художникам і іншим творчим людям підтвердити своє авторство за допомогою блокчейна. Стартапи начебто Civic і UniquID Wallet дозволяють людям за допомогою блокчейна і біометричного захисту створювати цифрові ID, які неможливо підробити і які в майбутньому можуть замінити звичайні посвідчення особи.

ВИСНОВКИ :

Блокчейн зміг перебудувати економіку Світу та вивести її на новий рівень, де учасники ринку можуть обходитися без посередників, блокчейн дозволяє розробити «розумні» контракти, які будуть складатися, відправлятися і підписуватися учасниками угоди в автоматичному режимі. Зараз ми маємо зв'ярок з такими сервісами як Ebay або Uber, сервіси блокчейна набирають велику популярність та повагу серед користувачів, за блокчейном є майбутнє.

Література :

1. *Блокчейн — прошлое, настоящее и будущее // http://cognitive.rbc.ru/blockchain-future*
2. *Блокчейн, его перспективы и долевая экономика https://habrahabr.ru/company/ibm/blog/316230/*
3. *Что такое блокчейн, и как это работает // Женя Щербань // https://revolverlab.com/how-its-works-blockchain-6d0355c43bfc*

Гречана Ольга Віталіївна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НАЙБЛИЖЧОГО МАЙБУТНЬОГО

Інтернет речей концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку.

Роботизація здатна звільнити людини. З одного боку, звільнити з роботи, від зарплати, з іншого - розкрити його творчі здібності.

Блокчейн як вічний цифровий розподілене журнал економічних транзакцій, який може бути запрограмований для запису не тільки фінансових операцій, але і практично всього, що має цінність.

Література :

1. *https://cyberleninka.ru/article/n/vozmozhnosti-ispolzovaniya-blokcheyna-i-virtualnyh-tokenov-v-tamozhennyh-operatsiyah?gclid=CjwKCAjwwbHWBRBWEiwAMIV7E9BBmGepKKXY8Dyr3LiS3dd5cuS58lM5Fd811mW903vEO5nFEhZrVxoCWpMQAvD_BwE*
2. *https://uk.wikipedia.org/wiki/Інтернет_речей*
3. *https://nv.ua/ukr/science/lectures/lektorij-shcho-take-internet-rechej-i-navishcho-vin-potriben-1326653.html*
4. *https://ru.tsn.ua/nauka_it/globalnaya-robotizaciya-planety-chem-grozit-chelovechestvu-iskusstvennyh-intellekt-1065800.html*

Читулян Вадим Олегович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

РОБОТИЗАЦІЯ

Важливим засобом інтенсифікації виробництва є роботизація, тобто застосування у виробництві промислових роботів.

Інтенсифіка́ція - процес суспільного виробництва, що ґрунтується на найбільш повному та раціональному використанні технічних, матеріальних, природних, фінансових і трудових ресурсів на базі науково-технічного прогресу. Інтенсифікації виробництва досягають удосконаленням функціонування всіх основних процесів, що беруть участь у відтворенні сукупного суспільного продукту. Інтенсифікація виробництва є поєднання передових методів господарювання та досягнень науково-технічної революції; вдосконалення структури, галузевих, міжгалузевих і територіальних пропорцій виробництва.

Промисловий робот — це технічний пристрій, призначений для виконання комплексу виробничих операцій в автоматичному режимі.

У виробництві застосовується велика кількість різновидів і типів роботів і робототехнічних комплексів від найпростіших до складних інтелектуальних роботів, здатних самостійно приймати рішення на основі отриманої інформації у складних виробничих умовах, адаптуватися до змін у навколишньому середовищі. У роботах і робототехнічних комплексах знайшли застосування останні досягнення інформаційної техніки: пристрої і система сприйняття інформації, цифрові пристрої і мікропроцесори для перетворення і обробки інформації, приводи робочих органів з цифровим програмним керуванням, сучасні програмні засоби. Для робототехнічного виробництва характерним є те, що виробництво здійснюється без участі або майже без участі людини. Застосування

роботів дає змогу звільнити людину від важкої одноманітної праці, від роботи у шкідливих для організму умовах, а також у недоступних для людини середовищах.

Адаптивні роботи в ході виконання технологічної операції залежно від обставин можуть перепрограмовуватись (адаптовуватись) автоматично. Наприклад, якщо до верстата надійшла заготовка, що має відхилення від розмірів, робот відбраковує її та бере іншу.

Інтелектуальні роботи є найдосконалішими. Вони можуть аналізувати ситуації, приймати рішення, розв'язувати задачі, навчатися. Їх називають роботами зі штучним інтелектом. Такі роботи можуть застосовуватися для дослідження космосу, океану, використовуватися в зонах високого радіаційного забруднення та ін.

Нині такі роботи набувають широкого застосування. Вони дають змогу виготовляти продукцію високої якості, знижувати її собівартість, виконувати різні виробничі операції в недоступних місцях, самостійно аналізувати виробничі або технологічні операції та ухвалювати потрібні рішення. За такими роботами майбутнє.

Висновки

Одним з найголовніших факторів науково-технічного прогресу в наш час є висока комп'ютеризація, автоматизація і роботизація виробництва. Комп'ютери стали незамінними і надзвичайно популярними засобами для обробки інформації, але самі вони появилися лише тоді, коли електроніка як наука почала інтенсивно поширювати свої знання, які мусіли перейти в практику.

Література :

1. *Лекція про роботизацію сучасного виробництва, види та функції роботів.*
2. *Синтез робототехнічних систем в машинобудуванні: підруч. для студентів вищ. техн. навч. закл., які навчаються за спец. 015 «Проф. освіта. Машинобудування»: присвяч. 100-річчю Вєтрова Ю. О., ректора Київ. інж.-буд. ін-ту, зав. каф. буд. машин / Л. Є. Пелевін, К. І. Почка, О. М. Гаркавенко та ін. ; М-во освіти і науки України, Київ. нац. ун-т буд-ва і архітектури. — Київ: ТОВ НВП «Інтерсервіс», 2016. — 258 с. : іл. — Бібліогр.: с. 257 (16 назв). — ISBN 978-617-696-447-6*

Тертична Юлія Михайлівна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

БЛОКЧЕЙН (BLOCKCHAIN)

Блокчейн, тобто ланцюжок блоків транзакцій (англ. Blockchain, Block chain від block — блок, chain — ланцюг) — розподілена база даних, яка підтримує перелік записів, так званих блоків, що постійно зростає. База захищена від підробки та переробки. Кожен блок містить часову мітку та посилання на попередній блок хеш дерева. Як відомо, блокчейн – це база даних, що від початку створена для проведення фінансових операцій. Для збереження інформації вона використовує не один загальний сервер, а одразу багато різних. При цьому інформація зберігається у спеціально структурованих блоках. Кожен блок «посилається» на попередній, надаючи таким чином доступ не тільки до власної інформації, але і до тієї, що зберігається у попередньому блоці. Непомітно змінити дані в одному з них не вийде – система одразу визначить, що вони відрізняються від даних у інших блоках та повідомить про це.

Разом з цим система постійно перевіряє дані в блоках, і, якщо вони змінюються, наприклад, внаслідок проведення якої-небудь трансакції – сповіщає про це, водночас записуючи нову інформацію в новий блок. Таким чином блокчейн є сам собі бухгалтером. Він відслідковує усі фінансові операції, в режимі реального часу сповіщає про всі зміни і

при цьому не допускає помилок або умисних маніпуляцій з цифрами – по суті, це і є ідеальний бухгалтерський облік.

Про необхідність впровадження блокчейну в бухгалтерську практику експерти говорять вже зараз. Це тренд, який повільно, але впевнено набуває популярності. Зокрема, в США обговорюються можливості використання цієї технології державними регуляторами для контроля фінансових операцій. У свою чергу експерти, в тому числі з IFAC (International Federation of Accountants – Міжнародна Федерація бухгалтерів), вже попереджають, що спеціалісти, здатні складати звітність через систему блокчейн, незабаром будуть цінуватися вище, ніж бухгалтери, що працюють з традиційними програмами бухобліку.

Висновки

Наразі сама екосистема ще досить невелика, але це вже екосистема, і вона стрімко розвивається. До розробників долучились юристи, аналітики, підприємці, держави, бізнеси не з IT-середовища та багато інших.

Підсумовуючи, хочеться сказати ще про таке:

- Blockchain як технологія вже відбулась, а процес змін вже почався, і він незупинний. Питання тільки в тому, хто перший в цьому буде найкраще розбиратись?
- Блокчейн — це технологія, яка дозволяє реалізовувати найстійкіші цифрові реєстри в світі. Увага: це рішення доступне БУДЬ-ЯКІЙ людині чи об'єкту з доступом до інтернету та практично безкоштовно. Корпорації та держави витрачають мільярди доларів для забезпечення цілісності своїх даних.
- Трансконтинентальні корпорації намагаються знайти застосування технології в своїх процесах, так як це справді може економити їм сотні мільйонів доларів щороку.
- Наразі відбувається стрімка адаптація технології до традиційних секторів економіки.
- Кількість успішних стартапів у цій сфері в десятки разів більша, ніж в традиційному IT.
- Бази даних публічних блокчейн не підконтрольні жодній з організацій чи держав. Запис в публічні блокчейни доступний абсолютно кожному. Варто тільки мати незначну технічну підготовку.
- Використання Blockchain дуже часто зводить нанівець потребу в посередниках. Держави розглядають та ухвалюють законодавчі ініціативи в цьому напрямку. Стенфорд, Гарвард та інші ТОП-університети світу почали з 2016 року активно вивчати Bitcoin та Blockchain. Принципи, закладені в технологію, — надзвичайно сильні, що є запорукою подальшого розвитку.

Світ невпинно глобалізується. Інтернет та технології є фундаментом цього руху. Блокчейн — це наступна фундаментальна технологія, що виведе процес на якісно новий рівень.

Література :

1. *Melanie Swan. Blockchain: Blueprint for a New Economy. — 2015. — 152 p..*
2. *Pedro Franco. Understanding Bitcoin: Cryptography, Engineering and Economics. — John Wiley & Sons, 2014. — 288 p.*
3. *Andreas M. Antonopoulos. 7. The Blockchain // Mastering Bitcoin. — 2014.*
4. *Nakamoto, Satoshi (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org.*

Читулян Вадим Олегович

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій та інформатизації

Факультет Інформаційних технологій
м. Київ

ІНТЕРНЕТ РЕЧЕЙ (INTERNET OF THINGS)

Інтернет речей (англ. Internet of Things, IoT) — об'єднання будь-яких об'єктів (речей) в мережу для покращення їхньої функціональності. Найкраща ілюстрація — система «розумного будинку», здатна самостійно підтримувати комфортну температуру, вологість та інші характеристики середовища. Спеціальні датчики дозволяють виміряти поточні показники, а далі система вмикає кондиціонер, термостат, зволожувач повітря або інші прилади — з потрібними налаштуваннями.

Автор терміну «Internet of Things» — «піонер технологій» Кевін Ештон. В кінці 1990-х Ештон вивчав RFID — радіочастотну ідентифікацію. Ця технологія дозволяє кріпити на предмети маленькі мітки, що містять важливу інформацію і дозволяють зчитувати її на відстані.

RFID-мітки можна побачити, приміром, на товарах в магазині. Це маленька наліпка або ж мітка в пластиковому корпусі. В будь-якій формі вона дозволяє, наприклад, запобігти крадіжкам: якщо товар з активною міткою наближуаться до сенсора, встановленого на виході, звучить сигнал тривоги.

У 1999 році Кевін Ештон, працюючи в компанії Procter & Gamble, запропонував своєму керівництву використовувати радіочастотні мітки, щоб створити покращену систему управління поставками. Пояснюючи ідею, він скористався терміном «інтернет речей».

Використання і перспективи.

Концепція інтернету речей дуже широка. Немає чіткого списку приладів, для яких можна застосувати цей підхід. Це можуть бути побутові прилади: пральна машинка, якою можна керувати онлайн, або холодильник, що сам напише список продуктів і замовить доставку. Ще один варіант — гаджети, котрі можна носити: фітнес-трекери, «розумні» годинники. Також до інтернету речей відносять автомобілі та інший транспорт з системою автопілоту — такі, що можуть їздити без водія.

Гаджет може під'єднуватись до глобальної мережі Інтернет або ж «співпрацювати» з іншими приладами, що знаходяться поряд. Так виникають системи «розумного» будинку або ж цілого «розумного» міста. Вже зараз інтернету речей приділяється увага на найвищому рівні, зокрема починаючи з 2009 року у Брюселі при підтримці Єврокомісії проходять конференції Annual Internet of Things, на який виступають з доповідями єврокомісари, науковці та керівники провідних IT-компаній. За прогнозами аналітиків у найближчі роки очікується справжній бум інтернету речей. Так, за прогнозами Gartner, до 2020 року кількість підключених до всесвітньої мережі пристроїв становитиме 26 мільярдів, а дохід від продажу устаткування, програмного забезпечення та послуг становитиме 1,9 трлн дол. Деякі інші аналітичні агентства висловлюють ще більш оптимістичні прогнози. Найбільші світові IT компанії вже почали перегони за лідерство на цьому ринку. Так корпорація Intel у 2014 році після випуску «HYPERLINK "https://uk.wikipedia.org/wiki/Intel_Edison"SoCHYPERLINK "https://uk.wikipedia.org/wiki/Intel_Edison" HYPERLINK "https://uk.wikipedia.org/wiki/Intel_Edison"EdisonHYPERLINK "https://uk.wikipedia.org/wiki/Intel_Edison"» оголосила конкурс «Make it Wearable» з призовим фондом $1,3 млн на найкраще застосування своєї системи для концепції IoT та створила власний підрозділ «Internet of Things Solutions Group» для розвитку цього напрямку. Компанія «HYPERLINK "https://uk.wikipedia.org/wiki/Google"GoogleHYPERLINK "https://uk.wikipedia.org/wiki/Google"» на початку 2014 року за 3,2 млрд доларів купила невелику фірму «Nest Labs», яка займається випуском інтелектуальних термостатів. Спеціалісти цієї компанії займались впровадженням на американському ринку технологій IoT. Виробники побутової техніки також працюють у цьому напрямку. Так на

виставці CES 2014 у Лас-HYPERLINK "Вегасі була представлена велика кількість побутової техніки (холодильники, телевізори, пральні машини) з можливістю підключення до інтернет. Значення на ринку прогнозується на рівні 80 мільярдів доларів. Лідерами у розробці та впровадженні інтернету речей є країни, в який розвинена індустрія виробництва мікропроцесорів та вбудованих комп'ютерів — це США, Китай, Південна Корея. Також значний прогрес у цій галузі демонструють європейські країни та Японія.

Література :

1. *The 2nd Annual Internet of Things 2010*
2. *Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020*
3. *Інтернет речей: друг чи ворог?*
4. *The Future News*

Андрющенкова Стелла Олександрівна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ПЕРСПЕКТИВИ БЛОКЧЕЙНА В УКРАЇНІ

Застосування блокчейну знайшлося не тільки в кріптовалютной індустрії.

Досить поширеним стає таке поняття, як смарт-контракт.

Винахід - справжня знахідка для юриста.

Основна особливість в тому, що контракт містить в собі інформацію, а точніше, правила його виконання. Поки одна сторона не виконає всі умови іншого боку, він не буде виконаний.

Перспективи блокчейна в Україні

Блокчейн - це однозначно прорив. Але в ньому є й невеликий негативний відтінок. Щоб його впровадити необхідно провести реструктуризацію величезних систем з величезною кількістю учасників. Одночасно ввести його в усіх сферах діяльності - неможливо.

Більш того, до централізованого регулювання блокчейна державою ще дуже далеко.

Головною складністю в цьому є підлаштування законодавства під єдиний стандарт і той факт, що для підтримки блокчейна потрібна наявність величезної кількості обчислювальних потужностей і електроенергії.

Україна абсолютно раптово для всіх стала одним з передових країн по впровадження блокчейн на державному рівні.

У вересні 2017 року СЕТАМ (Система електронних торгів арештованим майном). Більш того, починаючи з жовтня 2017 року розпочався переклад на блокчейн Державного земельного кадастру.

Фактично блокчейн робить повністю неможливим фальсифікацію і підробку інформації таким чином, щоб дані про це не залишали по собі «цифровий слід».

Крім того, блокчейн вже зараз дозволяє перевіряти правдивість отриманих з кадастру виписок. У перспективі ця технологія передбачає переклад на блокчейн транзакцій і збереження даних.

За задумом блокчейн повинен допомогти в подоланні так званої кризи довіри суспільства до державних реєстрів, який виник через випадки рейдерства, коли чиновники могли змінювати дані про власника землі або бізнесу.

Бердник Ірина Ігорівна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації

Факультет Інформаційних технологій
м. Київ

ПЕРЕВАГИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ «ІНТЕРНЕТ РЕЧЕЙ»

У 2008 р. число пристроїв, приєднаних до Інтернету перевищило число населення Землі. У 2013 р. таких пристроїв було 13 мільярдів. Це число росте на даний час. Згідно з Cisco, у 2020р. таких пристроїв буде 50 мільярдів, включаючи телефони, чіпи, сенсори, імплантати, і т.п. Способи взаємодії з технікою будуть покращуватись, особливо голосові команди та управління дотиком. Деякі експерти навіть передбачають, що у 2025 р. звичайною річчю буде безпосередній зв'язок мозку з Інтернетом. Особливої популярності набуває технологія Інтернет речей.

Технології, які дозволяють реалізувати Інтернет речей, вирішують чотири основні задачі: ідентифікацію, збирання даних, зберігання даних та обмін інформацією:

Інтернет речей буде розвиватись і поширюватись у майбутньому, а також потенційно може змінити багато навколишніх об’єктів, включаючи:

- тіла/одягу: люди носитимуть прилади, що дозволятимуть їм з’єднуватися з Інтернетом і повідомляти про їхню діяльність, показники здоров’я тощо. Вони також дозволятимуть слідкувати за іншими людьми (дітьми, найманими працівниками, тощо), хто також носить різні сенсори або знаходиться в місці де навколо є ці сенсори;
- дім: люди зможуть контролювати вдома майже все дистанційно, температура в приміщенні може самостійно регулюватись в залежності від потреб мешканців, вазони самостійно поливатись, енергія використовуватись оптимально, і т.п. Розумний дім також зможе повідомити про будь-які негаразди: від незаконного проникнення в помешкання до аварії, викликаної проривом труби;
- комунікації: встановлені пристрої дозволятимуть ефективніше проводити рух транспорту, контролювати рівень забруднення, запобігатимуть інфраструктурним проблемам;
- товари та послуги: впровадження цих технологій на виробництві може покращити швидкість та якість виготовлення товарів та послуг:
- навколишнє середовище: буде можливість у реальному часі отримувати дані з полів, лісів, океанів і міст щодо рівня забрудненості, вологості повітря/ґрунту, дані про видобуток ресурсів і, взагалі, про будь-які дані навколишнього середовища, що зацікавлять.

Для розвитку Інтернету речей слід буде вирішити питання стандартизації та інформаційної безпеки. Взаємодія з технікою вийде за межі кнопок та сенсорів і включатиме голос та жести. Комп’ютер буде здатен автоматично аналізувати обстановку: визначати об’єкти у полі зору, будинки, людей та інші об’єкти навколишнього середовища. Безперервний моніторинг буде великою частиною нашого життя: моніторинг показників здоров’я, навколишнього середовища, охорона та захист, рух транспорту, витрати ресурсів.

Заріцька О.М.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

НАПРЯМКИ ПРАКТИЧНОГО ЗАСТОСУВАННЯ ІНТЕРНЕТУ РЕЧЕЙ

Ідея Інтернету речей (Internet of Things, IoT) сама по собі дуже проста. Уявімо, що всі навколишні предмети і пристрої (домашні прилади і посуд, одяг, продукти, автомобілі, промислове обладнання та ін.) забезпечені мініатюрними ідентифікаційними і сенсорними пристроями. Тоді при наявності необхідних каналів зв'язку з ними можна не тільки відстежувати ці об'єкти і їх параметри в просторі і в часі, а й управляти ними, а також включати інформацію про них в загальну «розумну планету».

Простіше кажучи, Інтернет речей - це глобальна мережа комп'ютерів, датчиків (сенсорів) і виконавчих пристроїв (актуаторів), що зв'язуються між собою з використанням інтернет протоколу IP (Internet Protocol). Наприклад, для вирішення певної задачі комп'ютер зв'язується через інтернет з невеликим пристроєм, до якого підключений відповідний датчик .

Очевидно, що при впровадженні Інтернету речей все наше повсякденне життя кардинально змінюється. Підуть в минуле пошуки потрібних речей, дефіцити товарів або їх перевиробництво, крадіжки автомобілів і мобільних телефонів, оскільки буде точно відомо, що, в якому місці і в якій кількості знаходиться, виробляється і споживається. Якщо всі об'єкти (речі) будуть забезпечені мініатюрними радіомітками, то їх можна буде дистанційно ідентифікувати, а при наявності певного «інтелекту» - і керувати ними.

На основі Інтернету речей можуть бути реалізовані всілякі «розумні» (smart) додатки в різних сферах діяльності і життя людини.

«Розумна планета» - людина зможе буквально «тримати руку на пульсі» планети: своєчасно реагувати на упущення в плануванні господарств, забруднення та інші екологічні проблеми, а значить, ефективно розпоряджатися невідновлюваними ресурсами.

«Розумне місто» - міська інфраструктура і супутні муніципальні послуги, такі як освіта, охорона здоров'я, громадська безпека, ЖКГ, стануть більш пов'язаними і ефективними.

«Розумний будинок» - система буде розпізнавати конкретні ситуації, що відбуваються в будинку, і реагувати на них відповідним чином, що забезпечить мешканцям безпеку, комфорт і ресурсозбереження.

«Розумна енергетика» - надійна і якісна передача електричної енергії від джерела до приймача в потрібний час і в необхідній кількості.

«Розумний транспорт» - переміщення пасажирів з однієї точки простору в іншу стане зручніше, швидше і безпечніше.

«Розумна медицина» - лікарі і пацієнти зможуть отримати віддалений доступ до дорогого медичного обладнання або до електронної історії хвороби в будь-якому місці, буде реалізована система віддаленого моніторингу здоров'я, автоматизована видача лікарських препаратів хворим і багато іншого.

Існуючий нині Інтернет речей приносить реальну користь більшості індивідуальним користувачам, компаніям і цілим країнам. Всесвітня мережа стимулює економічний ріст шляхом електронної комерції і пришвидшує інноваційні процеси в бізнесі, розвиваючи спільну працю. Інтернет допоміг удосконалити систему освіти за допомогою демократизації методів доступу до інформаційних ресурсів. Ми не можемо уявити наше повсякденне життя(робота, освіта, розваги і багато чого іншого) без інтернету. Але зараз ми вступаємо в епоху, коли новий Інтернет речей (Internet of Things, IoT) може радикально покращити життя кожного жителя нашої планети – допомогти у вирішенні кліматичних проблем, вилікувати тяжкі хвороби, удосконалити процеси ведення бізнесу і зробити кожен день нашого життя більш безтурботним і щасливим.

Література :

1. *ИНТЕРНЕТ ВЕЩЕЙ А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков*

Курочкіна М., Троценко Д.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ПІДКЛЮЧЕННЯ РЕЧЕЙ

Інтернет підключає не тільки настільні комп'ютери і ноутбуки. Навколо вас багато підключених до Інтернету пристроїв, з якими ви можете щодня взаємодіяти.

Наприклад, з кожним днем люди все активніше користуються мобільними пристроями для спілкування і виконання повсякденних завдань, в тому числі, щоб дізнатися погоду або виконати банківські операції онлайн. Клацніть елементи на малюнку 1, щоб дізнатися більше про мобільні пристрої.

У майбутньому багато речей у вашому домі теж можна буде підключити до Інтернету, щоб контролювати і налаштовувати їх віддалено. Клацніть елементи на малюнку 2, щоб дізнатися більше про підключених домашніх пристроях.

Також за межами вашого будинку є багато підключених пристроїв, які забезпечують зручність і надають корисну і навіть життєво важливу інформацію. Клацніть елементи на малюнку 3, щоб дізнатися більше про ці поширених підключених пристроях.

Для роботи Всеохоплюючої Інтернету потрібно, щоб всі пристрої, які є частиною одного рішення, були підключені один до одного, щоб мати можливість передавати дані. Пристрої можуть бути підключені двома способами: провідним і бездротовим.

У більшості випадків підключення пристроїв між собою за допомогою кабелів вимагає занадто багато коштів і зусиль, тому такий спосіб навряд чи можна назвати практичним. Саме тому більшість пристроїв буде відправляти і отримувати дані по бездротовому зв'язку.

Існує багато різних типів бездротового зв'язку. До найбільш поширених з них належать Wi-Fi, стільниковий зв'язок, Bluetooth і ближній безконтактний зв'язок (NFC). Деякі пристрої, в тому числі смартфони і планшетні комп'ютери, використовують відразу декілька методів бездротової комунікації для підключення до різних пристроїв.

Троценко Д., Курочкіна М.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ЕЛЕКТРОНІКА ТА ДАТЧИКИ

Згідно зі світовою статистикою Інтернету (Internet World Stats, www.internetworldstats.com) станом на червень 2012 року Інтернетом користуються 2,4 мільярда людей. І це лише 34% від усього світового населення.

У 2012 році кількість підключених до Інтернету пристроїв перевищила населення планети. Сюди входять традиційні обчислювальні і мобільні пристрої, а також нові промислові та побутові пристрої, які ми називаємо «речами».

Незважаючи на те, що подібне кількість пристроїв, підключених до Інтернету, здається приголомшливим, це менше 1% від усіх об'єктів, які можна підключити. Наприклад, на даний момент до непідключеним пристроїв відносяться мікрохвильові печі, будильники і системи освітлення.

Датчики - це один із способів збору даних з пристроїв, які не є комп'ютерами. Вони перетворять фізичні властивості нашого середовища в електричні сигнали, які можуть бути оброблені комп'ютерами. Як приклад можна привести датчики грунтової вологи, температури повітря, радіації і руху. Різні датчики зіграють важливу роль в підключенні до всеосяжного Інтернету тих речей, які раніше не були підключені.

Популярний тип датчиків використовує радіочастотні мітки (RFID-мітки). RFID використовує радіочастотні електромагнітні поля для передачі інформації між невеликими мітками з кодом (RFID-мітки) і радіочастотним зчитувачем. Як правило, радіочастотні мітки використовуються для ідентифікації та відстеження об'єктів, в які вони вбудовані, наприклад домашніх тварин. Оскільки ці мітки зовсім невеликі, їх можна прикріпити практично до будь-яких предметів, в тому числі до одягу і грошей. Деякі радіочастотні мітки не вимагають батарейок. Харчування, необхідне для передачі

інформації, мітки отримують від електромагнітних сигналів, які відправляє зчитувач радіочастотних міток. Мітка отримує цей сигнал і використовує частину її енергії для відправки відповіді.

Дальність передачі в моделях, представлених на малюнку, становить кілька метрів, тоді як інші радіочастотні мітки оснащені батареєю і функціонують в якості маяка, який може в будь-який час відправити інформацію по широкомовної розсилки. Діапазон такого типу радіочастотних міток зазвичай становить кілька сотень метрів. На відміну від штрихкоду такі мітки працюють на основі радіочастот, тому не вимагають лінії прямої видимості.

Завдяки своїй гнучкості і низьким вимогам до харчування радіочастотні мітки - це відмінний спосіб підключити пристрій, який не є комп'ютером, до вирішення Всеохоплюючої Інтернету за допомогою передачі інформації на зчитувач радіочастотних міток. Наприклад, сьогодні автомобільні заводи нерідко прикріплюють радіочастотні мітки до корпусів своїх машин. Це дозволяє їм відслідковувати просування автомобіля через складальний конвеєр.

Перше покоління радіочастотних міток характеризується одноразовим записом і багаторазовим зчитуванням. Це означає, що після того, як їх вперше запрограмують на заводі, їх конфігурацію можна буде змінити. Нові радіочастотні мітки володіють можливістю багаторазового запису і багаторазового зчитування. Вони оснащені мікросхемами, які служать від 40 до 50 років і можуть бути перезаписані більше 100 тисяч разів. Ці мітки можуть зберігати всю історію активу, до якого вони прикріплені, в тому числі дату виробництва, історію місцезнаходжень, цикли множинного використання і інформацію про власників.

Галушко І.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ІНТЕРНЕТ РЕЧЕЙ ТА ВСЕОХОПЛЮЮЧИЙ ІНТЕРНЕТ

Всеохоплюючий Інтернет призначений для об'єднання в мережу людей, процесів, даних і речей.

Інтернет Речей представлений у вигляді ринкового перехідного періоду, що використовує низькі витрати при підключенні речей до Інтернету. Отже, Інтернет Речей має на увазі фундаментальну зміну стану нашої поточної економіки на шляху до 2020 року, коли кількість підключених пристроїв на планеті досягне 50 мільярдів.

Однак Інтернет Речей - це лише один з кількох подібних перехідних періодів, які дозволять реалізувати повний потенціал Всеохоплюючої Інтернету. Наприклад, нижче представлені переходи, які також реалізують потенціал Всеохоплюючої Інтернету.

Мобільний зв'язок - надає доступ до ресурсів від будь-якого пристрою, в будь-який час і в будь-якому місці.

Хмарні обчислення - надають розподілені обчислювальні ресурси і сервіси по мережі.

Великі масиви даних - у міру збільшення вироблених обсягів даних ростуть і наші можливості для їх аналізу і обробки.

IPv6 - розширення поточного адресного простору в Інтернеті на 3,4 × 10 ^ 38 адрес дозволить нам легко вмістити 50 мільярдів пристроїв до 2020 року, і навіть набагато більше.

Користь, яку організація може отримати від Всеохоплюючої Інтернету, залежить від уміння застосовувати ці переходи, в тому числі хмарні обчислення, мобільний зв'язок та Інтернет Речей. Наприклад, Іван переходить до використання Smart Grid, рішення, яке реалізує переваги Всеохоплюючої Інтернету за рахунок поліпшення ефективності

використання енергії в електромережі, яка до того ж використовується в будинках і офісах.

Інтернет Речей націлений на підключення того, що ще не підключено, завдяки чому все більше речей стане доступним через Інтернет. Якщо розглядати Інтернет Речей разом зі Всеосяжним Інтернетом, то останній дає зрозуміти, навіщо взагалі варто підключати то, що ще не підключено.

Зільберштейн В., Шаговий А.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

УПРАВЛІННЯ ДАНИМИ В ІНТЕРНЕТІ РЕЧЕЙ

Як правило, комп'ютерів не вистачає контекстних знань і інтуїції, якими володіє людина. І тому необхідно розглядати два стану даних: структуроване і неструктуроване.

Структуровані дані вводяться і зберігаються в фіксованих полях всередині файлу або запису. Комп'ютер легко вводить, класифікує, шукає і аналізує структуровані дані. Наприклад, коли ви вводите на сайті свої ім'я, адресу та банківські дані, то створюєте структуровані дані. Завдяки особливій структурі певний формат для введення даних мінімізує кількість помилок і допомагає комп'ютеру інтерпретувати інформацію. На малюнку 1 показано, як різні типи даних зберігаються в конкретних місцях, де комп'ютер може їх знайти.

Неструктуровані дані організовані не так добре, як структуровані. Неструктуровані дані не оброблені. У них немає тієї складової, що ідентифікує значення даних. Неструктуровані дані не володіють особливим способом введення або угруповання даних для їх подальшого аналізу. До прикладів неструктурованих даних відносяться фотографії, аудіо- та відеофайли. На малюнку 2 представлена картина Рафаеля Афінська школа. Вміст картини, наприклад фігури і елементи, не піддається пошуку, оскільки не має структури.

Структуровані і неструктуровані дані - це активи, які мають цінність для людей, організацій, галузей і урядів. Як і інші активи, інформація, зібрана з структурованих і неструктурованих даних, володіє вимірюваноївеличиною. Однак цінність таких даних може збільшуватися або зменшуватися в залежності від способу управління ними. Навіть найбільш значущі дані з часом можуть втратити свою цінність.

Організації повинні вміти інтерпретувати будь-які форми даних (структуровані, неструктуровані та слабоструктуровані), а також визначити способи їх форматування для подальшого управління та аналізу.

Щоб зрозуміти принципи управління даними, необхідно вивчити такі концепції, як сховище і передача даних.

Стеценко О., Нагорна Н.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ІНТЕРНЕТ ПРОВАЙДЕРИ ТА АДРЕСАЦІЯ В ІНТЕРНЕТІ РЕЧЕЙ

У середовищах централізованих і розподілених сховищ дані повинні передаватися по мережі або Інтернету.

Пристрої, які пересилають дані по Інтернету, повинні робити це за допомогою інтернет-провайдера (Internet Service Provider, ISP) Інтернет-провайдер надає підключення, які забезпечують доступ в Інтернет рядовим користувачам і компаніям. Крім того, інтернет-провайдер може підключатися до інших постачальників Інтернету.

Мережі підключаються до інтернет-провайдера в точці присутності (Point of Presence, POP).

На підприємстві інтернет-провайдера між різними POP дані переміщує мережу високошвидкісних маршрутизаторів і комутаторів. Точки POP з'єднані між собою за допомогою декількох каналів, що забезпечує для даних альтернативні маршрути на випадок збою або перевантаження одного з каналів.

Якщо потрібно відправити інформацію за межі мережі інтернет-провайдера, то пакети пересилаються іншим інтернет-провайдерам. Як показано на малюнку, Інтернет складається з високошвидкісних каналів передачі даних, які з'єднують безліч інтернет-провайдерів між собою. Ці зв'язки є частиною дуже великий і ємною мережі, яка відома як магістраль Інтернету.

Пересилання пакетів через Інтернет повинна здійснюватися по протоколу IP. У кожному IP-пакеті повинен бути достовірний IP-адреса джерела і призначення. Без правильної адресної інформації пакети не досягнуть вузла призначення, а повернуті пакети не зможуть дійти до свого початкового джерела. Протокол IP визначає структуру IP-адрес джерела і призначення. Протокол визначає метод використання цих адрес при маршрутизації пакетів від одного вузла або мережі в інший (-у).

На сьогоднішній момент Інтернет використовує протокол IPv4 (четверту версію IP), але поступово переходить на IPv6 (шосту версію IP). IPv6 пропонує поліпшені можливості доступу і масштабованості, більше доступних IP-адрес і інші переваги.

IP-адреса схожий на поштову адресу людини. Він називається логічним адресою, оскільки привласнюється логічно (в залежності від місця розташування вузла). Цей процес схожий на призначення адреси вулиці на підставі логічного опису міста, селища або його околиць. Було б неможливо запам'ятати все IP-адреси всіх серверів, що надають різні послуги через мережу Інтернет. Замість цього пропонується більш простий спосіб пошуку серверів - зіставити ім'я з деяким IP-адресою. На малюнку показано, як сервери в Інтернеті перетворять ім'я www.cisco.com в IP-адресу, щоб визначити місце призначення.

Шевченко О.О.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

IoT

IoT - це термін, який використовується для онлайн-пристроїв, які збирають дані у нашій роботі та особистому житті. Blockchain - це зашифрована, розподілена комп'ютерна система реєстрації, призначена для створення захисних записів в реальному часі.
Об’єднааня їх в теорії, дає перевірений, безпечний і постійний спосіб запису даних, оброблених "розумними" машинами в IoT.

Існує декілька переваг ідеї побудови інтелектуальних машин, здатних спілкуватися та управляти через blockchain.

По-перше, існує проблема нагляду. З операціями з даними, що відбуваються між кількома мережами, що належать і управляються кількома організаціями, постійне, незмінне зберігання засобів запису може відслідковуватися, оскільки дані або фізичні товари проходять між точками в ланцюжку постачання. Записи blockchain за своїм характером є прозорими - активність може відслідковуватись та бути проаналізованою будь-ким, хто уповноважений для підключення до мережі. Якщо щось трапиться не так,

відбудуться пошкодження, то запис блокування дозволяє легко визначити слабкий зв'язок і вжити заходів для виправлення ситуації.

По-друге, використання шифрування та розподіленої бази даних означає, що ці дані будуть перевірені всіма сторонами, що беруть участь у ланцюжку постачання. Машини надійно фіксують інформацію про транзакції, що відбуваються між собою, без контродю людьми.

Без приватних ключів, що дають доступ до запису blockchain, ніхто не зможе переписати запис із неточною інформацією.

По-третє, можливості "старт контракту", надані деякими blockchain мережами, такими як Ethereum, дозволяють створювати угоди, які будуть виконуватися при виконанні умов. Це буде дуже корисним, коли мова йде, наприклад, про дозволення одній системі здійснити платіж, коли умови вказують на те, що надана послуга була надана.

По-четверте, blockchain дозволяє значно підвищити загальну безпеку середовища IoT. Значна частина даних, створених IoT, дуже персональна - наприклад, розумні домашні пристрої мають доступ до інтимних подробиць про наше життя та повсякденну роботу. Це дані, які необхідно надати іншими машинами та службами, щоб вони були корисними для нас. Але це також означає, що хакери маютимуть набагато більше можливостей для атаки на нас. Дозвіл доступу до даних з пристроїв IoT, що проводиться з використанням blockchain означатиме додатковий рівень безпеки, який ніякий злочинець не зможе обійти.

Blockchain та IoT - дві технології, які мають великий потенціал. Обидві вже широко використовуються. Поєднання їх може бути способом для мінімізації ризиків безпеки та бізнесу, що супроводжуються технологічними змінами.

Ковтушенко Р., Шулц В.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ДАННІ В РУСІ (DATA IN MOTION)

Як правило, ми розглядаємо дані в якості інформації, зібраної за певний проміжок часу. Наприклад, дані можуть бути зібрані в результаті різних операцій з обробки замовлень організації. Ці дані несуть для організації певну цінність і мають історичну природу. Це статичні дані, які ми називаємо «нерухомими».

Однак, внаслідок безперервного зростання великих обсягів даних, цінність багатьох з них втрачається практично так само швидко, як і створюється. Пристрої, датчики і відео постійно створюють нові дані. Ці дані мають цінність, поки з ними взаємодіють користувачі. Їх ми називаємо «даними в русі».

Поява нових можливостей для використання даних відкриває нові шляхи щодо вдосконалення світу - від рішення проблем зі здоров'ям у всьому світі до поліпшення системи освіти. Інтелектуальні рішення мають величезний потенціал зі збору, управління та оцінки даних зі швидкістю людського спілкування. В результаті скоро «дані в русі» займуть перше місце у Всеосяжний Інтернеті. Клацніть «Відтворення», щоб дізнатися, як корпорація Cisco може почати еволюцію даних у Всеосяжний Інтернеті.

Білощицький Є., Зубер Є.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ВЕЛИКІ ДАНІ В ІНТЕРНЕТІ РЕЧЕЙ

Рушійний фактор такого зростання обсягів інформації - це кількість пристроїв, підключених до Інтернету, а також кількість з'єднань між цими пристроями. Але це тільки початок. Кожен день до Інтернету підключається все більше нових пристроїв, що створює надлишок нового контенту.

Через такої великої кількості інформації організаціям необхідно навчитися не тільки управляти цими даними, але і управляти великими масивами даних.

Необхідно взяти до уваги три основні виміри великих масивів даних: обсяг, різноманіття і швидкість.

Обсяг - це кількість переданих і збережених даних. Різноманіття - це тип, до якого відносяться конкретні дані. І відповідно, швидкість - це швидкість переміщення даних. Дані не можуть переміщатися без інфраструктури. Швидкість інфраструктури (введення-виведення, пропускна здатність і затримка) і можливість негайно застосовувати оптимальні ресурси (мережа, ЦП, пам'ять і сховище) безпосередньо впливають на швидкість передачі даних.

Додатки для великих масивів даних отримують інформацію від безлічі різних джерел, включаючи ПК, смартфони, планшетні комп'ютери, машини, датчики, соціальні мережі та мультимедійні додатки. Як показано на малюнку, переважна частина цього зростання даних відбувається завдяки мобільним пристроям. За допомогою мобільного зв'язку користувач може взаємодіяти з будь-яким вмістом коли завгодно, де завгодно і з будь-якого пристрою.

Великі масиви даних - це процес збору та аналізу великих обсягів даних організаціями для того, щоб визначати тенденції, передбачати поведінку і надавати максимальні можливості тим, хто приймає рішення. При цьому враховується наступне:

Скільки даних створено.

Як ці дані ідентифікуються і управляються як актив організації.

Як ці дані перетворюються в корисну інформацію.

Як організації використовують дані для прийняття бізнес-рішень.

Запитайте себе, що відбувається, коли ми ділимося в соціальній мережі інформацією або думкою про будь-якої компанії? Як поширюється ця інформація? Хто отримує ці відомості? І, що ще важливіше, як компанії реагують і використовують цю інформацію для створення нових зв'язків з клієнтами?

Додатки для великих масивів даних повинні вміти збирати ці дані і структурувати їх таким чином, щоб організації отримували від цього користь. Наприклад, додатки для великих масивів даних повинні враховувати мінливі джерела і тенденції даних, до яких відносяться:

-мобільний зв'язок - мобільні пристрої, події, поширення інформації та інтеграція датчиків;

-доступ до даних і їх використання - Інтернет, з'єднані між собою системи, соціальні мережі і моделі доступу;

-можливості екосистеми - головні зміни в моделі обробки інформації та доступності відкритої середовища.

В результаті збільшилася вартість і складність цих моделей, що тягне за собою зміни в принципах зберігання і аналізу великих масивів даних, а також доступу до них. Для розміщення великих масивів даних організаціям необхідно скорегувати свої поточні моделі даних. Внаслідок цього організації все частіше використовують віртуалізацію і хмарні обчислення для підтримки потреб великих масивів даних.

Павленко В., Гнатюк П.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій

м. Київ

ВІРТУАЛІЗАЦІЯ ТА ХМАРНІ ОБЧИСЛЕННЯ

Так исторически сложилось, что на каждом компьютере установлены собственные операционная система, приложения и специализированные компоненты оборудования. Теперь же с помощью эмуляции программного средства на одном физическом компьютере могут работать несколько виртуальных. Это означает, что на каждом компьютере установлены собственные операционная система, приложения и специализированные компоненты оборудования. Это называется виртуализацией в компьютерных технологиях. Каждая из показанных на рисунке виртуальных машин функционирует независимо.

В корпоративном мире в одной физической инфраструктуре могут функционировать несколько виртуальных. Благодаря виртуализации серверов и сетей компании сокращают эксплуатационные и административные расходы. Сэкономить на эксплуатации можно за счет снижения требований к энергопотреблению и охлаждению, а также сокращения количества физических машин. Для поддержания дополнительных приложений можно добавить виртуальный сервер.

Также виртуализацию можно использовать в личных целях. Вы можете опробовать на своем компьютере новую операционную систему, не затрагивая текущую. С помощью виртуальной машины можно безопасно просматривать веб-сайты в Интернете. Если что-то пойдет не так, то виртуальную машину можно будет просто удалить.

Облачные вычисления — это еще один способ управления, хранения и открытия данных.

При облачных вычислениях множество компьютеров подключено между собой через сеть. Для обеспечения облачных услуг их поставщики полагаются на виртуализацию. Облачные вычисления тоже могут сократить эксплуатационные расходы благодаря более эффективному использованию ресурсов. Эти компании предоставляют четыре отдельных категории услуг. Для просмотра подробных сведений щелкните категории на рисунке.

Облачные вычисления предоставляют пользователям доступ к данным откуда угодно и когда угодно. Возможно, в каком-то виде вы уже используете облачные вычисления, если прибегаете к услугам интернет-почты.

Кроме того, благодаря облачным вычислениям организации могут упростить свои ИТ-операции, подписываясь только на необходимые услуги. С помощью облачных вычислений организации могут избежать необходимости развертывать и поддерживать оборудование, а также управлять им на своей территории. Облачные вычисления позволяют организациям сократить свои расходы. Они сокращают затраты на оборудование, электроэнергию, уменьшают требования материальной части и потребности в обучении вспомогательного персонала.

Свинтицький К., Троянов Д.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ІНФОРМАЦІЯ ПЕРЕТВОРЮЄ ПОВЕДІНКУ

«У ньому [Всеосяжному Інтернеті] технологія не головне. Для нас важливіше змінити життя людей », - Джон Чемберс, головний виконавчий директор корпорації Cisco.

Користь дозволяє виміряти економічний прибуток. Саме люди визначають користь пропонованих можливостей через систему обміну. Важливо підкреслити, що, як би не були важливі дані і аналітика, тільки думка споживачів перетворює дані в знання, а знання на користь Всеохоплюючої Інтернету.

Всеохоплюючий Інтернет надає точну і своєчасну інформацію, яка може змінити людську поведінку з користю для всіх людей. Завдяки йому зворотний зв'язок стала

простіше, що дозволяє людям приймати обґрунтовані рішення і бачити різницю між фактичними і бажаними результатами. Це називається петлею зворотного зв'язку. Петля зворотного зв'язку надає інформацію реального часу, виходячи з поточного поведінки, а потім пропонує практичну інформацію, яка допоможе змінити цю поведінку.

Петля зворотного зв'язку - це актив, який важливий для компаній, оскільки він допомагає їм правильно реагувати на громадську думку і планувати свої дії відповідно до мінливого положенню бізнесу. Завдяки петлі зворотного зв'язку компанії роблять дійсно важливі і конкурентоспроможні пропозиції, які задовольняють потреби клієнтів. Наприклад, багато роздрібні продавці використовують картки клієнта для відстеження покупок та інтересів своїх клієнтів. Так роздрібні продавці можуть пропонувати товари безпосередньо найбільш зацікавленим покупцям, які можуть принести більше прибутку.

Сто років тому підприємства приділяли основну увагу створенню недиференційованих продуктів, продаючи всім один і той же товар. Це було пов'язано з еволюцією масового виробництва того часу. У тій же мірі використовувалися рекламні стратегії, масовий маркетинг з використанням відмінних комплектів фірми, памфлети і газети, які закликають людей купити товар.

Однак одиничний продукт або послуга навряд чи будуть затребувані усіма. Сучасний бізнес навчився використовувати цільової маркетинг, який створює диференційовані пропозиції, виходячи з потреб клієнтів. Саме тому компаніям необхідний доступ до даних про клієнтів.

Нагорна Н., Стеценко О., Конюшок С.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ПІДКЛЮЧЕННЯ РЕЧЕЙ ДЛЯ СПОЖИВАЧІВ В ІНТЕРНЕТІ РЕЧЕЙ

Як підключення речей впливає на наше особисте життя? Наприклад, розглянемо поточну структуру середньостатистичної домашньої мережі.

Домашня мережа - це локальна мережа з пристроями, які підключаються до домашнього маршрутизатора. Швидше за все, маршрутизатор також підтримує бездротові підключення. В даному прикладі до локальної мережі можна підключитися через бездротову локальну мережу (WLAN). На малюнку 1 показана типова домашня мережа WLAN з підключенням до Інтернету через місцевого інтернет-провайдера (ISP). Різні пристрої та сполуки, що використовуються на стороні інтернет-провайдера, який не видно домашнім користувачам, але тим не менше грають найважливішу роль в роботі підключення до Інтернету.

Місцевий інтернет-провайдер підключений до інших інтернет-провайдерам, що забезпечує доступ до веб-сайтів і контенту з усього світу. Як показано на малюнку 2, ці інтернет-провайдери підключаються один до одного за допомогою різних технологій, у тому числі по глобальній мережі (WAN).

Однак тип мережевого підключення «машина-машина» (M2M) можливий лише в разі Інтернету Речей. На малюнку 3 представлена група датчиків пожежної сигналізації та охоронних датчиків, які можуть обмінюватися даними один з одним і відправляти їх через шлюз (домашній маршрутизатор) в серверну середу в хмарі. У цьому середовищі можливий збір і подальший аналіз даних.

Для правильної роботи промислових додатків в Інтернеті Речей необхідна певна ступінь надійності і автономії, яка не настільки важлива для середовища споживачів. Для деяких промислових додатків потрібні операції і розрахунки, які виконуються дуже швидко, т. Е. Участь в них людини не представляється можливим. Наприклад, якщо ваш

смартфон через збій не нагадала про заплановану зустріч, це може привести до незручної ситуації. А ось відмова системи гальмування в кар'єрному вантажівці-самоскиді може привести до катастрофічних наслідків як для співробітників, так і для всієї організації

Бондаренко І.І.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ВНЕДРЕНИЕ RFID-УСТРОЙСТВ ИМПЛАНТИРУЕМЫЕ В ТЕЛО ЧЕЛОВЕКА

Радиочастотная идентификация (radio frequency identification - RFID) - это технология автоматического бесконтактного дистанционного обнаружения, распознания и оперативного сопровождения различных - неподвижных и подвижных, пространственно распределённых объектов.

Радиочастотная идентификация позволяет осуществлять одностороннюю или двухстороннюю связь между RFID-метками и RFID-приемником. Метки могут быть пассивными (без собственного источника питания), активными (со своей батареей) и полупассивными (также с батареей). Приемники имеют собственное питание и могут быть пассивными (работающими в режиме только чтения меток) и активными (они могут не только считывать, но и передавать информацию на метки). RFID-метки можно считывать на больших расстояниях, до 100 метров без прямой видимости между считывателем и меткой. Поэтому их можно использовать, например, для обработки багажа в аэропорту. RFID использует несколько радиочастотных диапазонов, показанных в таблице ниже. Связь между устройством чтения и метками осуществляется с использованием стандартизированных протоколов. Для разных диапазонов частот применяются различные протоколы.

В настоящее время изделия радиочастотной идентификации в форме «умных» - смарт, этикеток и ярлыков (инлееев, тагов) находят самое широкое применение в сферах бизнеса - производства, торговли, перевозок, а также здравоохранения, культуры, безопасности и других, самых разных, областей общественных отношений.

RFID-устройства, имплантируемые в тело человека
Человеческие RFID-метки обычно представляют собой пассивный RFID-транспондер, содержащий интегральную микросхему (называемую с подачи ленивых журналистов в просторечии чипом) в стеклянной капсуле. Метки имплантируются подкожно в руку или иную часть тела человека и обычно содержат уникальный идентификационный номер, который можно связать с информацией в базе данных, содержащей информацию о личности, проблемах с законом, медицинской истории, принимаемых лекарствах и так далее. Корпорация VeriChip приступила к производству RFID-имплантатов еще в 2002 году, а в 2004 году их устройства были сертифицированы Управлением по контролю качества пищевых продуктов и лекарственных препаратов США (FDA).

Будущие области применения пассивных RFID-меток, имплантируемых в тело человека:

• Предоставление данных для электронных систем хранения медицинской информации о пациентах;
• Мониторинг пациентов в больницах;
• Контроль времени приема лекарств пациентами в больницах;
• Управление медицинским оборудованием;
• Возможность извлечения медицинской информации при оказании срочной медицинской помощи;

• Помощь дезориентированным больным с болезнью Альцгеймера;
• Контроль местонахождения персонала;
• Поиск потерявшихся детей;
• Удобство открывания дверей, управления принтерами, разблокировки компьютеров в офисах;

Конечно, с человеческими имплантатами связано много проблем, включая возможные опухоли в месте инъекции метки, миграции метки в теле, возможная несовместимость меток с устройствами магнитного резонанса, риски, связанные с безопасностью и неприкосновенностью частной жизни.

Ткаленко О.М., Щетініна А.А.
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м.Київ

ВИБІР ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОРГАНІЗАЦІЇ ПОСЛУГ VoIP

Сучасні технології VoIP дозволяють компаніям різних масштабів впровадити у себе функціонал, раніше доступний тільки за допомогою великих і дорогих систем. На даний момент на ринку представлена велика кількість ПЗ і платформ для реалізації IP-PBX. Існують як комерційні продукти, так і безкоштовні. Використання комерційних продуктів в деяких випадках є єдиним виходом для фірм готових користуватися послугами VoIP. Причини можуть бути найрізноманітнішими, наприклад, надання кваліфікованої технічної підтримки 24 години на добу 365 днів у році або неможливість утримувати штат співробітників, які обслуговують таку інфраструктуру. Прикладом комерційного проекту можуть виступати рішення компанії Avaya, яка зарекомендувала себе на ринку як постачальник традиційного підходу до реалізації передавання голосової інформації. Один з варіантів інтеграції полягає в доукомплектуванні систем Definity платами IP-телефонії, інше рішення - придбання продукту IP Office. Інший варіант - використання вільно розповсюдженого ПЗ, як правило, з відкритим вихідним кодом (OpenSource) під ліцензією GPL. Для використання такого ПЗ потрібно мати в штаті висококваліфікованого системного адміністратора, що виправдано при достатніх розмірах організації, однак на сьогоднішній день досить часто з'являються компанії, що надають різного роду послуги IT-аутсерсінга, в тому числі і телефонії. До переваг вільно розповсюджуваних IP-PBX, як і деяких інших програмних продуктів, можна віднести їх високу якість та інтенсивний розвиток.

На базі IP-PBX

У даному методі використовується таке телекомунікаційне обладнання як: Cisco, D-Link, Panasonic.

Обладнання Cisco використовується при побудові мереж IP-телефонії, яка основана на архітектурній моделі CiscoAVVID. IP-телефонія за допомогою засобів Cisco може бути організована як для невеликих підприємств та офісів, що мають у своїй мережі не більше десятка користувачів, так і для великих компаній.

Дана мережа працює за допомогою головного керуючого сервера CiscoCallManager, який відповідає і перерозподіляє всі телефонні з'єднання, а також відеозв'язок. При цьому CallManager управляє всіма підключеними до мережі апаратами, такими як IP-телефони і відеоапаратура, а також надає додаткові функції, передбачені мережею. Для IP-мережі, яка побудована за допомогою засобів Cisco, використовуються IP-телефони, що підключаються у локальній мережі Ethernet, виконуючи всі функції традиційних цифрових телефонів з рядом нових можливостей.

PBX для Windows

Цей метод створення IP-телефонії розроблений спеціально для роботи під операційною системою Windows. Використання SIP стандартів дозволило спростити управління і організацію мережі в цілому. Також впроваджені рішення дають можливість підключати будь-які SIP-телефони в IP-мережу, які реалізовані як на програмному або апаратному рівнях.

Технологія 3CX, яка використовується в даному методі налаштування мережі - це програмна IP-PBX, яка, крім того, що замінює собою офісну PBX, має ще ряд нових можливостей. 3CX може бути встановлена на будь-який комп'ютер, що працює під ОС Windows (Windows 7, 8, 10, WindowsServer 2008 або 2012). У даній PBX для офісу є можливість працювати з VoIP-шлюзи, що у свою чергу, дає можливість максимально гнучко налаштовувати мережу.

IP-PBX під операційною системою Linux

Основною складовою IP-PBX є сервер VoIP-телефонії Asterisk – програмна PBX з відкритим вихідним кодом, платформою для установки якої служить операційна система Linux. Це означає, що при впровадженні Asterisk не потрібно витрачати кошти на покупку ліцензій – ПЗ, яке використовується, безкоштовне. Потрібно сплатити тільки за апаратну складову і роботу по інсталяції та конфігурації Asterisk. Платформа Asterisk не вимоглива до ресурсів і працює на звичайному комп'ютері. Asterisk працює на базі IP-протоколу і не потребує міні-АТС та прокладання телефонної мережі та ідеально відповідає вимогам сучасного бізнесу. Все, що потрібно співробітнику для роботи – це VoIP-телефон або комп'ютер з гарнітурою.

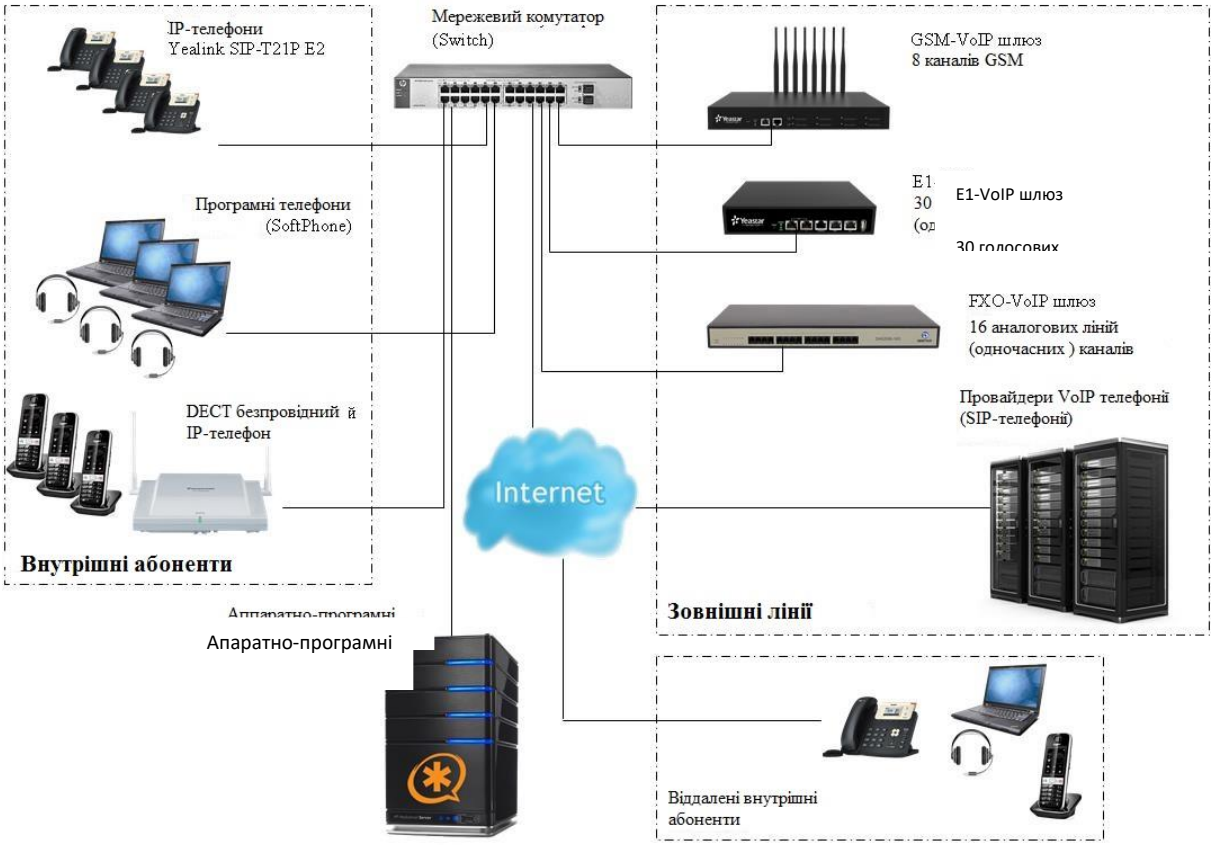


Рисунок 1 – Схема організації зв'язку на базі платформи Asterisk

Asterisk у комплексі з необхідним обладнанням має всі можливості PBX, підтримує множину VoIP протоколів та надає наступні функції: голосова пошта, голосові конференції, інтерактивне голосове меню (IVR), центр обробки викликів (встановлення дзвінків в чергу

та розподіл їх по агентам, використовуючи різні алгоритми), запис телефонних розмов, запис CDR (детальний запис про виклик).

Висновок. Впровадження Asterisk корпоративному клієнту дає розвиток компанії, еволюційний підхід: нові можливості можна добавляти по мірі необхідності. Можна вносити зміни в обслуговування викликів без придбання платних ліцензій, а також здійснювати моніторинг дзвінків в режимі online та запис розмов, можливість комутувати абонентів через панель управління; голосові привітання, динамічні черги розподілу вхідних дзвінків; відсутність необхідності у придбанні додаткових ліцензій і плат телефонії; можливість інтегрування з іншими системами, використовуючи AMI/API інтерфейс, наприклад, CRM системами та базами даних; розподіл дзвінків, адже в першу чергу Asterisk – це IP-PBX з усіма можливостями VoIP.

Література

1. *А.В. Росляков, М.Ю. Самсонова, И.В. Шибаев. IP-телефония - М.: ЭкоТренд, 2007 – 252с.*
2. *Б.С.Гольштейн, А.В.Пинчук, А. Л.Суховицкий: IP- телефония - М.: Радиосвязь, 2009.- 366с.*
3. *Б. С. Гольдштейн, А. А. Зарубин, В. В. Саморезов: Протокол SIP справочник - Санкт-Петербург. – 2009.*
4. *Джонатан Девідсон, Джеймс Пітерс, Манож Бхатія, Сатіш Калідінді, Судіпто М. Основи передачі голосових даних по мережах IP (IP Voiceover IP Fundamentals); Вільямс, 2012.*
5. *www.asterisk.org/ - сайт IP-PBX Asterisk.*

Мельник Микола Віталійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет інформаційних технологій
м. Київ

ТЕХНОЛОГІЯ ПЕРЕДАЧІ ДАНИХ LI - FI

У даній роботі розглянуто безпровідну технологію Li-Fi. Преведений аналіз переваг і недоліків даної технології в порівнянні з іншими безпроводними комунікаційними технлогіями, як Wi – Fi. Приведені характеристики, які покажуть, чи зможе данна технологія замінити замінити свого конкурента. Описано реалізацію, принцип дії,основні компоненти, терміни реалізації та де використовується зараз дана технологія Li-Fi.

Li-Fi (Light Fidelity, світлова точність) - це двонаправлена, високошвидкісна безпровідна комунікаційна технологія. Запатентував термін Li-Fi, німецький фізик Гаральд Хаас в 2011 році, продемонструвавши світлодіодну лампу, яку можна використовувати в якості роутера, який роздає сигнал. Такий вид передачі даних використовує видиме світло, як канал зв'язку, таким чином Li-Fi належить до технологій VLC.

VLC (Visible Light Communication, зв'язок по видимому світлі) - технологія, яка дозволяє джерелу світла, на додаток до висвітлення передавати інформацію, використовуючи той же самий світловий сигнал. Робоча швидкість світлодіода становить 1 мкс, тобто вона буде непомітна для людського ока. Li-Fi влаштована так, що в якості бездротових маршрутизаторів можуть використовуватися електричні світлодіодні лампочки. Паралельна передача даних за допомогою масивів світлодіодів, кожен з яких передає окремий потік, може збільшити швидкість передачі.

Для забезпечення роботи Li-Fi необхідно наступне апаратне забезпечення:

1. Світлодіодна система освітлення.
2. Маршрутизатор, встановлений разом з системою освітлення.
3. Приймач, який оснащений декодером з метою розшифровки світлового сигналу.

Технологія Li-Fi – більш дешева і швидка версія Wi-Fi, яка діє в видимому діапазоні довжин хвиль. Технологія передбачає передачу даних із застосуванням видимого світла зі

спектром від 400 ТГц (780нм) до 800 ТГц (350Нм). Li-Fi працює на електромагнітних хвилях. Стандарт IEEE 802.15.7 для Li-Fi визначає фізичний рівень мережі OSI PHY (Physical layer), в тому числі рівень управління доступом до області Media Access Control (MAC-адреса). На поточний момент досягнута практична швидкість становить 1 Гбіт / с, в найближчому майбутньому вона складе 15 Гбіт / с.

Сагайдак Виктор Анатольевич
Государственный университет телекоммуникаций
Учебно-научный институт Телекоммуникаций и информатизации
Факультет информационных технологий
г. Киев

СПАМ И СПОСОБЫ БОРЬБЫ С НИМ НА ВЕБ-ФОРУМЕ

Реклама – современный способ передать информацию о продукте компании, самой компании, в общем, это способ рассказать о чем-то. Сейчас она практически везде и содержит в себе самую различную информацию, которая засоряет общий информационный поток, что затрудняет поиск нужной информации.

Цели применения могут самыми различными: накрутка популярность посредством «клик бейтов», нанесение вреда владельцу устройства, дискредитация кампании конкурента, информационная война и прочее. К примеру, в 2011 году из нескольких супермаркетов в США выкинули партию бананов из Коста-Рика, под предлогом того, что они заражены вирусом, вызвавшим смерть 15 тысяч обезьян. Прекратились эти действия только после того, как менеджер компании, поставляющей эти бананы, прояснил ситуацию.[4]

Существует несколько способов борьбы со СПАМом веб-форм: [1]

Капча-картинка — данный способ очень распространён на различных веб сайтах, форумах, социальных сетях. Пользователю, обычно, отправляют картинку с набором букв-цифр и просят ввести текст с данного изображения.

Текстовые капчи разного типа — это капчи, которые используют связку вопрос-ответ и предлагают написать ответ на предложенный вопрос. Сюда также относятся капчи предлагающие проделать некоторые арифметические действия и ввести правильный ответ в поле ввода.

Интерактивные капчи — это довольно новый и пока малораспространенный вид капч, смысл которых заключается в интерактивном взаимодействии пользователя с некоторыми объектами.

Основными сервисами, предоставляющими такие услуги, являются KeyCAPTCHA и reCAPTCHA

Также существуют **«Бескапчавые» метода фильтрации спама**:

- Установка форм или каких-то полей, которые позже будут проверены на корректность веб-сервером.
- Создание невидимых разделов сайта, куда попадают только роботы и позже баняться по IP
- Проверка задержек на скорость заполнения форм
- Фильтрация анонимных прокси
- Сервисы по борьбе со СПАМОМ. К ним относятся Akismet, Disqus.

Список использованных источников:

1. Хабрахабр[электронный ресурс]// Взгляд на современные системы защиты от спама веб-форм - Режим доступа - https://habr.com/post/107286/

2. Google [электронный ресурс]// Google reCAPTCHA – Режим доступа - https://www.google.com/recaptcha/intro/v3beta.html

3.KeyCAPTCHA[электронный ресурс]// Improve your CAPTCHA in 5 minutes! – Режим доступа - https://www.keycaptcha.com/

4. Хабрахабр[электронный ресурс]// «Автоматический детектор спама». Или «О чем предупреждали Хемингуэй, Хаксли и Постман?» - Режим доступа - https://habr.com/post/343268

Савіцький Вячеслав
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет інформаційних технологій
м. Київ

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ

Виртуальная реальность — созданный техническими средствами мир , передаваемый человеку через его ощущения : зрение, слух, обоняние, осязание и другие. Виртуальная реальность имитирует как воздействие, так и реакции на воздействие. Для создания убедительного комплекса ощущений реальности компьютерный синтез свойств и реакций виртуальной реальности производится в реальном времени.

Объекты виртуальной реальности обычно ведут себя близко к поведению аналогичных объектов материальной реальности. Пользователь может воздействовать на эти объекты в согласии с реальными законами физики (гравитация, свойства воды, столкновение с предметами, отражение и т. п.).

Однако часто в развлекательных целях пользователям виртуальных миров позволяется больше, чем возможно в реальной жизни (например: летать, создавать любые предметы и т. п.).

Не следует путать виртуальную реальность с дополненной. Их коренное различие в том, что виртуальная конструирует новый искусственный мир, а дополненная реальность лишь вносит отдельные искусственные элементы в восприятие мира реального.

Маринич Олексій Олексійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
м. Київ

АНАЛІЗ КІНОСТРІЧКИ «МАТРИЦЯ» (ТРИЛОГІЯ) ЯК ПРИКЛАДУ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ

Сучасне використання віртуальної реальності (далі за текстом ВР) має практично необмежені і перспективні напрямки розвитку. Одним з найбільш вражаючих прикладів використання ВР для 100% контролю за якістю життя людей є фантастична «Матриця» з однойменної стрічки. Геніальність ідеї фільму базується саме на тому, що абсолютно все світосприйняття людини створюється завдяки електричним імпульсам, що отримує центральна нервова система людини від сенсорів організму.

Вперше поняття ВР та створення перших її апаратних засобів датується 60-ими роками минулого століття. Метою її створення була спроба створити реальність, що зможе замінити існуючу для розумних істот.

В сучасних варіантах ВР людський організм здебільшого знаходиться під впливом візуальних та тактильних (механічних) ефектів. Основним недоліком цих систем є неможливість балансування відчуттів та реакції на них, особливо вестибулярного апарату (відчуття гравітації та орієнтації у просторі). Це пов’язано з недосконалістю систем заміни фактичних відчуттів синтетичними (програмно створеними і наданими технічними засобами). Фізично людина, підключена до системи життєзабезпечення нічого не відчувала, оскільки була повністю ізольована від зовнішнього світу, але жила повноцінним життям у ВР. Реалії Матриці людина отримувала напряму в головний мозок, в обхід сенсорів організму.

Принципова різниця між існуючими ВР та Матрицею полягає у способі взаємодії з людиною, а саме те що людина не використовує власну фізіологічну сенсорну систему.

Враховуючи недосконаліть систем ВР, їх вкрай високі вимоги щодо продуктивності й швидкодії сучасних комп'ютерів, прогнозувати широке застосування інтерактивних ВР в повсякденному житті та побуті не є доцільним.

Список використаної літератури

1. *iCube — технологія створення трьохвимірної віртуальної реальності.*
2. *«Велике випробування для VR». Головний науковий співробітник «Oculus» Міхаэль Абраш о майбутньому людських взаємодій.*
3. *Эндрю и Лоуренс Вачовски – автори сценарію трилогії «Матриця».*

Бабенко Марія Олексіївна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
м. Київ

ШТУЧНИЙ ІНТЕЛЕКТ, ЕМОЦІЇ, АСОЦІАЦІЇ ТА ПАМ'ЯТЬ

Розглянуто історію створення штучного інтелекту, розвитку штучного інтелекту. Показано та сформульовано інженерію знань і наведені моделі придбання знань.

В рамках першого підходу об'єктом досліджень є структура та механізми роботи мозку людини, а кінцева мета полягає в розкритті таємниць мислення. Необхідними етапами досліджень в цьому напрямку є побудова моделей на основі психофізіологічних даних, проведення експериментів з ними, висування нових гіпотез щодо механізмів інтелектуальної діяльності, вдосконалення моделей і т. Д.

Другий підхід як об'єкт дослідження розглядає штучний інтелект. Тут мова йде про моделювання інтелектуальної діяльності за допомогою обчислювальних машин. Метою робіт в цьому напрямку є створення алгоритмічного і програмного забезпечення обчислювальних машин, що дозволяє вирішувати інтелектуальні завдання не гірше людини.

Нарешті, третій підхід орієнтований на створення змішаних людино-машинних, або, як ще кажуть, інтерактивних інтелектуальних систем, на симбіоз можливостей природного і штучного інтелекту. Найважливішими проблемами в цих дослідженнях є оптимальний розподіл функцій між природним і штучним інтелектом і організація діалогу між людиною і машиною.

Термін інтелект (intelligence) походить від латинського intellectus - що означає розум, розум, розум; розумові здібності людини.

Відповідно штучний інтелект (artificial intelligence) - II (AI) звичайно тлумачиться як властивість автоматичних систем брати на себе окремі функції інтелекту людини, наприклад, вибирати і приймати оптимальні рішення на основі раніше отриманого досвіду і раціонального аналізу зовнішніх впливів.

У словниках даються такі визначення штучного інтелекту.

Штучний інтелект - здатність прикладного процесу виявляти властивості, асоційовані з розумною поведінкою людини.

Штучний інтелект - розділ інформатики, що займається питаннями імітації мислення людини за допомогою комп'ютера.

Цей клас пакетів включає: інформаційні системи, що підтримують діалог на природній мові (природно-мовний інтерфейс); експертні системи, що дозволяють давати рекомендації користувачеві в різних ситуаціях; інтелектуальні пакети прикладних програм, що дозволяють вирішувати прикладні завдання без програмування.У сучасному світі будь-якої організації потрібно бачити і розуміти особливості структури внутрішньої/зовнішньої систем. У цьому допомагають спеціальні плаформи для створення мультимедія в інформаційних технологіях, які надають ряд можливостей, викладених нижче.

Для фахівців в області штучного інтелекту термін «знання» означає інформацію, яка необхідна програмі, щоб вона вела себе «інтелектуально».

Функціонування засобів інтелектуального інтерфейсу спирається на розвинені методи роботи зі знаннями: їх уявлення, зберігання, перетворення і т. п. Під терміном «знання» при цьому розуміється вся сукупність інформації, необхідної для вирішення завдання, що включає в себе, в тому числі інформацію про:

системі понять предметної області, в якій вирішуються завдання; системі понять формальних моделей, на основі яких вирішуються завдання; поточний стан предметної області; методах вирішення завдань.

Отже, виходячи з цього можна зробити висновок, що люди будуть постійно вирішувати проблему штучного інтелекту, постійно стикаючись все з новими проблемами. І, мабуть, процес цей нескінченний.

Література:

1. *Шихов Е. Варіанти реалізації штучного інтелекту - ресурс Інтернету, http://neural.narod.ru/, 2002 з 125*
2. *Ендрю А. Штучний інтелект - М .: Світ, 1985. с. 256*
3. *Брушлинский А.В. Чи можливий штучний інтелект?*
4. *Квасний Р. Штучний інтелект - ресурс Інтернету, http://neural.narod.ru/, 2001. с.111*

Петровська Анастасія

Державний університет телекомунікацій

Навчально-науковий інститут Телекомунікацій та інформатизації

м. Київ

ГРАФИЧЕСКОЕ ИЗОБРАЖЕНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА

В современном мире любой какой организации нужно видеть и понимать особенности структуры внутренней / наружной систем. В этом помогают специальные плаформы для создания мультимедиа в информационных технологиях, которые предоставляют ряд возможностей, изложенных ниже.

Технологический процесс может быть представлен графически с помощью различных схем. На различных уровнях детализации могут использоваться схемы данных, схемы программ, схемы работы системы, схемы взаимодействия программ и т.д.

Схемы работы системы отображают управление операциями и поток данных в системе (т.е. собственно технологический процесс решения задачи).

Схема данных отображает путь данных при решении задачи, определяет этапы обработки, применяемые носители данных.

Схемы взаимодействия программ отображают путь активации программ и взаимодействий с соответствующими данными.

Схемы программ отображают последовательность операций в программе. Основные обозначения символов схем, которые рекомендуется использовать при составлении программной документации, приведены в ГОСТ 19.701-90. В данном документе приводятся следующие определения.

Основной символ — символ, используемый тогда, когда точный тип (вид) процесса или носителя данных неизвестен или отсутствует необходимость в описании конкретного носителя данных.

Специфический символ — символ, используемый тогда, когда известен точный тип (вид) процесса или носителя данных или когда необходимо описать фактический носитель данных.

Схема — графическое представление определения, анализа или метода решения задачи, в котором используются символы для отображения операций, данных, потока, оборудования и т.д.

Для оформления технологического процесса используется три вида документов: схема данных; схема работы системы; схема взаимодействия программ.

На заключительном этапе в условиях может осуществляться визуальный контроль выходного документа, его оформление и копирование. Под визуальным контролем понимается проверка четкости печати, проверка отсутствия печатной строки на сгибах бумаги и др. Оформление сводится к визированию выходного документа (проставлению даты, подписей и т.д.). В случае необходимости получения выходных документов в нескольких экземплярах предусматривается операция копирования.

При решении многих экономических задач (бухгалтерского учета, статистической отчетности и др.) оперативная информация подготавливается на машинных носителях в течение всего отчетного периода по мере ее сбора и поступления, а задача решается только по окончании отчетного периода.

Исходя из этого можно сделать вывод, что моделирование с помощью информационных технологий - является основной целью любого предприятия, открывая возможности при поставленных задач и визуализации структуры.

Література:

1. *Информационные технологии в культуре : курс лекций / Е. С. Толмачева, С. Л. Замковец, Ю. В. Виланский, Н. Л. Гончарова. – Минск : Соврем. знания, 2010. – 264 с.*
2. *Карп Е. И. Роль интерактивных мультимедийных систем в вопросе информационного обеспечения деятельности управленческих структур // Вестн. акад. права и упр. – 2010. – № 21. – С. 159-165.*
3. *Лобанова Ю. В. От телевидения к интернету: открытая стратегия коммуникации // Упр. мегаполисом. – 2011. – № 2. – С. 129-132.*
4. *Мухлаев В. А. Использование информационных технологий в развитии познавательной активности учащихся // Образование и саморазвитие. – 2012. – Т. 1, № 29. – С. 50-55.*

Dmytro Danylets

Institute of Computer and Information Technologies
National Aviation University
Kyiv, Ukraine

ALLOCATION OF RESOURCES AND RISK FORECASTING IN PROJECTS USING NEURAL NETWORKS

Дана робота розповідає про проблему розподілення ресурсів та передбачення ризиків у проектах, існуючих способів вирішення даної проблеми, введення до нейронних мереж, і пояснення, як нейронні мережі можуть використовуватись для вирішення даної проблеми.

Introduction to a problem

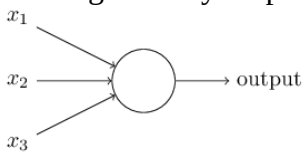
Resource allocation is the process of assigning and scheduling available resources in the most effective and economical manner. Projects will always need resources and resources are scarce. The task therefore lies with the project manager to determine the proper timing of those resources within the project schedule. However, project manager is only human that is not always finds a best way. For instance, if we have 20 different kinds of resources in limited quantity (material, non-material, human resources, time, etc), and 10 different nodes of project(backend, frontend, testing, integration, logistics, supplies, etc), there are a multiplication of 20 till 10 (20*19*18*…*10) different ways to distribute resources among different stakeholders[1].

Projects are designed to take advantage of resources and opportunities and with these, come uncertainty, challenges and risk. Hence risk management becomes a very important key to all project success. The project risk management plan addresses the process behind risk management and the risk assessment meeting allows the project team to identify, categorize, prioritize, and mitigate or avoid these risks ahead of time. Risk assessment is a step in a risk management

procedure, and risk forecasting is a possibility to predict which pieces of project are weaker then supposed to be[1].

Main part

Neural network is build from smaller nodes, which are called neurons. A basic example of neuron is a perceptron. A perceptron is a logic node, that takes several binary inputs x1,x2,…, and produces a single binary output:



Pic. 1. Perceptron

The ways to provide an output called weights, w1,w2,…[2], real numbers expressing the importance of the respective inputs to the output. The neuron's output, 0 or 1, is determined by whether the weighted sum $\sum_j w_j x_j$ is less than or greater than some threshold value. Just like the weights, the threshold is a real number which is a parameter of the neuron. To put it in more precise algebraic terms[3]:

$$\text{output} = \begin{cases} 0 & \text{if } \sum_j w_j x_j \leq \text{ threshold} \\ 1 & \text{if } \sum_j w_j x_j > \text{ threshold} \end{cases}$$

For this particular problem (resource allocation and risk forecasts), a network of perceptrons might be used as well. For each risk we can prepare a separate neural network, which will return us a real value between 0 and 1. This value will determine the probability with which the risk will occur. Such neural network will be posessed by two factors: global data, and input values. Global data – response from other neural network which will try to allocate resources, capacity of resources (entered by user), did risk occurred on this project previously, resource types that are needed by this project, and how much of any kind. Input data – the real number of resources which project could get. In such way I will cover two points – how to distribute resources with lack of latter, and which consequences this may lead to.

Conclusions

While the problem of risk forecasting is being lot underestimated to be solved with help of neural networks, it could be. The main part of solution is how to distribute input data over the neural network, how to convert real-world abstract objects and values into a binary form, and how to proof correctness of input data. For this purpose several iterations of training with various training data may be used.

References

1. *"Project management body of knowledge(PMBOK guide)". Project management institute, Inc. 2001.*
2. *Alex Smola and S.V.N. Vishwanathan. "Introduction to Machine Learning". Cambridge university press. 2008.*
3. *David Kriesel. "A Brief Introduction to Neural Networks". 2007.*

Duchkova Krystyna
Scientific curator: Grinenko O. O.
National Aviation University
Kiev, Ukraine

MODERN WAYS OF QUANTIFYING AND RENDERING THE USER INTERFACE

Annotation — The work is devoted to the consideration of the problem user interface usability and quantifying it in automatic way. In this work examined existed methods of quantifying interface – manual and automatic ways, also suggestions for improvement interface usability checking.

In the field of user interface design there are some problems, such as development efforts, the problem of semantic gap, the problem of adaptive interfaces to changing conditions, the problem of interface usability. On the other hand, there are several approaches to the construction

of the interface trying to solve a particular problem. The paper gets the analysis of some approaches on the subject of whether they solve these problems. Some approaches focus on the description of the user interaction with the system, some are focused on building models of the future interface, but none of approaches does not describe in detail the process of interface developing. There is no considered approach that solve all the problems. It is proposed to develop a new approach to user interface development, allowing to solve all considered problems and assuming representation of the interface development process and user interaction process as a set of mechanisms. User interface; problems in interface design; approaches to interface design.

The user interface is the central element of any modern pro- system because systems exist to work with them. users, and users interact with the system through in- interface. The effectiveness of the interface can be judged by how effective the The user is working with the system. At present, in the field of development user interfaces for information systems there is a number of pro- helmet. First, the efforts spent on the design, development, modification, and user interface support, are estimated to be experts to 70% of the complexity of developing software. Therefore, mu developers tend to reduce the complexity of developing the interface. The second problem is that the same people who develop the product - programmers. Developer has only necessary technical skills, and he can not act on rone business and technology at the same time. The programmer is only interested in ensuring the quality of the code that he writes, and is not interested in providing full compliance with the requirements of the end user. In the process of mutual user and developer issues a semantic va.

Therefore, many iterations are necessary before the the product as a whole, and the interface in particular, will meet the requirements the user. The next problem lies in the field of ergonomics and concerns the convenience of using the interface. The non-optimal distribution of functions between human beings computer and computer, the wrong algorithm and the pace of performance of work- without taking into account human capabilities or features of the tasks to be solved, adequate planning of the interaction between the user and the system are consequences lack of orientation to the needs, representations and possibilities of man. Convenience of user interaction with the system will be achieved only in that If the interface corresponds to the user's activity, i.e. The structure of the user activity and the structure of the interface must be and interpenetrate.

Another problem is that the domain conditions still exist, constantly change in connection with the development of business processes. Especially critical is the situation when they change during the operation phase. Therefore, with the help of which it will be possible to change the interface of the system and adjust it to the new environmental conditions. Adaptation of information systems - this is the process of adjusting them to changing operating conditions and needs users and business processes. This iterative process, which requires an appropriate can be considered an important part of the life cycle information system.

Usability is one relevant factor of a Web application’s quality. Recently, it has received great attention, and been recognised as a fundamental property for the success of Web applications. Defining methods for ensuring usability is therefore one of the current goals of Web engineering research. Also, much attention is currently paid to usability by industry, which is recognizing the importance of adopting usability methods during the development process, to verify the usability of Web applications before and after their deployment. Some studies have demonstrated how the use of such methods reduces costs, with a high cost benefit ratio, as they reduce the need for changes after the application is delivered

High competition in the Internet environment leads to the fact that owners of web projects need to constantly generate new ideas, improving usability, and also introducing various trend chips on their site.

At the same time, it is necessary to minimize the costs of introducing innovations, monitor their real efficiency, and take care of the profits of their business. In order to understand which idea will be more useful, it is necessary to conduct testing.

Nowadays there are two techniques of such testing:

- External audit (manual)
- Automatic checking by the external soft

Usability audit - a set of activities aimed at identifying problem areas that cause users difficulties in interacting with the site. And also the definition of possible ways of solving the detected problems. Any audit must pursue specific objectives. To make the site more beautiful is rarely an end in itself - the result of a successful usability audit is the improvement of business indicators. If you have an ugly footer or a button of the wrong color, it rarely affects the conversion, but 15 points in the questionnaire can weed out even the staunchest customers.

During a UX audit, an auditor will use a variety of methods, tools and metrics to analyse where a product is going wrong (or right):

- Review of business and user objectives
- Conversion metrics
- Customer care data
- Sales data
- Traffic/engagement
- Compliance with UX standards
- Usability heuristics
- Mental modeling
- Wireframing & Prototyping
- UX Best Practices

The difference between usability testing and a UX audit is one of information flow direction: an audit infers problems from a set of pre-established standards or goals, whereas testing infers problems from user actions. Granted, an auditor may use usability testing during an audit if they do not have access to the fundamental metrics, but they will combine the results with data collected over the longer term and weigh them up against industry standards and product goals.

Usability audit is primarily needed by sites of companies, whose business is built on Internet marketing and electronic sales. For such businesses, increasing the conversion rate of a site is an important and constant task.

The worse situation with automatic checkers by the external soft. There only one program, what allows users quantifying and exploring interface. Hotjar - service for advanced Internet marketers who analyze user behavior, conduct surveys, build funnels and the like. The main purpose of the service is to help you increase the conversion on the site.

It allows to:

- Visualize behavior
- Make visitor Recordings
- Make conversion Funnels
- Make form Analysis

Hotjar's analysis tools record how traffic engages with the site, and from which device and browser. User session recordings show what individual visitors are doing on each of your pages.

- Heatmaps: See where your users are clicking, tapping and scrolling on every web page.
- Conversion Funnels: Track conversions. Identify where your users are converting more and where they are leaving your site.
- Form Analysis: Discover which fields your users are leaving in blank, which take too long to fill, and why they're abandoning your form page.
- Visitor Recordings: In my opinion, the coolest feature ever. Track user navigation on each page they visit, see how they move their mouse and what they're clicking on. See for yourself in the image below.

The feedback tools enable you to directly ask your visitors about their experience. As a business owner, it is crucial to better understand the people who use your product or service. Hotjar gives you the keys to make simple, yet powerful improvements to make the experience better for your clients and to improve sales for your business.

- Polls: Get real-time insight to questions you may have for specific users. Find out what is preventing visitors from achieving what they want.
- Surveys: Invite users to fill it out before they abandon the site to uncover comments, questions or concerns.
- Recruiters: Ask your visitors to help you with user testing. Invite them to a live user test via screen-sharing (e.g. via Skype or Join.me). Collect profiling information, contact details and offer a gift in exchange for their help.

Hotjar has the potential to be a huge asset for almost any business, however, its features cross uncharted territory. Just as there are great pro's, there are also drawbacks to consider.

- The company is young, which means they lack the years of experience and customer support systems that their competitors have.
- There's a lack of attention to mobile.
- The information is not recorded in continuous streams, rather the different packages have limits on the number of visitors recorded on each "snapshot".
- There's no integration of CRM with other programs, which is a setback for large companies with massive amounts of data to analyze.

To produce all needed calculations, program use usability metrics. The ISO 9241-11 standard defines usability as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use". The reason why I marked effectiveness, efficiency and satisfaction in bold is because this definition clearly states that usability is not a single, one-dimensional property but rather a combination of factors.

The ISO/IEC 9126-4 Metrics recommends that usability metrics should include:

- Effectiveness: The accuracy and completeness with which users achieve specified goals
- Efficiency: The resources expended in relation to the accuracy and completeness with which users achieve goals.
- Satisfaction: The comfort and acceptability of use.

Effectiveness can be calculated by measuring the **completion rate**. Referred to as the fundamental usability metric, the completion rate is calculated by assigning a binary value of '1' if the test participant manages to complete a task and '0' if he/she does not.

Due to its simplicity, the completion rate is a metric that is very easy to understand, hence the reason why it is very popular. Moreover, it can be collected during any stage of development.

The overall relative efficiency uses the ratio of the time taken by the users who successfully completed the task in relation to the total time taken by all users.

After users attempt a task (irrespective of whether they manage to achieve its goal or not), they should immediately be given a questionnaire so as to measure how difficult that task was. Typically consisting of up to 5 questions, these post-task questionnaires often take the form of Likert scale ratings and their goal is to provide insight into task difficulty as seen from the participants' perspective.

The most popular post-task questionnaires are:

- ASQ: After Scenario Questionnaire (3 questions)
- NASA-TLX: NASA's task load index is a measure of mental effort (5 questions)
- SMEQ: Subjective Mental Effort Questionnaire (1 question)
- UME: Usability Magnitude Estimation (1 question)

- SEQ: Single Ease Question (1 question

Test Level Satisfaction is measured by giving a formalized questionnaire to each test participant at the end of the test session. This serves to measure their impression of the overall ease of use of the system being tested. For this purpose, the following questionnaires can be used (ranked in ascending order by number of questions):

- SUS: System Usability Scale (10 questions)
- SUPR-Q: Standardized User Experience Percentile Rank Questionnaire (13 questions)
- CSUQ: Computer System Usability Questionnaire (19 questions)
- QUIS: Questionnaire For User Interaction Satisfaction (24 questions)
- SUMI: Software Usability Measurement Inventory (50 questions)

As highlighted in this article, using usability metrics, it is possible to observe and quantify the usability of any system irrespective if it is software, hardware, web-based or a mobile application. This is because the metrics presented here are based on extensive research and testing by various academics and experts and have withstood the test of time.

Moreover, they cover all of the three core elements that constitute the definition of usability: effectiveness, efficiency and satisfaction, thus ensuring an all-round quantification of the usability of the system being tested.

In the scope of the state, the problem of interface quantification has been considered. As the result there two solutions for investigation of interface usability checking have been found. So, there is effectively only one tool that allows people working with interface to make automatic audit and quantification of interface, and this is the main problem in this branch.

REFERENCES

1. *"Archived copy". Archived from the original on 2015-02-16. Retrieved 2015-02-15*
2. *Nielsen, Jakob (4 January 2012). "Usability 101: Introduction to Usability". Nielsen Norman Group. Archived from the original on 1 September 2016. Retrieved 7 August 2016.*
3. *Nielsen, Jakob; Norman, Donald A. (14 January 2000). "Web-Site Usability: Usability On The Web Isn't A Luxury". JND.org. Archived from the original on 28 March 2015.*
4. *Kuniavsky, M. (2003). Observing the User Experience: A Practitioner's Guide to User Research, San Francisco, CA: Morgan Kaufmann.*

Duchkova Krystyna
Scientific curator: Grinenko O. O.
National Aviation University
Kiev, Ukraine

MODERN WAYS OF QUANTIFYING AND RENDERING THE USER INTERFACE

Annotation — The work is devoted to the consideration of the problem user interface usability and quantifying it in automatic way. In this work examined existed methods of quantifying interface – manual and automatic ways, also suggestions for improvement interface usability checking.

In the field of user interface design there are some problems, such as development efforts, the problem of semantic gap, the problem of adaptive interfaces to changing conditions, the problem of interface usability. On the other hand, there are several approaches to the construction of the interface trying to solve a particular problem. The paper gets the analysis of some approaches on the subject of whether they solve these problems. It is proposed to develop a new approach to user interface development.

Therefore, many iterations are necessary before the the product as a whole, and the interface in particular, will meet the requirements the user. The next problem lies in the field of ergonomics and concerns the convenience of using the interface. The non-optimal distribution of functions between human beings computer and computer, the wrong algorithm and the pace of performance of work.

Another problem is that the domain conditions still exist, constantly change in connection with the development of business processes. Especially critical is the situation when they change during the operation phase. Adaptation of information systems - this is the process of adjusting

them to changing operating conditions and needs users and business processes. This iterative process, which requires an appropriate can be considered an important part of the life cycle information system

High competition in the Internet environment leads to the fact that owners of web projects need to constantly generate new ideas, improving usability, and also introducing various trend chips on their site.

At the same time, it is necessary to minimize the costs of introducing innovations, monitor their real efficiency, and take care of the profits of their business. In order to understand which idea will be more useful, it is necessary to conduct testing.

Nowadays there are two techniques of such testing:

- External audit (manual)
- Automatic checking by the external soft

Usability audit - a set of activities aimed at identifying problem areas that cause users difficulties in interacting with the site. And also the definition of possible ways of solving the detected problems. Any audit must pursue specific objectives. To make the site more beautiful is rarely an end in itself - the result of a successful usability audit is the improvement of business indicators. If you have an ugly footer or a button of the wrong color, it rarely affects the conversion, but 15 points in the questionnaire can weed out even the staunchest customers.

Usability audit is primarily needed by sites of companies, whose business is built on Internet marketing and electronic sales. For such businesses, increasing the conversion rate of a site is an important and constant task.

The worse situation with automatic checkers by the external soft. There only one program, what allows users quantifying and exploring interface. Hotjar - service for advanced Internet marketers who analyze user behavior, conduct surveys, build funnels and the like. The main purpose of the service is to help you increase the conversion on the site.

It allows to:

- Visualize behavior
- Make visitor Recordings
- Make conversion Funnels
- Make form Analysis

In the scope of the state, the problem of interface quantification has been considered. As the result there two solutions for investigation of interface usability checking have been found. So, there is effectively only one tool that allows people working with interface to make automatic audit and quantification of interface, and this is the main problem in this branch.

REFERENCES

1. "Archived copy". Archived from the original on 2015-02-16. Retrieved 2015-02-15
2. Nielsen, Jakob (4 January 2012). "Usability 101: Introduction to Usability". Nielsen Norman Group. Archived from the original on 1 September 2016. Retrieved 7 August 2016.
3. Nielsen, Jakob; Norman, Donald A. (14 January 2000). "Web-Site Usability: Usability On The Web Isn't A Luxury". JND.org. Archived from the original on 28 March 2015.
4. Kuniavsky, M. (2003). Observing the User Experience: A Practitioner's Guide to User Research, San Francisco, CA: Morgan Kaufmann.

Мельник Микола Віталійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ТЕХНОЛОГІЯ ПЕРЕДАЧІ ДАНИХ LI – FI

У даній роботі розглянуто безпровідну технологію Li-Fi. Преведений аналіз переваг і недоліків даної технології в порівнянні з іншими безпроводними комунікаційними технлогіями, як Wi – Fi. Приведені характеристики, які покажуть, чи зможе данна технологія замінити замінити свого конкурента. Описано реалізацію, принцип дії,основні компоненти, терміни реалізації та де використовується зараз дана технологія Li-Fi.

Li-Fi (Light Fidelity, світлова точність) - це двонаправлена, високошвидкісна безпровідна комунікаційна технологія. Запатентував термін Li-Fi, німецький фізик Гаральд Хаас в 2011 році, продемонструвавши світлодіодну лампу, яку можна використовувати в якості роутера, який роздає сигнал. Такий вид передачі даних використовує видиме світло, як канал зв'язку, таким чином Li-Fi належить до технологій VLC.

VLC (Visible Light Communication, зв'язок по видимому світлі) - технологія, яка дозволяє джерелу світла, на додаток до висвітлення передавати інформацію, використовуючи той же самий світловий сигнал. Робоча швидкість світлодіода становить 1 мкс, тобто вона буде непомітна для людського ока. Li-Fi влаштована так, що в якості бездротових маршрутизаторів можуть використовуватися електричні світлодіодні лампочки. Паралельна передача даних за допомогою масивів світлодіодів, кожен з яких передає окремий потік, може збільшити швидкість передачі.

Для забезпечення роботи Li-Fi необхідно наступне апаратне забезпечення:

1. Світлодіодна система освітлення.
2. Маршрутизатор, встановлений разом з системою освітлення.
3. Приймач, який оснащений декодером з метою розшифровки світлового сигналу.

Технологія Li-Fi – більш дешева і швидка версія Wi-Fi, яка діє в видимому діапазоні довжин хвиль. Технологія передбачає передачу даних із застосуванням видимого світла зі спектром від 400 ТГц (780нм) до 800 ТГц (350Нм). Li-Fi працює на електромагнітних хвилях. Стандарт IEEE 802.15.7 для Li-Fi визначає фізичний рівень мережі OSI PHY (Physical layer), в тому числі рівень управління доступом до області Media Access Control (MAC-адреса). На поточний момент досягнута практична швидкість становить 1 Гбіт / с, в найближчому майбутньому вона складе 15 Гбіт / с.

Ліщенко Віталій Миколайович
Харківський національний університет Повітряних Сил
ім. Івана Кожедуба
м.Харків

ПРОПОЗИЦІЇ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ СИНХРОНІЗАЦІЇ ПРОСТОРОВО-РОЗНЕСЕНИХ ЕЛЕМЕНТІВ МУЛЬТИРАДАРНОЇ СИСТЕМИ

В роботі запропоновано на базі існуючих оглядових радіолокаційних станцій сформувати мультирадарну систему. Одним з головних завдань імплементації таких систем є синхронізація у часі усіх елементів та організація широкосмугових ліній передачі даних для сумісної обробки даних в єдиному центрі. Розглянуті сучасні методи синхронізації, що можуть бути застосовані в просторово-рознесених мультирадарних системах. Проаналізовано їх переваги та недоліки. Вказані перспективні варіанти, виходячи з необхідної потенційної точності, економічної доцільності та надійності.

З аналізу досвіду ведення збройних конфліктів, сучасних мережецентричних та гібридних війн [1] відомо, що однією з тенденцій ведення збройної боротьби є підвищення ролі малорозмірних повітряних об’єктів (ПО). Основну складність при веденні радіолокаційної розвідки в таких умовах представляє виявлення ПО типу безпілотних

літальних апаратів з малими ефективними поверхнями розсіяння [1]. Запропоновано вирішення означеної проблеми шляхом створення мультирадарної системи (МРС) з більш високим результуючим енергетичним потенціалом. Важливим завданням при побудові МРС є синхронізація всіх елементів системи за єдиною системною шкалою часу та передача значних обсягів інформації для сумісної обробки даних в єдиному центрі. **Мета роботи** — аналіз можливостей сучасних методів синхронізації для об'єднання існуючих оглядових радіолокаційних станцій (РЛС) в МРС.

Розвиток інформаційних технологій, зокрема підвищення пропускної здатності телекомунікаційних систем, розширює функціональні можливості засобів радіолокаційної розвідки. Це дозволяє здійснити реалізацію нових рішень для підвищення якості виявлення ПО. Для забезпечення можливості реалізації багатопозиційних методів виявлення та визначення місцеположення ПО при об'єднанні автономних оглядових РЛС в МРС з сумісним прийомом, необхідно виконання умови синхронізації у часі РЛС (елементів) МРС [2]. Синхронізація полягає у встановленні й підтримці точної часової відповідності сформованих у передавальній частині й прийнятих у приймальній частині сигналів.

Для побудови когерентних МРС актуальними є всі три основних поняття синхронізації: фазова, тактова (символьна) і часова (циклова, кадрова). Для випадку малобазових МРС найбільша ефективність буде отримана при формуванні системної шкали часу від одиниць до десятків наносекунд. Система синхронізації має відповідати вимогам щодо її перешкодозахищеності й живучості [3].

Відомі методи синхронізації можуть бути реалізовані за допомогою сигналів супутникової радіонавігаційної системи, за допомогою радіорелейних ліній S-діапазона та при використанні волоконних оптичних ліній зв'язку. Більш висока точність синхронізації досяжна, незалежно від засобів телекомунікації, при використанні двосторонніх методів передачі сигналів синхронізації у порівнянні з односторонніми за умови рівності інших параметрів.

Висновки. Найкращі можливості використання методів багатопозиційної радіолокації при об'єднанні існуючих РЛС в МРС забезпечуються, якщо використовується високоточна (наносекундна) синхронізація елементів МРС на основі сучасних цифрових технологій з двосторонніми методами передачі даних. Це, в свою чергу, підвищує якість радіолокаційної інформації, що отримується МРС.

Література:

1. *Banasik M. How to understand the Hybrid War / M. Banasik // Securitologia. – 2015. – № 1. –P. 19–34.*
2. *Chernyak V.S. Fundamentals of Multisite Radar Systems / V.S. Chernyak. – Amsterdam : Gordon and Breach Science Publishers, 1998. – 475 p.*
3. *Крючков И.В.Синхронизация подвижных модулей распределенных радиолокационных комплексов / И.В. Крючков, А.А. Филатов. – Вестник МГТУ им. Н.Э. Баумана сер. Приборостроение, 2012. – С. 45–52.*

Ярош В.О
доцент кафедри мобільних та
відеоінформаційних технологій
Огородник А.С
студент
Державний університет телекомунікацій
м. Київ

ОСНОВНІ ЗАВДАННЯ АЛГОРИТМУ САМООРГАНІЗАЦІЇ

ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ

Розглянуто основні причини переходу до програмно-конфігурованих мереж. Наведено основні властивості цих мереж. Сформовано вимоги до алгоритму самоорганізації програмно-конфігурованих мереж

Актуальними тенденціями розвитку телекомунікацій є перехід до мереж майбутнього покоління FGN (Future Generation Network). Згідно з визначенням МСЕ мережа майбутнього [1] являє собою глобальну інформаційну інфраструктуру, яка об'єднує в собі вже існуючі інформаційно-комунікаційні мережі з врахуванням компонент, які тільки плануються до впровадження.

Одним з напрямків модернізації класичного підходу до організації мережевої архітектури є створення програмно-конфігурованих мереж (англ. Software Defined Networks - SDN).

Основною відмінністю програмно-конфігурованих мереж є здатність до самовідновлення та самоорганізації за рахунок її сталості та стійкості до дії стихійних лих. Безвідмовне функціонування SDN під час дії стихійного лиха забезпечує потреби управління державою, оборони, безпеки, охорони правопорядку, економіки країни, а також потреби фізичних і юридичних осіб в новітніх та інноваційних послугах телекомунікацій.

Для досягнення функцій самоорганізації [2] мереж SDN доцільно використовувати алгоритм самоорганізації програмно-конфігурованих мереж (рис.1). На вхід еталонної моделі і основної системи надходить один і той же сигнал. Вихідні величини моделі $\beta_м$ і основної системи β порівнюються в елементі порівняння контуру адаптації. Якщо характеристики моделі і системи не ідентичні, то виникає сигнал непогодженості, який подається на вхід механізму настроювання параметрів для виправлення.

Таким чином, самоорганізація програмно-конфігурованих мереж досягається за рахунок зміни параметрів і структури основного пристрою управління*, а саме повинна мати можливість при змінні зовнішніх або внутрішніх умов її функціонування удосконалювати свою організацію шляхом зміни своєї структури.*

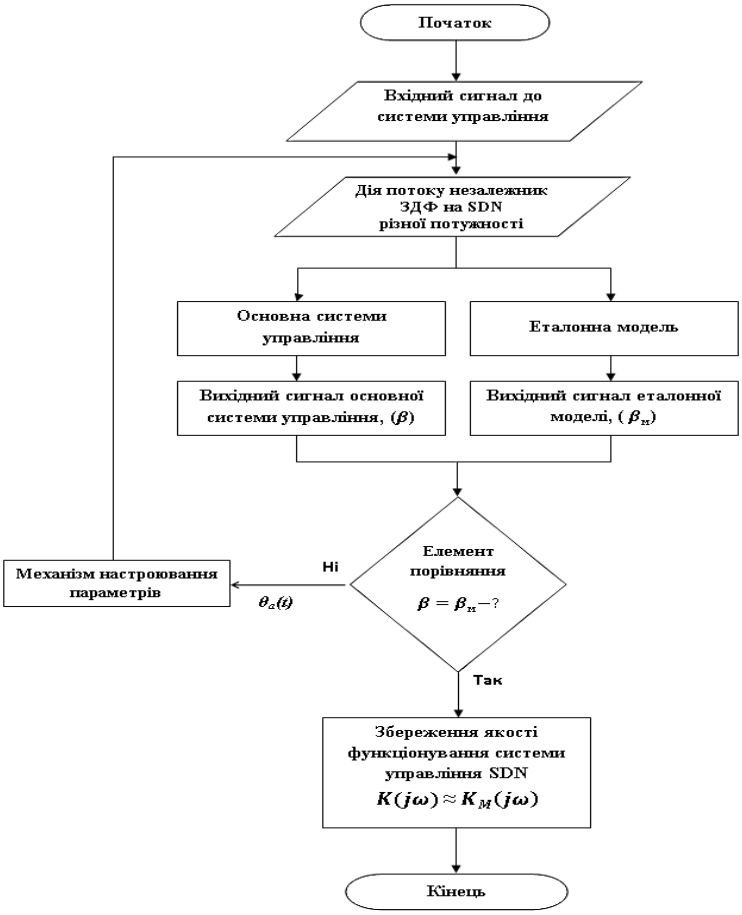


Рисунок 1 – Алгоритм самоорганізації SDN

Список використаної літератури:

1. Global information infrastructure, internet protocol aspects and Next Generation Networks – future networks. Future Networks: Objectives and Design Goals // Recommendation ITU-T Y.3001. – 2011.

2. Ashby W.R. Princi ples of the Self-Organizing Dynamic System // Journal of General Psychology. – 1947. – Vol. 37. – P. 125-128.

Золотухіна Оксана Анатоліївна,
Державний університет телекомунікацій,
м. Київ

УНІФІКАЦІЯ ПРЕДСТАВЛЕННЯ НЕДОСКОНАЛОЇ ІНФОРМАЦІЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ КОНТРОЛЮ ВИТРАТ РЕСУРСІВ

Дані в задачах контролю витрат ресурсів дуже часто мають ознаки недосконалості, що вимагає застосування спеціальних засобів і методів їх представлення та обробки. Розглядаються способи формування нечітких множин для суперечливих, ненадійних та неповних даних інформаційної системи контролю витрат ресурсів. Уніфіковане представлення даних забезпечить можливість застосування нечітких моделей та методів прийняття рішень в задачах управління ресурсами незалежно від характеру недосконалості вхідних даних системи контролю витрат ресурсів.

Дані в задачах контролю витрат ресурсів дуже часто мають ознаки недосконалості, що вимагає застосування спеціальних засобів і методів їх представлення та обробки. Більшість недосконалої інформації може бути представлена у вигляді нечітких множин. До

таких даних відносяться, наприклад, інформація з датчиків (з урахуванням похибки), інтервальні показники (діапазони) або якісні характеристики режимів роботи, обладнання, витратних матеріалів або людських ресурсів. Можливість представлення подібних даних у вигляді нечітких множин витікає з їх сутності: для чисельних даних існують діапазони значень з певними трактуваннями, що дозволяє поставити у відповідність кожному діапазону деяку функцію належності, для визначення функцій належності якісних характеристик можна, наприклад, застосувати метод експертних оцінок [1]. Така нечітка інформація може бути опрацьована із використанням великої кількості існуючих методів та алгоритмів [2].

Для забезпечення можливості застосування нечітких моделей та методів прийняття рішень в задачах управління ресурсами незалежно від характеру недосконалості вхідних даних системи контролю витрат ресурсів пропонується уніфікувати представлення різних видів недосконалої інформації із використанням нечітких множин.

Розглянемо можливі способи формування нечітких множин для суперечливих, ненадійних та неповних даних [3] системи контролю витрат ресурсів.

Суперечливі дані виникають в наслідок наявності інформації про один і той же об'єкт чи процес одночасно в різних джерелах. Кожне із джерел $r_i \in R$ (R - множина всіх джерел для суперечливої ознаки $IncAttr$), формує відповідне значення. При цьому може спостерігатися як ситуація, коли генеровані різними джерелами значення співпадають, так і ситуація, коли дані відрізняються. Для скорочення кількості операцій обробки даних, з усіх джерел r_i, які генерують однакові значення, необхідно залишити тільки одне. Одним із шляхів формування функцій належності може бути використання ваг ресурсів v_i. Вага виражає ступінь достовірності або значущості певного ресурсу для виробничого процесу. Суперечлива характеристика визначається на підставі значення нечіткого даного, яке відповідає джерелу цієї характеристики.

Ненадійні (невизначені) дані характеризуються наявністю ступенів істинності своїх значень. Наприклад, ймовірність того, що при роботі певного обладнання MR у заданому режимі MODE буде витрачено X матеріалів CR, складає N%. Таким чином, функції належності можуть формуватися на підставі ймовірностей значень характеристик.

Неповнота означає, що деякі елементи моделі не мають повної семантики, що приводить до декількох можливих інтерпретацій. Цей вид недосконалості характерний для складних атрибутів, значення яких формується як функція багатьох змінних. Визначення даних з ознаками неповноти можна виконати із застосуванням бази правил, вихідними атрибутами якої є пари *<інтерпретація, експертна оцінка>*. Експертна оцінка може бути виражена лінгвістичним поняттям або чисельним значенням.

Запропоновані засоби перетворення недосконалої інформації дозволяють представити всі дані предметної галузі контролю витрат ресурсів у вигляді нечітких множин. Таке уніфіковане представлення забезпечить можливість застосування нечітких моделей та методів прийняття рішень в задачах управління ресурсами незалежно від характеру недосконалості вхідних даних системи контролю витрат ресурсів.

Література:

1. *Штовба С.Д. Введение в теорию нечетких множеств и нечеткую логику /С.Д.Штовба. - Винница: Издательство Винницкого государственного технического университета, 2001. – 198с.*
2. *Дискретная оптимизация и моделирование в условиях неопределенности данных / Перепелица В. А., Тебуева Ф. Б. – М. : Акад. Естествознания, 2007. – 152 с. : ил.*
3. *Ma Z. M. A Literature Overview of Fuzzy Conceptual Data Modeling/ Z. M. Ma, Li Yan. // Journal of Information Science and Engineering, vol. 26. – 2010. – №2. – P. 427-441.*

Кузьменко М.М., Лосєв М.О., Лосєв Є.О.
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
м. Київ

СТАН СУЧАСНОГО IT-НАВЧАННЯ В УКРАЇНІ

Сфера інформаційних технологій - одна з небагатьох, яка продовжує рости навіть в умовах нестабільності. Ось тільки думки про майбутнє галузі у експертів часто протилежні. Адже дійсно в України є всі шанси для перетворення в потужного IT-гравця на глобальному ринку. Але чи скористається наша країна цим потенціалом? Все залежить від багатьох факторів. Один з них - негайне вирішення проблем в сфері освіти.

Україна займає 38-е місце за рівнем освіти в глобальному рейтингу Організації економічного співробітництва і розвитку (ОЕСР). У нас завжди були дуже талановиті інженери, а якість технічної освіти відомо далеко за межами України. І наші українські інженери сьогодні беруть участь в найскладніших R & D-проектах, створюючи рішення, які рятують людські життя і роблять життя людей у всьому світі яскравіше.

Наприклад, в GlobalLogic часто звертаються компанії зі сфери охорони здоров'я. Так, наші інженери з Харкова беруть участь в розробці програмного забезпечення, завдяки якому працюють кардіостимулятори і інсулінові помпи. Від справності роботи цих медичних приладів залежить здоров'я пацієнта, а іноді і людське життя. Чим більше вплив пристрої на організм, тим жорсткіші вимоги до розробки програмного забезпечення. IT-компанії, які розробляють рішення для сфери охорони здоров'я, регулярно проходять складну сертифікацію на дотримання стандартів якості розробки. Уявляєте, наскільки велика відповідальність лежить на кожному фахівця?

Або інший приклад. Коли ви дивитеся черговий західний серіал, блокбастер або трансляцію Олімпійських ігор, слухаєте концерт або запис відомої групи, з великою ймовірністю ви споживаєте продукт, створений за участю українських інженерів. Тільки дійсно висококваліфіковані фахівці можуть займатися комплексним R & D і створювати такі складні системи.

Українські вузи щорічно готують 16 тис. Випускників IT-спеціальностей. Може здатися, що це значна цифра. Однак конкуренція за технічних фахівців серед IT-компаній ще серйозніше, ніж боротьба за нових клієнтів. Головне питання - як збільшити кількість таких технічних кадрів в Україні?

Ще одна проблема - якість нинішнього IT-освіти. Підготовка молодих фахівців часто не відповідає запитам бізнесу - приступити до реальних проектів вони можуть тільки через три-шість місяців додаткової підготовки після випуску.

Справа в тому, що в останні роки технічні науки в Україні розвиваються не так швидко, як того вимагає ринок. Так, у випускників є серйозні базові знання, розвинений аналітичний підхід до вирішення завдань, але сучасні технічні інструменти їм часто доводиться доучувати самостійно. В першу чергу молодим фахівцям не вистачає практичних навичок роботи над проектами, знань сучасних інструментів і методів розробки або тестування програмного забезпечення.

Лосєв М.О., Кузьменко М.М., Лосєв Є.О.
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
м. Київ

МАШИННЕ НАВЧАННЯ ЯК ТЕХНОЛОГІЯ ІНФОРМАЦІЙНИХ СИСТЕМ

Як тільки ви починаєте розуміти, наскільки легко машинні методи навчання можуть бути застосовані до проблем, які здаються дійсно важкими (наприклад, розпізнавання рукописного тексту), у вас починає з'являтися почуття, що ви можете використовувати

машинне навчання для вирішення будь-якої проблеми і отримати відповідь, якщо у вас буде достатньо даних.

Але важливо пам'ятати, що машинне навчання працює тільки в тому випадку, коли проблема дійсно вирішується з даними, які у вас є.

Наприклад, якщо ви побудуєте модель, яка прогнозує ціни на житло залежно від типу кімнатних рослин в кожному будинку, це ніколи не спрацює. Просто немає ніяких залежностей між кімнатними рослинами в будинку та ціною на цей будинок. Тому незалежно від того, наскільки сильно комп'ютер буде намагатися, він ніколи не зможе вивести співвідношення між ними.

Тому пам'ятайте, що якщо експерт не може використовувати дані для вирішення проблеми вручну, то комп'ютер, ймовірно, також не зможе цього зробити. Замість цього концентруватися на проблемах, коли людина може вирішити проблему, але де би було здорово, якби комп'ютер міг вирішити її набагато швидше.

На мою думку, сама велика проблема з машинним навчанням прямо зараз полягає в тому, що вона в основному живе у світі наукових кругів і комерційних дослідницьких груп. Существует не так багато простих для розуміння матеріалів для тих, хто хотів би отримати широке розуміння, не став фактично експертом. Але з кожним днем ситуація стає все краще.

Дацишин Ігор Валерійович
Одеська національна академія зв'язку ім. О.С. Попова
м. Київ

ОРГАНІЗАЦІЯ ЦИФРОВОГО ТРАНКІНГОВОГО ЗВ'ЯЗКУ СТАНДАРТУ ТЕТРА

Досліджено системи транкінгового зв'язку. Виділено та проведено характеристику цифрових цифрових транкінгових систем TETRAPOL, APCO-25 і TETRA. Визначено переваги системи TETRA та обґрунтовано доцільність її використання. Досліджено характеристики системи та визначено необхідні параметри.

Розвиток систем професійного рухомого радіозв'язку (транкінгових систем рухомого радіозв'язку) характеризується зміною поколінь і переходом від аналогових систем різних стандартів і протоколів (Smartrunk, LTR, MPT1327) до цифрових систем [1].

В результаті проведеного дослідження цифрових транкінгових систем було виділено такі системи як TETRAPOL, APCO-25 і TETRA. Проведений порівняльний аналіз систем показав, що з погляду функціональних можливостей і виконуваних операцій технології TETRAPOL, APCO-25 і TETRA дуже схожі, причому всі ці стандарти розроблені для задоволення потреб замовників, що вирішують такі важливі завдання, як охорона суспільної безпеки, захист державної границі та ін. Система TETRA не здатна взаємодіяти з існуючими системами, що використовують метод FDMA, однак вона забезпечує кращий зв'язок з телефонними мережами загального користування й можливість роумінгу між абонентами особистого й суспільного сектору. Набір функціональних можливостей, розрахованих для стратегічно важливих клієнтів, на противагу можливостям, звичним для стільникових систем, може бути різним у кожному випадку залежно від сегмента ринку. У цілому, система TETRA пропонує більш високі швидкості передачі пакетів даних і більшу ємність каналів у порівнянні із системами APCO-25 і TETRAPOL. На основі проведеного аналізу можна зробити певні висновки: технології, засновані на методі FDMA (APCO-25 і TETRAPOL), виявляються оптимальними для систем з великою зоною охоплення при низької щільності користувачів, у той час як системи, побудовані на TDMA (TETRA) – для менших зон охоплення при високій концентрації користувачів. Додаткова ємність каналів і кращі показники по передачі даних – це переваги систем на TDMA. Хоча набір функціональних можливостей у системах TETRAPOL, APCO-25 і TETRA приблизно однаковий, зниження цін на системи TETRA за рахунок жорсткої конкуренції усе більше спонукує споживачів вибирати саме цей стандарт, щоб мати більш прогресивний протокол

[2]. Усе більш зростаючі потреби в передачі даних і економії радіочастотного ресурсу сприяють поширенню стандарту TETRA [3].

Стандарт TETRA один з найпоширеніших стандартів цифрового радіозв'язку. Перші системи даного стандарту були реалізовані в 1997 році. Стандарт був розроблений Європейським інститутом стандартизації (ETSI) і найбільш широко використовується в Європі, хоча останнім часом одержав розвиток у країнах Азії, Середнього Сходу й СНД. Одним із ключових факторів, що зіграли свою роль у просуванні стандарту в Європі, є більш висока пропускна здатність TETRA у порівнянні з існуючими системами радіозв'язку, що в умовах високої щільності населення й перевантаженістю радіочастотного спектра зіграло основну роль. Використовуваний метод часового доступу до каналів (TDMA) дозволяє передавати 4 розмовних каналу зв'язку в стандартній смузі частот.

Остання версія стандарту TETRA (Release 2, R2) передбачає необхідність інтеграції з мобільними мережами третього й четвертого поколінь, значне збільшення швидкості передачі даних, перехід від спеціалізованих Sim-Карт до універсальних, розширення можливих зон обслуговування. Процес обслуговування викликів у системі стандарту TETRA описується як робота системи масового обслуговування. При проектуванні систем стандарту TETRA рекомендується використовувати калькулятор Ерланга, визначаючи необхідне число радіоканалів і число приймально-передавачів базових станцій залежно від передбачуваного числа користувачів і інтенсивності навантаження. Розрахунки пропускної здатності системи враховує особливості використовуваних у конкретних випадках режиму й дисципліни обслуговування викликів.

Захист інформації – найважливіший аспект побудови системи TETRA, оскільки однією з основних груп користувачів є служби суспільної безпеки, для яких високий рівень захисту – обов’язкова вимога. До стандарту увійшли тільки добре перевірені методи захисту, передусім із систем GSM і DECT. Це механізми аутентифікації мобільного термінала, забезпечення конфіденційності радіоканалу (GSM), а також взаємна аутентифікація термінала з мережею і функції управління ключами кодування (DECT).

Проведено дослідження характеристик мережі транкінгового зв’язку стандарту TETRA. Однією з основних характеристик є завадостійкість мережі, показником якої є відношення сигнал-шум. Також визначено зони покриття через максимально прийнятні втрати при поширенні сигналу. Зоною покриття прийнято називати територію навколо радіопередаючої станції, на межі якої гарантується прийманням з заданою якістю. Дослідження проведені з врахуванням рельєфу місцевості та без, що дозволило визначити більш точний та ідеальний варіант.

Безпосередньому проектуванню самої транкінгової мережі зв’язку стандарту TETRA передує визначення наступних значень: кількість каналів (необхідно обрати оптимальну кількість частотних каналів, що дасть змогу ефективно використати матеріальні ресурси); втрати на трасі (зручно визначати за моделлю Окумура-Хата); баланс потужностей; електроживлення базової станції (максимальна споживана потужність для базових станцій мереж TETRA – 40 Вт); надійність мережі зв’язку (використовуючи параметри надійності такі як середній час відпрацювання на відмову та час відновлення системи, можна обчислити коефіцієнт доступності (готовності) послуг).

Розраховані показники надійності свідчать про задовільні показники якості роботи системи. Система здатна працювати на відмову 13888,89 годин з інтенсивністю відмови в $7{,}2 \cdot 10^{-5}$ 1/год. Зі збільшенням часу випробовування ймовірність безвідмовної роботи зменшується.

Отже, серед безлічі існуючих типів транкінгових мереж найбільш перспективною є цифрова система стандарту TETRA.

Література:

1. Громаков Ю.А. Системы подвижной радиосвязи Технологии

электронных коммуникаций. Том 48. – М.: Эко-Трендз, 1994.

2. Бабков В.Ю., М.А. Вознюк, П.А. Михайлов. Сети мобильной связи: частотно-территориальное планирование. – СПб.: Питер, 2000.

3. Иванов В.И., Гордиенко В.Н. и др. Цифровые и аналоговые системы передачи: Учебник для вузов. – 2-е изд. – М.: Горячая линия – Телеком, 2003. – 232с.

Коба Андрій Борисович
Державний університет телекомунікацій
м. Київ

ЛІЦЕНЗУВАННЯ ПРОГРАМНОГО ПРОДУКТУ

Досліджено комп'ютерну програму як об'єкт авторського права. Досліджено процес ліцензування програмного продукту в Україні.

Вперше у світі комп'ютерну програму зареєстрували як об'єкт авторського права у листопаді 1961 р. в США. Але американці продовжували дослідження щодо доцільності застосування моделі авторського права до комп'ютерних програм, і лише у 1980 р. внесли відповідне доповнення до свого закону про авторське право.

В Україні комп'ютерна програма стала користуватись охороною з набранням чинності Законом України "Про авторське право і суміжні права" від 23 грудня 1993 р. № 3792-XII. Причому ст. 5 цього закону визначала комп'ютерну програму як один з видів літературних письмових творів.

Сьогодні українське законодавство визначає комп'ютерні програми виключно як об'єкти авторського права. Так, ст. 8 Закону про авторські права в редакції від 11 липня 2001 р., що діє на даний момент, визначає комп'ютерні програми як окремий об'єкт авторського права; ст. 18 цього самого закону в повній відповідності з міжнародними конвенціями, учасницею яких є Україна, встановлює, що комп'ютерні програми охороняються як літературні твори незалежно від способу чи форми вираження програм. Разом з тим, ч. 3 ст. 6 Закону України "Про охорону прав на винаходи і корисні моделі" від 15 грудня 1993 р. з наступними змінами й доповненнями визначає, що комп'ютерні програми не можуть одержати охорону згідно з цим законом. З іншого боку, п. 3 ст. 8 Закону про авторські права стверджує, що передбачена цим законом правова охорона поширюється тільки на форму вираження твору й не поширюється на будь-які ідеї, теорії, принципи, методи, процедури, процеси, системи, способи, концепції, відкриття, навіть якщо вони виражені, описані, пояснені, проілюстровані в творі. Це означає, що в Україні охороняються лише форма виразу програм (по суті, вихідний та об'єктний коди), а їхні структура, алгоритми й ідеї, що лежать в основі програм, не підлягають охороні й можуть вільно використовуватись третіми особами.

На практиці порушення прав на програмне забезпечення може здійснюватися у декілька способів. Найбільш поширеними з них є такі: відтворення й розповсюдження програмного забезпечення на дискетах та компакт-дисках; установка "піратського" програмного забезпечення на комп'ютер, що продається; відтворення й розповсюдження програмного забезпечення через Інтернет.

Найскладнішим завданням є виявлення порушень авторських прав на програмне забезпечення шляхом розповсюдження програм по Інтернету. Тут необхідно з'ясовувати безпосередньо в правовласників, чи надавали вони дозвіл на таке розповсюдження, і яким чином користувач може використовувати програму, яку він "скачав" з Інтернету. Так, деякі правовласники розміщують свої продукти (повністю або демо-версії) в Інтернеті й надають право необмеженій кількості осіб використовувати їх, але лише для власних некомерційних цілей.

Залежно від потреб у програмному забезпеченні, внутрішніх процедур, виділення коштів та способів придбання можуть бути вибрані, наприклад, ліцензії, куплені в розстрочку (Open Value або Enterprise Agreement) чи придбані по підписці (Open Value Subscription, Enterprise Agreement Subscription), коробкові ліцензії чи OEM-версії

програмного забезпечення, передустановлені на нові ПК. У кожному з цих варіантів є свої особливості, та використовуватися вони можуть державними та комерційними організаціями на рівних умовах.

Крім стандартних програм для корпоративних клієнтів, для державних установ пропонується також спеціальна програма ліцензування – Microsoft Open License Government. Схема постачання ліцензій за цією програмою здебільшого подібна до стандартних умов програми Microsoft Open License, проте існують і відмінності, а саме – більш низькі ціни на програмне забезпечення для державних замовників.

При придбанні коробкових та OEM-версій підтвердженням ліцензійності продуктів слугують усі компоненти придбаного пакету (ліцензійна угода, носії, документація, купон реєстраційної картки, сертифікат автентичності), а також чек/інвойс, що підтверджує факт придбання продукту. В разі, якщо пакет укомплектований ліцензією в електронному форматі, її рекомендується роздрукувати й зберігати з іншими документами на продукт.

При придбанні корпоративних ліцензій підтвердженням ліцензійних прав є іменний сертифікат.

Збереження зазначених документів здійснюється не тільки для підтвердження ліцензійності продуктів перед правоохоронними органами, а є необхідним для подальшого продажу продукту іншій особі, оскільки в такому разі всі компоненти продукту слід передати цій останній.

Література:

1. *Законом України "Про авторське право і суміжні права" від 23 грудня 1993 р. № 3792-XII – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3792-12.*
2. *Закон України «Про внесення змін до Закону України "Про авторське право і суміжні права"» від 11 липня 2001 р. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2627-14.*
3. *Закону України "Про охорону прав на винаходи і корисні моделі" від 15 грудня 1993 . – Режим доступу: p.http://zakon0.rada.gov.ua/laws/show/3687-12.*

Оробей Віталій Володимирович
Національний авіаційний університет
м. Київ

АЛГОРИТМИ ПОШУКУ В РЯДКУ

Розглянуто деякі з найефективніших алгоритмів пошуку підрядка в рядку. Проведено порівняння описаних алгоритмів зі стандартним (примітивним) алгоритмом пошуку. Наведено рекомендації по використанню того чи іншого алгоритму в залежності від умов проведення пошуку

Інформаційно-комунікаційні технології є сукупністю методів та технічних засобів, що використовуються з метою пошуку, зберігання, опрацювання та поширення інформації.На сьогоднішній день пошук інформації є однією з основних задач комп’ютера. Пошук заданого підрядка в рядку - не складна, але дуже важлива задача для сучасних пошукових систем, систем керування базами даних (СКБД), текстових редакторів, мов програмування, систем перевірки на плагіат тощо. Існує доволі велика кількість алгоритмів аналізу рядків і кожен з них має свої переваги та недоліки. Вибір того чи іншого алгоритму пошуку підрядка потрібно робити в залежності від наступних факторів:

1. Об’єми текстів, в яких потрібно буде проводити пошук.
2. Архітектура процесора. Деякі процесори мають SIDM-операції, які дозволяють швидко порівняти дві ділянки ОЗУ.
3. «Ворожість користувача». Тобто чи буде він навмисно ставити такі дані, на яких алгоритм буде повільно працювати?
4. Чи потрібна оптимізація, або вистачає примітивного алгоритму?
5. Розмір алфавіту. При великих алфавітах таблиця символів буде займати багато пам’яті.

6. Можливість проіндексувати рядок у якому буде проводитись пошук
7. Чи потрібен одночасний пошук кількох рядків, приблизний пошук?

Алгоритм Кнута-Морріса-Пратта (КМП) є одним з найефективніших алгоритмів пошуку підрядка в рядку. Він виконує передобробку шуканого рядка, а саме, на його основі створюється префікс-функція. Наприклад, для підрядкаabcWordabc таким підрядком є abc (також він одночасно є і префіксом, і суфіксом). Переваги використання префікс функції у тому, що можна відкинути свідомо невірні варіанти, тобто якщо при пошуку збіглося 4 символа, на наступній ні, то має сенс продовжувати перевірку не з другого, а з п'ятого символу. Час роботи даного алгоритму залежить тільки від розміру тексту, у якому виконується пошук. Даний алгоритм є дуже швидким, повільнішим лише за алгоритм Бойєра-Мура, однак алгоритм КМП є швидшим при невеликих розмірах текстів. Тому, алгоритм Кнута-Морріса-Пратта можна використовувати як універсальний, коли невідомі розміри текстів і фрагментів текстів, які потрібно знайти.

Алгоритм послідовного пошуку є стандартним алгоритмом для всіх стандартних бібліотек мов програмування, та багатьох текстових редакторів. Він є найпростішим і найбільш неефективним. Принцип його роботи полягає у послідовному проходженні по тексту з кроком в 1 символ і порівнянні всіх підслів з шуканим словом. При цьому виконується дуже велика кількість порівнянь, більшість з яких є зайвими.

Алгоритм Рабіна є модифікацією алгоритму послідовного пошуку. Прохід по слову відбувається аналогічним способом. Різниця полягає тільки в тому, що при проході на словах фіксується деяка числова функція і тоді все завдання зводиться до порівняння отриманих чисел, що є швидше. Якщо значення цієї функції на слові, пошук якого виконується і фрагменті тексту різні, то збігу немає, а якщо однакові, то тільки тоді вже необхідно виконувати перевірку послідовного збігу по буквах. Даний алгоритм хоч і є ефективнішим та швидшим за послідовний алгоритм, але поступається по цим показникам алгоритму КМП та Бойєра-Мура.

Алгоритм Бойєра-Мура вважається найшвидшим і найефективнішим серед алгоритмів призначених для пошуку підрядка в рядку. При його використанні будується таблиця зміщень для шуканого слова (зразка). Далі поєднуються початок рядка і шуканого слова та розпочинається перевірка з останнього символу шуканого слова. Якщо він не співпадає, то зразок зміщується щодо рядка на величину, отриману з таблиці зміщень, і знову проводиться порівняння, починаючи з останнього символу зразка. Якщо ж символи збігаються, проводиться порівняння передостаннього символу і т.д. Якщо всі символи шуканого слова збіглися з накладеними символами рядка, то шукане слово знайдено і пошук завершено. Даний алгоритм є найшвидшим і найефективнішим для великих текстів. У випадку, коли пошук проводиться в невеликому тексті і розмір шуканого слова невеликий, то його ефективність трохи знижується і у такому випадку краще використовувати алгоритм КМП.

Таким чином, можна зробити висновок, що кожен з алгоритмів має як свої плюси так і мінуси. Так реалізація алгоритму може бути дуже простою, але і його ефективність буде доволі поганою. Тому, вибір того чи іншого алгоритму пошуку є доволі важливим і відповідальним завданням.

Література:

1. *Вступ до методів створення програмних продуктів: навч. посіб. для студентів вищ. навч. закл. / С.Л. Кривий. – Чернівці – Київ : Букерк, 2012. – 271с.*
2. *Т. Кормен, Ч. Лейзерсон, Р. Ривест. Алгоритмы: построение и анализ. — М.: МЦНМО, 2000.— с. 801*

Савочкіна Анастасія Юріївна, студент
Свид Ірина Вікторівна, к.т.н., доц.
Харківський національний університет радіоелектроніки

кафедра Радіотехнологій інформаційно-комунікаційних систем
м. Харків

SELENIUM ЯК ІНСТРУМЕНТ ДЛЯ АВТОМАТИЗОВАННОГО ТЕСТУВАННЯ

Більшість програмних продуктів, що існують, - це веб-програми, призначені для роботи в інтернет-браузері. Контроль якості - це дуже важливий крок у створенні продукту, який допомагає створювати безпечні, надійні та зручні програмні продукти. Ефективність тестування таких програм відрізняється в різних компаніях та організаціях. У епоху високої інтерактивності та сумісності в процесі проектування, коли багато організацій використовують методологію Agile, в тій чи іншій формі, автоматизація тестування є необхідністю. Робота присвячена сучасним системам тестування автоматизації.

Починаючи проект по автоматизації тестування, перш за все, необхідно вибрати інструментальні засоби автоматизованого тестування і підготувати персонал. Автоматизоване тестування має безліч переваг, пов'язаних головним чином з високою швидкістю виконання тестів і можливістю виконувати однотипні тести знову і знову. Існує велика кількість як комерційних, так і безкоштовних інструментів, які допомагають в розробці автоматизованих тестів. Selenium, ймовірно, є найбільш поширеним серед інструментів з відкритим кодом [1].

Автоматизоване тестування забезпечує переваги, які можуть підвищити ефективність роботи відділу тестування в довгостроковій перспективі. Автоматизоване тестування дозволяє:

- проводити частіше регресійне тестування;
- швидко надавати розробникам звіт про стан продукту;
- отримати потенційно нескінченне число прогонів тестів;
- забезпечити підтримку Agile і екстремальних методів розробки;
- зберігати сувору документацію тестів;
- виявити помилки, які були пропущені на стадії ручного тестування.

Selenium - це комплект з декількох інструментів, кожен з яких передбачає свій власний підхід до автоматизації тестування. У сукупності набір інструментів Selenium надає багатий набір можливостей, спеціально зібраних разом для тестування всіх типів веб-додатків. Selenium надає кілька варіантів для ідентифікації елементів інтерфейсу, порівняння очікуваного і спостережуваного поведінки тестованої програми. Однією з ключових особливостей Selenium є можливість запуску одних і тих же тестів в різних браузерах [2].

Selenium складається з декількох інструментів, кожен з яких має своє призначення.

1. Selenium 2 (або Selenium Webdriver).

Selenium 2 - останнє поповнення в пакеті інструментів Selenium і є основним вектором розвитку проекту. Це абсолютно новий інструмент автоматизації, який забезпечує відмінний набір можливостей для керування браузером, має більш цілісний і об'єктно-орієнтований програмний інтерфейс (API), а також не має обмежень, властивих більш ранніх версій.

Розробники WebDriver і Selenium прийшли до висновку, що кожен продукт має свої достоїнства, і злиття двох проектів дозволить отримати набагато більш надійний інструмент автоматизації. Результатом цього злиття став Selenium 2. Цей інструмент надає для використання WebDriver API, а в якості ядра може використовуватися як новіша власна реалізація WebDriver, так і реалізація, яка лежала в основі Selenium 1. Крім того, в Selenium 2 вбудований інтерфейс Selenium RC для забезпечення зворотної сумісності. Це, зокрема, дозволяє без особливих зусиль мігрувати існуючі тести на нову версію [1].

2. Selenium 1 (або Selenium Remote Control).

Протягом тривалого часу Selenium RC був основним напрямком розвитку проекту, поки в результаті злиття WebDriver і Selenium не з'явилося Selenium 2, новіший і потужний інструмент.

Selenium 1 все ще активно підтримується (в основному в режимі супроводу), тому що він надає деякі можливості, які все ще недоступні в Selenium 2, включаючи підтримку деяких мов програмування (наприклад, Perl) і підтримку всіляких браузерів [3].

3. Selenium IDE.

Selenium IDE (Integrated Development Environment, вбудована середовище розробки) - інструмент для розробки і створення прототипів тестових сценаріїв. Це плагін для браузера Firefox, з простим і зручним інтерфейсом для створення автоматизованих тестів. У Selenium IDE вбудована функція запису, яка дозволяє записувати дії, що здійснюються користувачем, і потім зберігати їх у вигляді коду на одній з мов програмування, підтримуваних Selenium [1].

4. Selenium Grid.

Selenium Grid дозволяє масштабувати великі тестові набори, а також запускати тести, які необхідно виконати в декількох середовищах. Selenium Grid дозволяє запускати тести паралельно, тобто різні тести можуть бути запущені в один і той же час на декількох віддалених машинах. Це обіцяє дві переваги. По-перше, якщо у вас дуже багато тестів або час виконання ваших тестів занадто велике, ви можете значно збільшити продуктивність за допомогою Selenium Grid, розділивши тести на кілька потоків і запускаючи їх одночасно на декількох серверах. По-друге, якщо тести необхідно запускати в різних середовищах, ви можете налаштувати віддалені сервера відповідним чином і запустити одні і ті ж тести відразу в декількох різних середовищах. В обох випадках використання паралельних процесів в Selenium Grid дозволяє значно прискорити тестування [4].

Більшість людей починає з Selenium IDE. За допомогою IDE ви можете дуже швидко, часом лише за кілька секунд, створювати прості тести. Однак не рекомендується будувати всю автоматизацію тестування на базі Selenium IDE. Для найбільш ефективного використання Selenium, вам необхідно створювати і запускати тести за допомогою Selenium 2 або Selenium 1 в поєднанні з одним з підтримуваних мов програмування. Вибір мови - на ваш розсуд.

Література:

1.Selenium / WebDriver. Автоматизация веб-приложений через браузер. [Електронний ресурс]. – Режим доступу: https://selenium2.ru/. – Дата доступу: 05.05.2018.

2.Satya Avasarala. Selenium WebDriver Practical Guide: Interactively Automate Web Applications Using Selenium WebDriver. - Packt Publishing, 2014, - 246 p.

3.Selenium WebDriver. [Електронний ресурс]. – Режим доступу: https://www.seleniumhq.org/projects/webdriver/ . – Дата доступу: 05.05.2018.

4.Selenium-Grid [Електронний ресурс]. – Режим доступу: https://www.seleniumhq.org/docs/07_selenium_grid.jsp. – Дата доступу: 03.05.2018.

Сметанін Валентин Сергійович, студент
Свид Ірина Вікторівна, к.т.н., доц.
Харківський національний університет радіоелектроніки
кафедра Радіотехнологій інформаційно-комунікаційних систем
м. Харків

ОСОБЛИВОСТІ РОЗРОБКИ ДОДАТКІВ ПІД МОБІЛЬНІ ПЛАТФОРМИ

Розглянуто особливості розробки додатків під мобільні платформи. Проаналізовано платформи мобільних систем та показано, що оптимальним є використання Android-платформи. Визначено основні критерії відбору середовища розробки мобільних додатків та показано, що доцільно використовувати Android Studio.

Смартфони сьогодні - основний пристрій більш ніж для мільярда людей, тому мобільні веб-додатки стали необхідністю як з технічної, так і з комерційної точки зору. Є кілька підходів до розробки таких програм, і, з огляду на, що сьогодні лідируючі компанії можуть за лічені місяці піти на другий план, а нові гаджети з'являються практично безперервно, важливо проаналізувати основні технології створення мобільних веб-додатків. Новий додаток у багатьох випадках буде веб-додатком, тоді як в минулому зазвичай починали зі створення програми спеціально для будь-якої операційної системи, наприклад Windows або Unix. Зараз же актуальна задача створення додатків, здатних працювати на всіх мобільних пристроях, тому дуже непросто прийняти рішення про вибір відповідного інструментарію хоча б через зростаючу кількість платформ та інструментальних середовищ. У зв'язку з цим проаналізуємо види мобільних веб-додатків та які існують підходи до їх створення.

Оцінюючи технології розробки мобільних додатків, слід зазначити, що даний напрямок вимагає вибору критеріїв оцінки.

До основних належать такі критерії: час розробки; наявність фахівців; зручність розробки і налагодження; документація та технічна підтримка; швидкість роботи; юзабіліті; охоплення платформ. Найважливіші з цих критеріїв: вибір платформи і функціональність для визначення найбільш важливих критеріїв розробки, для конкретного додатка та його комерційного успіху.

Рейтинг основних операційних систем на квітень 2017 за матеріалами StatCounter наведено у таблиці 1 [1].

Таблиця 1 - Рейтинг основних операційних систем на квітень 2017 за матеріалами StatCounter

Операційна система	Розробник	Ринкова доля
Android	Google	40,06%
Windows	Microsoft	36,74%
iOS	Apple	12,59%
macOS	Apple	5,88%
others		2,66%
Linux	Canonical та інші	0,77%

Android на сьогодні – найкраща операційна система за темпами збільшення числа своїх користувачів. Ще рік тому Android займала близько 30% ринку, а тепер вже більше 40%. Тобто зростання не припиняється і навіть не сповільнюється.

За даними App Annie [2], галузь мобільних додатків створила колосальні $ 41,1 млрд валового річного доходу, очікується зростання цього показника до $ 50,9 млрд. Згідно з прогнозами Statista, в 2020 році валовий річний дохід перевищить $ 189 млрд. Незважаючи на те, що дані різних аналітиків трохи відрізняються, загальний висновок такий: ринку мобільних додатків ще далеко до насичення.

В залежності від виконуваних функцій слід визначити, якого типу буде додаток. На даний момент існує три види додатків для мобільних пристроїв: нативний додаток; web-додаток; гібридний додаток.

Нативний додаток – це розробка, доступна для однієї платформи пристрою. Особливість в тому, що вони розробляються для конкретної платформи, з використанням «рідних» мов програмування при їх написанні. Якщо додаток створено під конкретну операційну систему, воно добре працює та виглядає органічно. До того ж додаток з легкістю використовує функції програмного забезпечення смартфона, такі як камера, мікрофон, плеєр, і економить ресурси пристрою.

Веб-додатки мають спільні риси з мобільними версіями сайтів, але у них розширений інтерактив. Вони створюються для того, щоб можна було користуватися сайтом через смартфон. Його головна відмінність: додаток не потрібно встановлювати. Вся робота здійснюється через браузер. Різниця між нативною і веб-додатком полягає в можливості вільно управляти інформацією.

Гібридні додатки поєднують в собі функції двох попередніх. Цей додаток працює з програмним забезпеченням смартфону, так як є кросплатформним. Завантажується з магазину додатків, працює через Інтернет. Гібридний додаток – найпопулярніший серед користувачів.

Основним набором інструментом яким повинна володіти платформа для програмування мобільних додатків, є Android SDK. В склад Android SDK входять такі види інструментів як [3]:

- SDK manager (завантажує і встановлює компоненти Android SDK);
- Debug Monitor (призначений для налагодження графічного інтерфейсу);
- Android Emulator (інструмент для тестування програми безпосередньо на комп'ютері);
- AVD manager (створює віртуальні Android пристрої);
- Android Debug Bridge (інструмент для управління емулятором).

Проаналізувавши наступні середовища розробки додатків: Android Studio, Eclipse IDE, Intel XDK, Intel Mobile Development Kit for Android, Intel Beacon Mountain, XCode, та визначивши основними критеріями відбору: різноманітність мов програмування, зручність для користувача інтерфейсу, різноманітність для розробки мобільних платформ, монетизація середовища розробки. Рентабельно використовувати платформу Android Studio. В першу чергу, тому що у неї найзручніший для користувача інтерфейс, багато доступного матеріалу для навчання, цілком достатній спектр мов програмування, безкоштовність користування і найбільший рейтинг цільової платформи в світі, це середовище постійно розвивається і вдосконалюється завдяки компаній Google.

Як видно, з вище зазначеного, на вибір технології та середовища розробки мобільних додатків впливає: контингент для якого розроблюється додаток та необхідне функціональне наповнення додатку. Наявність різноманітного програмного забезпечення дозволяє створювати додатки під мобільні платформи, що можуть задовольнити будь-які вимоги замовників.

Література:

1. *StatCounter. Operating System Market Share Worldwide. [Електронний ресурс]. – Режим доступу: http://gs.statcounter.com/os-market-share . – Дата доступу: 03.05.2018.*
2. *AppAnnie: business intelligence company [Електронний ресурс]. – Режим доступу: https://www.appannie.com/ru/platform/intelligence/?solution=monetize-mobile-app-data. – Дата доступу: 03.05.2018.*
3. *Android Studio [Електронний ресурс]. – Режим доступу: http://developer.android.com/intl/ru/sdk/index.html. – Дата доступу: 03.05.2018.*

Хитров Андрій Олександрович
Національний авіаційний університет,
м. Київ

ВЕЛИКІ ДАНІ

Розглянуто поняття Великі Дані (Big Data) і основні способи їх отримання, зберігання та оброблення. Наведено реальні приклади застосування у таких галузях: енергетика, наука, e-commerce, фінансові системи, IT, телекомунікації.

Big Data – це з одного боку набір технологій, методів, інструментів і підходів, що призначені для рішення проблеми обробки великих об‘ємів даних, а з іншого боку під

BigData розуміють об‘єм даних, який неможливо обробити загальноприйнятими, тобто традиційними способами.

Результати обробки великих масивів інформації використовуються для виявлення закономірностей і тенденцій. Для великих компаній статистика і аналіз даних завжди лежали в основі для ведення бізнесу на великих ринках, але аналітичний підхід став набагато більш необхідним із розвитком телекомунікацій і набагато більш ефективним завдяки наявності потужних обчислювальних машин і сучасним методам обробки даних за допомогою технологій штучного інтелекту.

Великі дані - це сукупність технологій, які покликані здійснювати три операції. По-перше, обробляти великі в порівнянні з «стандартними» сценаріями обсяги даних. По-друге, вміти працювати даними, що швидко надходять у дуже великих обсягах. Тобто даних не просто багато, але їх постійно стає все більше і більше. По-третє, вони повинні вміти працювати зі структурованими і погано структурованими даними паралельно в різних аспектах. Великі дані припускають, що на вхід алгоритми отримують потік не завжди структурованої інформації і що з нього можна витягти більше, ніж якусь одну ідею.

З огляду на величезний обсягів даних особливого значення набуває інфраструктура для їх зберігання і обробки. Але проблема полягає не стільки в нестачі дискового простору, скільки в неадекватності традиційних сховищ для задач Великих Даних.

Зараз отримала визнання ідея озер даних, куди можна записувати дані з багатьох джерел в початковому вигляді і ефективно обробляти. Архітектура озера даних значно еволюціонувала. Тепер вона передбачає наявність ще одного рівня обробки - рівня пам'яті, або Speed Layer. Він додає нові можливості обробки даних в потоці реального часу. Для розподілу потоків даних між різними рівнями зберігання і обробки додані черги, потокові завантаження і т. д.

Незважаючи на невеликий строк існування технології Великих Даних, уже є оцінки ефективного використання на реальних прикладах:

- енергетика (вплив погоди на генерацію енергії), аналіз даних від лічильників, дослідницькі інфраструктури для ефективного використання енергії у приміщеннях;
- наука (Великий адронний колайдер, пан-Європейська інфраструктура для оцінки якості тестуванні наноматеріалів);
- e-commerce (аналіз поведінки і купівельних моделей, інтеграція каналів взаємозв‘язку, моделювання поведінки клієнтів);
- фінанси (рішення по ризикам, аналіз клієнтів);
- IT (аналіз логів від трансакційних систем);
- Телекомунікації (аналіз операцій і збоїв мережі).

Отже, можна зробити наступні висновки: технології являють собою роботу із величезними масивами інформації. Універсального методу їх обробки не існує, але є можливість використання різних методів для часткового рішення даної задачі. Розробка технологій обробки BigDataє перспективним напрямком діяльності.

Література:

1. *Черняк Л. Большие данные – новая теория и практика // Открытые системы. СУБД. – М.: Открытые системы, 2011. - №10. – С. 12-25*
2. *Иванов П.Д., Вампилова В.Ж. Технологии Big Data и их применение на современном промышленном предприятии // Электронное научно-техническое издание «Инженерный журнал: наука и инновации». – М.: МГТУ. – 2014. - №8 (32). – 10 с.*

Дєдов Анатолій Олександрович
студент магістратури

Харківський національний університет радіоелектроніки
Кафедра радіотехнологій інформаційно-комунікаційних систем
м. Харків

ВИБІР АРХІТЕКТУРИ НЕЙРОННОЇ МЕРЕЖІ В ЗАДАЧАХ РОЗПІЗНАВАННЯ ОБРАЗІВ

Робота присвячена аналізу різноманітних підходів до побудови рішень на основі методів штучного інтелекту та машинного навчання у задачах розпізнавання образів. Однією з проблем при розробці програмних продуктів з використанням вищезгаданих підходів є вибір правильної архітектури нейронної мережі, а також інших критеріїв, таких як функції активації, вхідні дані та супроводжувальні технології. В роботі було загально описано існуючі типи архітектур.

Успіхи, що були досягненні в галузі штучного інтелекту, а саме в розпізнаванні образів висунули необхідність розуміння того, в якому випадку можна застосовувати ту чи іншу архітектуру для створення нейронної мережі. Задачі, які зараз вирішуються за допомогою найпередовіших методів машинного навчання, дуже часто потребують значних обчислювальних потужностей і займають багато часу. Тому вибір тої, чи іншої архітектури мережі може зекономити, чи навпаки, відбирати час при тренуванні моделі.

До того ж, вибір архітектури може позитивно впливати на об’єм та якість набору даних для тренування моделі.

Наприклад, якщо у побудованій моделі глибокого навчання (для прикладу візьмемо багатошаровий персептрон, що є класичним прикладом нейронної мережі прямого розповсюдження) є лише три приховані шари по 100 нейронів кожен, і виходом у 10 класів (задача класифікації), і на вхід подається зображення 100*100 пікселів, то кількість кінцевих параметрів буде дорівнювати 1021000 [1].

Для зменшення кількості оброблювальних параметрів та для підвищення ефективності розпізнавання можна застосувати архітектуру згорткових нейронних мереж. Згорткові мережі мають у собі згортковий шар (що по суті є набором карт ознак, у кожної з яких є синаптичне ядро), слої субдескритизації (задача яких зменшити розмір зображення у 2 рази), повнозв’язні шари (як у звичайному персептроні), та шари з функцією об’єднання (рис.1)[2]. Цей тип архітектури обробляє вхідні дані зображення не повністю, а окремими частинами, при цьому, необхідності розбивати вхідні дані немає. Дана архітектура є більш оптимальною за критеріями для вищезгаданої задачі ніж багатошаровий персептрон, за рахунок можливостей паралельних обчислень, що дає можливість використовувати графічні процесори і наприклад, технологію CUDA (англ. Compute Unified Device Architecture).

Якщо взяти нейронну мережу такого типу з наведеними параметрами: 2 згортальних шари по 100 площин кожен (conv. 5x5), повнозв’язний шар на 100 нейронів та вихід у 10 класів, то кількість параметрів буде дорівнювати 68500[1]. Тобто, ефективність архітектури в задачах розпізнавання образів експерементально доведена.

Рекурентні нейронні мережі – інша дуже потужна технологія, у якій структурні зв’язки мають можливість створювати направлену послідовність і таким чином обробляти події у часі. До того ж, ці мережі Тьюринг-повні(універасльні), тобто теоретично можуть реалізувати будь-яку обчислювальну функцію. На відміну від вищезгаданих архітектур, нейрони у рекурентних мережах можуть взаємодіяти самі з собою. До того ж, існує підвид рекурентних нейромереж під назвою: «Довга короткочасна пам’ять»[3]. Вона є універсальною, як було вище згадано, достатньо лише мати параметри вагових коефіцієнтів, що можуть бути розглянуті як її команди. Досить велику ефективність можна отримати якщо об’єднати рекурентні мережі зі згортковими.

До того ж, потрібно мати на увазі те, що вибір архітектури нейромережі може залежати не тільки за рахунок обраної задачі, але і за рахунок вхідних даних (розмірність, вектори ознак, об’єм самих даних і т.д.).

Будь яка архітектура може коригуватися за допомогою гіперпараметрів.

Гіперпараметри – це такі значення, які розробник нейромережі повинен підбирати самостійно, або ж за допомогою стохастичних методів. Серед гіперпараметрів можна виділити такі: кількість прихованих шарів (від 1 до N), момент та швидкість навчання (пов'язано з градієнтним спуском), кількість саме нейронів у кожному шарі (а значить і кількості зв'язків між ними), наявність нейронів зміщення. До того ж, деякі гіперпараметри в кожного типу архітектури можуть бути специфічні.

Підбір кількості нейронів у шарах мережі дуже сильно залежить від необхідної точності вихідних розрахунків, тому чим більше нейронів – тим вихідний результат точніший. Проте, зважаючи про обчислювальну складність системи, рекомендовано не застосовувати архітектурно складні мережі до вирішення тривіальних задач.

Підбір швидкості навчання також в більшості випадків залежить від задачі. Наприклад, обчислення якоїсь простої функції не потребує дуже малого кроку, а от задача прогнозування поведінки об'єкта на відео у реальному часі потребує. Не правильний підбір вищезгаданих гіперпарметрів призводить до поганої сходимості нейронної мережі.

Сходимість – це ще один з критеріїв, що може сигналізувати розробнику про те, чи правильно була підібрана архітектура нейромережі та відповідні гіперпараметри. Сходимість системи можна ідентифікувати по похибці обчислень, що з кожною наступною ітерацією буде зменшуватись. Якщо похибка збільшується або ж застигла на одному рівні, то обрана нейромережа не сходиться. Це можна корегувати за допомогою зміни гіперпараметрів. Також, сходимість може впливати на перенавчання мережі.

Перенавчання – це такий стан нейронної мережі, при якому вона переповнена вхідними даними. Тобто, мережа не буде навчатися на цих даних, а буде їх запам'ятовувати. Тому, при передачі нових даних про об'єкт дослідження, мережа не зможе ідентифікувати ці данні як інформацію про об'єкт. Наприклад, можна подавати на вхід мережі фотографії тільки жовтих автомобілей, а потім подати фото автомобілів зеленого, червоного, чорного кольору тощо, то модель не зможе ідентифікувати в них автомобіль, тому що «вважає», що автомобілі можуть бути тільки жовтого кольору. Також перенавчання може бути викликано занадто складною архітектурою, або занадто великою кількістю параметрів які розробник подає на вхід мережі [2].

Існує багато методів навчання нейронних мереж. Проте, можна виділити один найвідоміший: метод зворотного розповсюдження помилки, в основі якого лежить ідея про градієнтний спуск.

Градієнтний спуск – це засіб знаходження мінімуму чи максимуму функції за допомогою переміщення вздовж градієнта. Градієнт- це вектор, який обумовлює крутизну кривої та вказує на направленість руху відносно обраної точки. Тобто, якщо значення знаходиться в глобальному мінімумі, то помилка при навчанні буде дорівнювати 0. Проте, це не завжди вдається, тому що при розрахунку можна потрапити на локальний мінімум і тоді кінцеве значення помилки буде не вірним. Ця проблема частково вирішується за допомогою придання більшого кроку функції, так названого моменту, що у кінцевому випадку призведе до потрапляння у глобальний мінімум.

Література:

1. *Введение в архитектуры нейронных сетей. – Режим доступу:* https://habr.com/company/oleg-bunin/blog/340184/ *(дата звернення: 10.05.2018).*

2. *Москалев Н. С. Виды архитектур нейронных сетей // Молодой ученый. - 2016. - №29. - С. 30-34. - URL https://moluch.ru/archive/133/37121/ (дата обращения: 10.05.2018).*

3. Нейронные сети для начинающих. Часть 2/ *– Режим доступу:* - https://habr.com/post/313216/ *(дата звернення: 10.05.2018*

Кравчук Анастасія Вікторівна, студент
Свид Ірина Вікторівна, к.т.н., доц.
Харківський національний університет радіоелектроніки
кафедра Радіотехнологій інформаційно-комунікаційних систем

м. Харків

АНАЛІЗ ТА ФОРМУВАННЯ ВИМОГ ДО РОЗРОБКИ БАГАТОФУНКЦІОНАЛЬНОЇ БІЛІНГОВОЇ СИСТЕМИ

Метою роботи є аналіз та формування вимог до розробки багатофункціональної білінгової системи оператора зв'язку. Виконано огляд основних функціональних модулів, що мають бути розроблені та основні вимоги, яким вони мають задовольняти. Наведено принципову схему взаємодії компонентів системи. Актуальність розглянутої теми зумовлена активним ростом ринку інфокомунікаційних послуг та збільшенням спектру «побічних» послуг, що надаються операторами зв'язку.

Основною тенденцією розвитку сучасних інфокомунікаційних систем є конвергенція різноманітних мереж, що означає конвергенцію надання послуг на їх основі, а отже в свою чергу необхідність налаштування білінгових систем на обробку такої інформації. Також слід підкреслити те що, в зв'язку зі збільшенням ринку, кожен оператор намагається максимально орієнтуватися на потреби своїх, або потенційних клієнтів. В цих умовах білінгові системи, як сховище детальної інформації о споживачах, стають не просто архівом з можливістю елементарних розрахунків, але інструментом реалізації ринкової політики оператора.

Таким чином, можна сказати, що сучасна білінгова система – це не тільки система обробки, аналізу та збереження подій використання тих чи інших послуг з можливістю проведення розрахунків, але система, що повинна підтримувати значний обсяг бізнес-логіки компанії. Тому доцільно формувати систему, що буде складатися з декількох, логічно пов'язаних, функціональних модулів. Така архітектура дозволяє реалізувати більш гнучку масштабованість системи під час подальшого її розвитку. Концептуальна схема функціональних модулів білінгової системи наведена на рис. 1.

Розглянемо функціональні модулі, що мають бути реалізовані більш детально:

– Системи самообслуговування – ці системи надають можливість клієнту (абоненту) самостійно керувати станом своїх послуг. Всі системи розгорнуті на базі платформи Hybris для їх більш гнучкої взаємодії та масштабованості. Ці системи можуть розділятися на такі логічні блоки:
  - безпосередньо системи самообслуговування, наприклад особистий кабінет;
  - інтернет-магазин, як приватний випадок системи самообслуговування. Виділяється в окремий модуль так як має більш широкий набір функціональних можливостей:
  - система зовнішнього доступу – така система, до якої клієнт не має безпосереднього доступу, але вона виконує приблизно такі ж функції, що і особистий кабінет, а тому доцільно розгортати їх на тому ж рівні, що і особистий кабінет. Наприклад, робоче місце оператора з обслуговування клієнтів.
– Product catalog - система, що надає можливості створення та управління життєвим циклом тарифних планів, послуг та цінових пропозицій (вартість послуг, знижки). Система складається з бази даних та графічного інтерфейсу користувача. За допомогою інтерфейсу оператор має змогу управляти продуктами або реєструвати нові.
– Web-платформа TIBCO - ця платформа призначена для розгортання web-сервісів, що необхідні для взаємодії систем між собою. Такий підхід, коли всі системи взаємодіють через універсальну "шину" зручний тим, що при зміні технологій в одній системі, інші системи, що звертаються до першої не потребуватимуть змін.
– безпосередньо білінгова система, що реєструє факт використання послуги на основі отриманого CDR-файлу та ініціює збереження детальної інформації про основні характеристики використання послуги, а також плати, що має бути списана з абонента;

– система реєстрації клієнтів - дозволяє реєструвати клієнтів; керувати їх життєвим циклом; назначати їм послуги; переглядати та формувати рахунки на основі переданої білінгом інформації; корегувати баланс на рахунках клієнтів. Ця система, в свою чергу, може розбиватися на менші функціональні під-модулі;

– системи обробки заявок – ці системи працюють в асинхронному режимі та можуть одночасно оброблювати велику кількість абонентів або клієнтів. Такий підхід дозволяє зняти з основної системи обробки клієнтів зайве навантаження, а також перенести виконання великого об'єму робіт, наприклад на нічний час, коли основна активність по роботі з клієнтами маловірогідна.

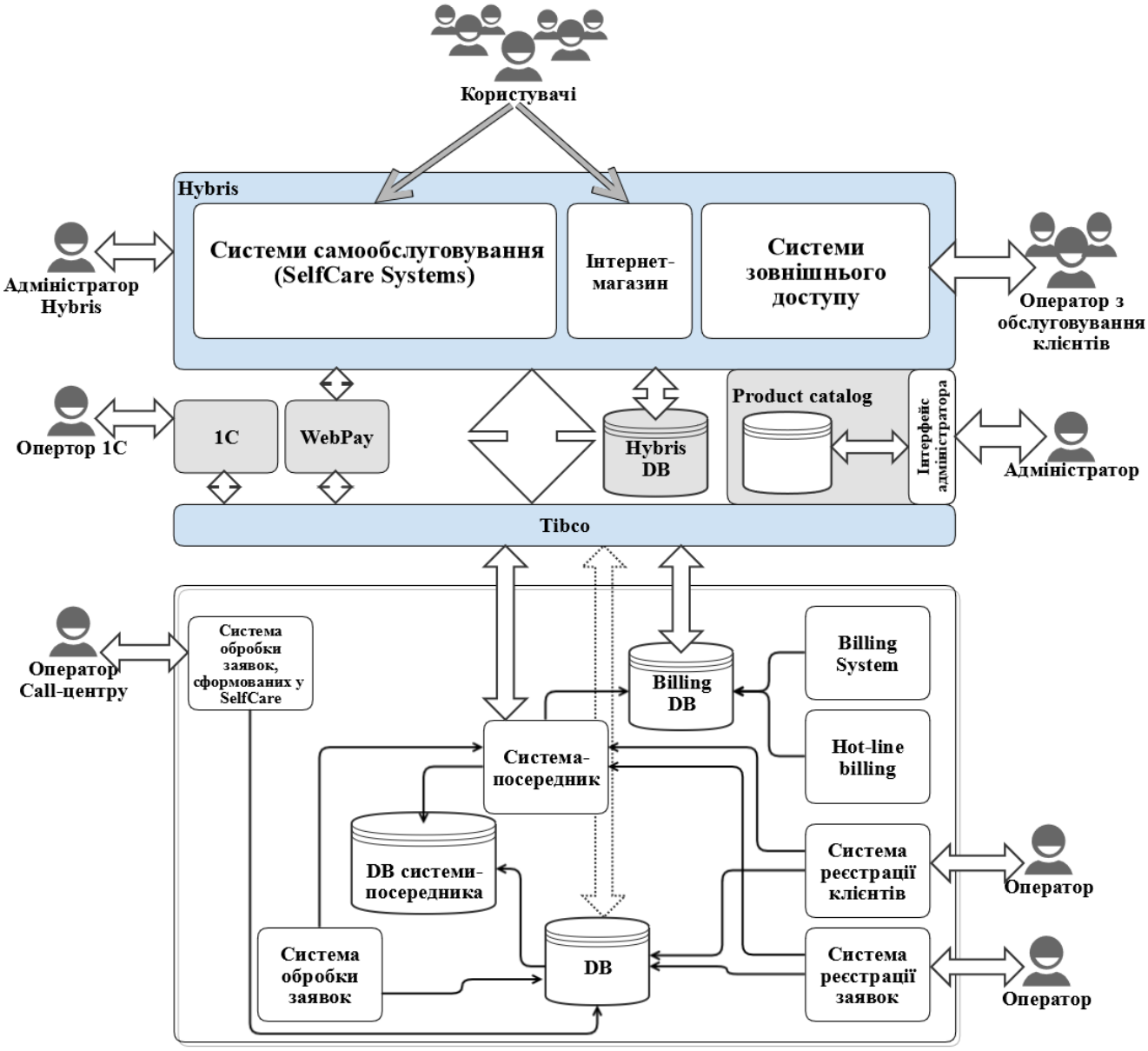


Рисунок 1 – Концептуальна схема функціональних модулів.

Література:

1. *Биллинг [Электронный ресурс] - Режим доступа: www/ URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%B8%D0%BB%D0%BB%D0%B8%D0%BD%D0%B3 - 04.04.18 г. – Загл. с экрана.*
2. *Муссель, К.М. Предоставление и биллинг услуг связи. Системная интеграция [Текст] / К.М. Муссель – М.: ЭКО-ТРЕНДЗ, 2003. – 320с*

Скворцов Юрій Олексійович,
Трифонова Катерина Олексіївна
Одеський національний політехнічний університет,
м. Одеса

КОНТЕНТНО-ЗАЛЕЖНЕ МАСШТАБУВАННЯ ЦИФРОВОГО ЗОБРАЖЕННЯ

В результаті реалізації просторового афінного перетворення, пропорційного масштабування цифрового зображення, виконується зміна розмірів зображення з пропорційним збереженням його контенту. Для врахування вмісту цифрового зображення при виконанні масштабування, застосовують непропорційне або контентно-залежне масштабування цифрового зображення. У поданій роботі виконано дослідження та реалізація непропорційного масштабування цифрового зображення. Досліджені функції визначення важливості пікселів зображення, що є основою представленого алгоритму.

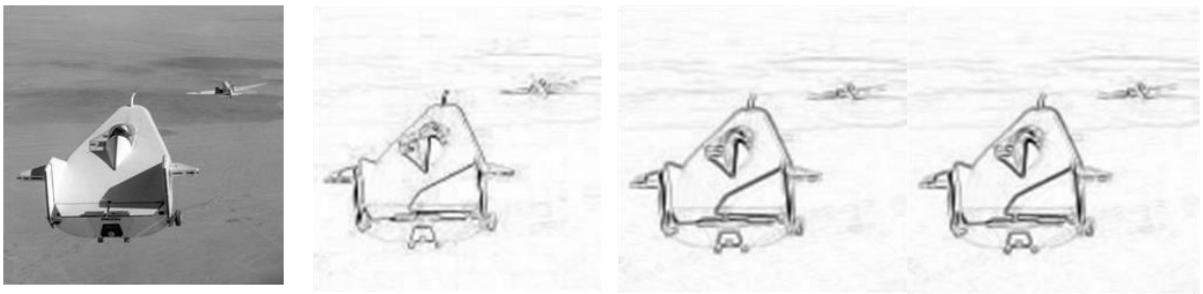
З масовим поширенням різноманітних засобів відтворення та передачі інформації, різного формату, ще більшого застосування отримало масштабування візуального контенту. В даному випадку, окрім реалізації адаптивної верстки відповідного інтерактивного візуального контенту, цифрові зображення, що не можуть бути відображені у повному масштабі, повинні генеруватися у відповідному форматі.

Реалізація ефективної та швидкої інтерактивної взаємодії користувача з візуальним контентом постійно вимагає якісно нових методів обробки цифрових зображень. Саме тому дуже важливою є розробка вдосконалених методів масштабування, що робить тему даної роботи надзвичайно актуальною.

Оскільки основною метою непропорційного масштабування є зміна розмірів зображення за рахунок зміни розмірів незначних ділянок зображення без спотворення вмісту цифрового зображення, тоді першим кроком не пропорційного масштабування є призначення кожному пікселю цифрового зображення його важливості. Для визначення ступеня важливості кожного пікселя застосовують градієнт.

Градієнт цифрового зображення представляє собою напрямок та норму максимальної швидкості зміни яскравості в кожному пікселі цифрового зображення. Найпоширеніший спосіб розрахунку градієнта зображення з використанням ядер фільтрів Робертса, Прюітта або Собеля.

На рисунки 1 для цифрового зображення а) представлено графічне відображення норми градієнта зображення, що отримані за допомогою оператора двомірної кореляції з відповідними ядрами фільтрів.



а) б) в) г)

Рисунок 1. – Графічне представлення модуля градієнта цифрового зображення а) цифрове зображення б) – ядро Робертса в) – ядро Прюітта г) – ядро Собеля

Для непропорційного масштабування цифрового зображення в результаті його збільшення чи зменшення необхідно визначити пікселі з найменшою важливістю, таким чином щоб крім того, щоб врахувати вміст зображення, його кожний рядок (стовбець) змінились на однакову кількість пікселів. Тому в [1] запропоновано будувати ланцюжки пікселів – послідовності пікселів, такі, що в кожному рядку вибрано рівно по одному пікселю, і сусідні пікселі в ньому поєднані сторонами або кутами. Тому наступним кроком алгоритму непропорційного масштабування є побудова матриці мінімальних сум важливості пікселів:

$$m_{y,x} = \begin{cases} g_{y,x} & , y = 1 \\ g_{y,x} + \min\limits_{k=-1}^{1}(m_{y-1,x+k}), & y \neq 1 \end{cases}. \quad (1)$$

Останнім кроком є визначення послідовності координат для подальшого збільшення чи зменшення зображення:

$$l_y = \begin{cases} num(\min\limits_{x=1}^{C}(m_{y,x})) & , y = R \\ num(\min\limits_{k=-1}^{1}(m_{y,l_{y+1}+k})), & y = \overline{R-1,1} \end{cases}. \quad (2)$$

В залежності від обраного способу розрахунку ступеня важливості кожного пікселя цифрового зображення рис.2 а), встановлено відповідно б), в), г) послідовності координат для подальшого збільшення чи зменшення. Визначення якості цифрового зображення в залежності від обраного способу встановлення ступеня важливості пікселів зображення, представляє тему для подальшого дослідження авторів роботи.

а) б) в) г)

Рисунок 2. – Графічне представлення послідовності координат для подальшого збільшення чи зменшення зображення а) цифрове зображення б) – ядро Робертса

Література

1. *Shai, A. Seam Carving for Content-Aware Image Resizing / A. Shai, S. Ariel // ACM Transactions on Graphics. – Vol.26, №10. – 2007. – P. 82–91.*
2. *Делаем Liquid Resize своими руками: [Електронний ресурс] // Хабрахабр. Режим доступу: https://habrahabr.ru/post/48518/ (Дата звернення: 10.04.2018).*
3. *Шийка, Ю. Енергетичні функції в задачах масштабування з врахуванням вмісту растрових зображень / Ю. Шийка, Р. Шувар // Теоретична електроніка. – Вип.60. – 2009р. – С. 139–146.*
4. *Гонсалес, Р. Цифровая обработка изображений в среде Matlab / Р. Гонсалес, Р. Вудс, С. Эддинс. – М.: «Техносфера», 2006. – 616 с.*

Володарець Микита Віталійович, к.т.н.
Український державний університет залізничного транспорту
м. Харків

ЗАСТОСУВАННЯ ANYLOGIC ДЛЯ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ РУХУ ТРАНСПОРТНИХ ЗАСОБІВ В УМОВАХ ЕКСПЛУАТАЦІЇ

Розглянуто можливість застосування пакету програм AnyLogic для імітаційного моделювання руху транспортних засобів в умовах експлуатації, а також підходи, методи і моделі, що покладені в основу цього програмного комплексу. Наведено можливості цього продукту з точки зору транспортного моделювання, а також його основні переваги і недоліки в порівнянні з іншими подібними програмними засобами імітаційного моделювання

Сьогодні вже стало очевидно, що забезпечити баланс пропускної здатності і транспортного попиту тільки за рахунок будівництва нових доріг не можливо. Тому найбільш актуальними є завдання управління транспортним попитом і вдосконалення організації дорожнього руху. Вирішення цих завдань без використання імітаційного моделювання є занадто складним, а в деяких випадках і неможливим. З цією метою був виконаний огляд існуючих програмних продуктів, що дозволяють виконувати імітаційне моделювання на транспорті.

В результаті огляду був обраний програмний комплекс AnyLogic - сучасне середовище розробки моделей на мові Java з російськомовним графічним інтерфейсом і ретельно продуманою контекстною довідковою системою [1, 2]. У сучасному імітаційному моделюванні використовуються такі підходи (методології) [3]: агентне моделювання, системна динаміка, дискретно-подієве моделювання. Кожен з підходів має свою термінологію, свої методології та стандарти. AnyLogic, на відміну від багатьох інших програмних продуктів, дозволяє здійснювати імітаційне моделювання з використанням всіх цих підходів і їх комбінацій. Також це програмний засіб містить велику бібліотеку

візуальних компонентів. Для використання цього продукту досить мати базову підготовку в області інформаційних технологій. Розробник може також створювати і додавати в середу власні компоненти. Моделі зберігаються як Java-аплети. У професійній версії працює відладчик і можна створювати автономні JARфайли. AnyLogic-моделі мають гарні засоби 2D-3D симуляції, інтерактивності і розвинені можливості проведення експериментів (в тому числі оптимізаційних).

Починаючи з версії AnyLogic 7.3 до складу програми була включена Бібліотека дорожнього руху. Вона призначена для детального моделювання доріг, перехресть, розв'язок, під'їздів до складів, виробничих і громадських будинків і включає в себе сім блоків, використання яких дає можливість задати сценарії руху потоків машин. За допомогою елементів розмітки простору можна створити дорожню мережу будь-якої складності [1]. При русі по транспортній мережі машини дотримуються правил дорожнього руху і враховують поточне завантаження смуг. У AnyLogic використовується модифікована версія моделі слідування за лідером. Водій прагне підтримувати швидкість, виходячи з таких параметрів: заданої максимальної швидкості, безпечної дистанції на поточній швидкості до автомобіля, що йде попереду, обмежень швидкості на ділянці і випадкової безпечної відстані при нульовій швидкості (близько метра). При цьому враховується швидкість реакції водія (1 секунда). Кожен автомобіль являє собою агента, який діє як живий водій (враховує дорожню обстановку і приймає рішення по швидкості).

Остання версія AnyLogic 8.2.3 включає в себе [4]: графічні елементи розмітки простору для малювання дорожніх мереж (дорога, перехрестя, автобусна зупинка, парковка, стоп-лінія); вибір шляху автомобіля з урахуванням обмежень швидкості, логіки зміни смуг, вибору менш завантаженою смуги, виявлення (можливих) зіткнень і вжиття заходів щодо їх уникнення на перехрестях; можливість завдання різних типів автомобілів зі специфічними атрибутами і анімацією.

Але на даний момент Бібліотека дорожнього руху не підтримує рух машин заднім ходом і смуги, по яких машини можуть рухатися в обох напрямках (смуги доріг строго однонаправлені). Також неможливо використовувати в одній транспортній мережі смуг руху з різною шириною, при цьому остання задається для всієї мережі однакова, в зв'язку з чим доводиться імітувати рух не по одній більш широкій смузі, а за двома вузьким. Ще одним недоліком є неможливість відображення зупиночних пунктів громадського транспорту на смузі руху без виїзної кишені, що вносить певні похибки в процес імітаційного моделювання. Ще однією відмінною рисою є те, що стандартна бібліотека не передбачає об'єкт трамвай, а його рух доводиться імітувати, як рух будь-якого іншого агента (або створювати новий агент) і по ходу його проходження вносити безліч обмежень, які також будуть впливати на адекватність імітаційної моделі.

Література:

1. AnyLogic [Электронный ресурс] // Официальный сайт компании AnyLogic. – Режим доступа: http://www.anylogic.ru, свободный. – Загл. с экрана. (27.12.2017).

2. Куприяшкин, А.Г. Основы моделирования систем [Текст]: учеб. пособие / А.Г. Куприяшкин; Норильский индустр. ин-т. – Норильск: НИИ, 2015. – 135 с.

3. Григорьев И. AnyLogic за три дня. Практическое пособие по имитационному моделированию / И. Григорьев // Санкт-Петербург. 2017. – 273 с.

4. О системе справочной документации AnyLogic [Электронный ресурс] // Сайт компании AnyLogic. – Режим доступа: https://help.anylogic.ru/index.jsp, свободный. – Загл. с экрана. (27.12.2017).

Mischenko Volodymyr, Yurechko Sergiy
State University of Telecommunications
Faculty of Information Technology
Kyiv

IMPLEMENTATION OF THE 4G NETWORK

Continuously in the field of communications, there is a continuous progress - one after another follows the innovations of telecommunication technologies. Fast and rapid development of personal and local networks, wide-scale implementation of regional networks of wireless networks. A corporate user who needs more and more information has always provided an incentive for the development of all areas of this industry - from phone to Internet -. Access to the Internet and to the Internet, remote work and the emergence of a virtual office - these concepts become today everyday.

The development of wireless communication is accompanied by a continuous change in technology, which every few years adjust the previously made forecasts. The basis of the standards of cellular communication GSM and CDMA, as well as the standards of data transmission systems IEEE 802. Historically, wireless technology developed in two independent areas - the telephone system (cellular) and data communication systems (Wi -Fi, WiMAX). But in recent years there is a clear tendency to merge these functions. Moreover, packet data in third-generation cellular networks (3G) already exceeds the amount of voice traffic associated with the introduction of HSPA technologies. In turn, modern networks of information transfer necessarily provide the given level of quality of services (QOS) for various types of traffic. Support is provided for prioritizing individual streams of information, both at the network, transport levels (at the level of TCP / IP), and at the MAC level (IEEE 802.16 standards). This allows them to use them to provide voice services, multimedia messaging, and the like.

In this regard, the concept of networks of the next, fourth, generation (4G) is inextricably linked (if not synonymous) with the creation of universal mobile multimedia network information transmission. Today, the main promising technologies that are clearly aimed at providing universal communications services are WiMAX and LTE. Moreover, each of them takes its place in the large wireless communications market. The characteristics of the technology are alike, but WiMAX is ahead of LTE for 2 years not only in development but also in the implementation. The main focus of technology is on the efficient use of the spectrum, and most importantly, it is an increase in speed, which increases the quality and quantity of services.

The difference between the two mentioned 4G technologies reflects the origins of their origin. Some are trying to position WiMAX as a broadband standard. LTE is more suited to these tasks, since this technology originated from the world of telecommunications, while WiMAX came to us from the world of data transmission. Most of the major service providers, such as Verizon, have committed themselves to adapt to the 4G version of LTE. Smaller players like Sprint are more attracted to Mobile WiMAX.

The scale of relative success of LTE-Advanced and mobile WiMAX technologies will differ depending on the country and local market conditions. North America does not need broadband access now offered under the mobile WimaX script. They have easy access to the broadband community. However, in those parts of the world where there is no quick access to fixed or mobile broadband access, Mobile Wimax is able to offer significant benefits.

Implementing a further "big step" may look a little seductive. However, the actual state of infrastructure and the economic component in the transition to a new generation of communication technology (4G), indicate that the adaptation of 4G will occur more slowly than it would be desirable for its supporters. In more than 100 countries, operators have already implemented HSPA

(high-speed packet data) technology - or 3G, which is now the most widely used mobile communication technology. Even if the 4G actually reflects a revolutionary approach to increasing the speed of transmission, as its supporters affirm, all of them will have to overcome the enormous inertia of processes during the replacement of the existing base of mobile communications networks. After all, each operator, building a new network, wants to be sure that new speeds, applications and services will be demanded by subscribers, while investment in technology will pay off in a fairly short time.

1.1. Principle of LTE technology

The LTE radio interface is a solution to which operators will gradually move from the current 3GPP and 3GPP2 standards, and its development is an important step in the process of transitioning to the fourth generation 4G networks. In fact, the LTE specification already contains most of the functions originally intended for 4G systems, which is why it is sometimes referred to as the "3.9G technology".

LTE is based on three main technologies: Orthogonal Frequency-Division Multiplexing Multiplexing, Multiple Input Multiple Output MIMO, and System Architecture Evolution Evolution.

Basically, duplex channel separation can be both Frequency (FDD) and Time (TDD).

The exchange between the base station (BS) and the mobile station (MS) is based on the principle of recurring personnel (in LTE terminology - radio frame). Radio frame length - 10 ms. All time parameters in the LTE specification are tied to the minimum time clock Ts = 1 / (2048 · f), where f is the step between the subcarriers, and is standard at 15 kHz. Thus, the duration of the radio frame is 307200 Ts. The same quantum of time corresponds to a clock frequency of 30.72 MHz, which is a multiple of the standard 3G systems (WCDMA with channel band 5 MHz) with a processing frequency of 3.84 MHz (8 3.84 = 30.72).

LTE provides two types of video frames. Type 1 is designed for frequency duplexing - both for a full duplex and for a half duplex. Type 2 radio is intended only for time duplexing.

OFDM technology involves the transmission of a broadband signal by means of an independent modulation, located with a certain step in frequency f. One OFDM symbol contains a set of modulated subcarriers. In the time domain, the OFDM symbol includes a data field (useful information) and a so-called cyclic prefix CP (Cyclic Prefix) - the retransmitted fragment of the end of the previous character. The purpose of the prefix is to combat cross-symbol interference in the receiver due to multi-beam signal propagation. The signal that comes with a delay arrives in the prefix area and does not overlap with a useful signal. LTE adopted a standard step between the sub-carriers f = 15 kHz, which corresponds to the length of the OFDM symbol 66.7 μs.

Each subscriber device (AP) in each cell is assigned a certain range of channel resources in the frequency-range range - the resource grid. The resource cell grid - the so-called resource element - corresponds to one subcarrier in the frequency range and one OFDM symbol in the time domain. Resource elements form a resource block - the minimum information unit in the channel. The resource block has 12 subcarriers (that is, 180kHz) and 7 or 6 OFDM characters, depending on the type of cyclic prefix so that the total cell duration is 0.5 msec. The number of NRB resource blocks in the resource grid depends on the bandwidth of the channel and ranges from 6 to 110 (the bandwidths of uplink and downlink channels in LTE range from 1.4 to 20 MHz). Resource block is the minimum resource element allocated to the subscriber unit by the base station scheduler. The distribution of resources in each cell the base station reports in a special control channel.

– The prefix length of 4.7 μs can be used to deal with the delay of the reflected signal, which has gone a way 1.4 km more than a straightforward signal. For cellular systems in cities this is usually quite enough. If not, an extended prefix is used to ensure that the inter-symbol interference in cells with a radius of up to 120 km is reset. Such enormous cells are useful for various types of broadcast services (MBMS) such as mobile TV. For these same modes (only in the downstream channel), a special cell structure is provided, with a step between subcarriers of 7.5 kHz and a cyclic prefix of 33.4 μs. The cell has only three OFDM characters in it. A special case of a

broadcast service is MBSFN (multimedia broadcast service for single-frequency network) mode. In this mode, several BSs in a specific MBSFN zone simultaneously and synchronously broadcast a common broadcast signal.

– Each subcarrier is modulated using 4-, 16- and 64-position quadrature phase-amlite modulation (QPSK, 16-QAM or 64-QAM). The LTE specification defines several fixed values for the uplink and downlink channel between the BS and ACOM (in the E-UTRA networks). Since OFDM uses Fast Fourier Transform (FFT), the number of formal digital signal processing procedures subjected to simplification must be multiple N = 2n (that is, 128, 256 ..., 2048). In this case, the frequency of the samples should be Fs = f · N. When given in the standard values, it turns out to be a multiple of 3.84 MHz - the standard frequency of samples in technology WCDMA. This is very convenient for creating multi-modal devices that support both WCDMA and LTE. It is clear that when forming a signal, the amplitude of the extra carriers is equated to zero.

– In the downstream and ascending channel, the use of OFDM technology is different. In the downstream channel, this technology is used not only for signal transmission, but also for the organization of multiple access (OFDMA) - that is, for multiplexing subscriber channels.

– In the ascending channel, the permissible radiation power is much lower than in the downstream. Therefore, the primary energy efficiency of the method of information transfer is to increase the coverage area, reduce the cost of the terminal device and the power consumed by it.

– The main drawback of OFDM technology is the high ratio of peak and average signal strength (PAR). This is due to the fact that in the time domain the spectrum of the OFDM signal becomes analogous to Gaussian noise, which is characterized by high PAR. In addition, the OFDMA technology itself, taking into account the need to minimize the step between those that excite and reduce the relative duration of SR, imposes very high requirements for composite signal formation. Not only is the frequency discrepancy between the transmitter and the receiver and the phase noise in the received signal can lead to inter-symbol interference on the ones that individual substitutes (that is, to the interference between the signals of different subscriber channels). At a small step between the sub-carriers and similar effects, the Doppler effect, which is very relevant for cellular systems, envisaging high mobility of subscribers, can also result.

– For LTE, the 3GPP has proposed a new network infrastructure (SAE - System Architecture Evolution). The purpose of the SAE concept is to effectively support the widespread commercial use of any IP-based services and to ensure continuous subscriber service when it is moved between wireless networks that do not necessarily meet 3GPP standards (GSM, UMTS, WCDMA, etc.) (Fig. 2.15).

– Only two types of nodes (evolved NODEB, eNodeB) and Access Gateway (AGW) can be used in the SAE architecture. Reducing the number of node types will allow operators to reduce costs both for deploying LTE / SAE networks and for their further exploitation. The core of the SAE network includes four key components:

– □ The Mobility Management Entity (MME) ensures the storage and management of the service information of the subscriber, authorization of terminal devices in terrestrial networks of mobile communication and general mobility management;

– □ The User Plane Entity (UPE) is responsible for establishing downlink, data encryption, routing and packet forwarding;

– □ 3GPP anchor plays the role of a gateway between 2G / 3G and LTE networks;

– □ The SAE anchor is used to maintain the continuity of the service when moving the subscriber between networks, as appropriate to the 3GPP specifications, and no (I-WLAN and the like).

An important feature of SAE - user data can be forwarded directly between base stations, both via wired and wireless communication (interface X2). This is especially important when hovering, for fast seamless switching between the user. Of course, it is permissible to transfer data between the

BS and through the gateway of the transport IP-network. The ability to directly transmit wireless data between the BS actually means that the SAE architecture incorporates the functionality of the mesh network.

Like all modern wireless communication technologies, LTE supports multi-antenna systems (MIMO). Given the orientation of this technology to the most simple subscriber devices, the technology of MIMO in LTE is as simple as possible. The standard considers MIMO circuits 1, 2 and 4 for transmitting and receiving antennas in various combinations. In MIMO systems there are two main types of transmission - spatial multiplexing and diversified transmission. The first mode means that each antenna channel broadcasts an independent information stream. In this case, the channels themselves should be uncorrelated. Possible two types of spatially-multiplexed transmission - for one SU (MIMO) and for the group AP (MU-MIMO). In the first case, the BS transmits several independent data streams to one AU. At the same time in the AP there should be at least not less antennas than in the BS. In MU-MIMO, resource elements with the same time-frequency parameters should be taken to different APs (thus, there is no reference to the digital formulation of the directional diagram).

1.2. The principle of building WiMAX technology.

WiMAX, Worldwide Interoperability for Microwave Access, sometimes Wireless MAN (Metropolitan Access Network) - a system (network) of wireless transmission to users of various types of information: voice, streaming video (broadcasting), audio (broadcast radio), Internet access guaranteed quality and so on.

WiMAX radio interface is based on the IEEE 802.16 standard:

- 802.16-2004 (without mobility) and
- 802.16e-2005 (with portability).

WiMAX network specifications are based on packet switching technology, IP and Ethernet protocols, as needed. The architecture of the WiMAX network should ensure the independence of the architecture of the access network, including the radio network, from the functions and structure of the transport IP-network. The WiMAX network should be easily scalable and flexible, based on the principles of decomposition (that is built on the basis of standard logic modules, which are united through standard interfaces).

Wimax (BM) base model is a logical representation of WiMAX network architecture. The MB consists of three main elements: the set of subscriber (mobile) stations (MSs), the set of access networks (ASN access service network) and the set of connection networks (CSNs). In addition, the BM includes so-called base points (R1-R8), through which there is a combination of functional modules. Network (ASN) belongs to the Network Access Provider (NAP), an organization that provides access to the radio network for one or more WiMAX service providers (NSPs). In turn, the service provider WiMAX - an organization that provides Wi-Fi connections and Wimax services to end-users. In the frameworks of this model, the service providers Wimax conclude agreements with Internet providers, operators of other networks, access agreements, roaming agreements, and the like. Service providers with respect to the subscriber may be home and guest, each with its own CSN network.

The ASN access network is a set of IEEE 802.16 wireless access base stations (BSs) and gateways for communication with an IP transport network (that is, with a local or global data transmission network). In fact, this network connects the IEEE 802.16 and IP network. The ASN includes at least one BS and at least one ASN gateway. But both base stations and gateways in one ASN can be several, with one BS can be logically linked to several gateways.

The BS in this model is a logical device that supports the IEEE 802.16 protocol suite and external connectivity. Logical BS - single-sector, with one frequency par. Obviously, the real base station is a set of several logical BSs.
The ASN gateway is also a logical device that connects the base stations of one ASN with other access networks and the CSN connection network. The ASN gateway provides connectivity both at the data link layer level and at the management level. For each MS, the base station is logically linked to one gateway. But the actual ASN gateway functionality for each MS can be distributed among several gateways belonging to one or more access networks.
The ASN gateway can be represented as a set of two groups of functional elements - DP - Decision Point and EP (Enforcement Point). ER implements the functions associated with data flow transmission, while DPs focus on functions that do not directly relate to data transmission (for example, the functions of the radio resource management controller of the network). These two function modules are connected through the base point R7. Why the standard introduced such a model, you can only guess. Nowhere else is it disclosed, but without mentioning the possibility of such a decomposition of ASN-gateway functions, it is impossible to explain the presence of R7. In general, the distribution of functions between real gateways and base stations is determined by so-called ASN profiles. Today, three such profiles (A, B, and C) are described.
The CSN connection network is the WiMAX operator's own network, it implements the functions of authorization management, authentication and access (AAA), the connection of Wimax subscribers to global IP-networks, the provision of services such as IP telephony, access to public telephone networks, access to the Internet and private networks, and the like. It is important to note that the Wimax network base model assumes that one ASA access network can be used by several Wimax service providers (each with its own CSN). And on the contrary - one CSN can connect to access networks of different access providers.
The CSN has implemented such functions as providing mobile subscribers with IP addresses and other network parameters for the duration of the network session, the policy server / access control and storage of subscriber profiles, the transmission (tunneling) of data between access and connection networks, WiMAX subscriber billing, and interoperability calculations, tunneling data between different CSNs when roaming, ensuring mobility when leaving an MS outside of one ASN. The following WiMAX services are supported, such as point-to-point connection, authorization and connection to multimedia IP-services, functions of legal interception of traffic, and the like.
The CSN can include elements such as routers, servers (and proxy servers) for authorization functions, authentication, access to the user database, gateways, and the like.
In connection with the support of mobility in the base model of Wimax network introduced the concept of home and guest service providers - H-CSP and V-CSP, respectively. Home NSP is an operator who has signed a service agreement with Wimax subscriber. It is he who implements the functions of authorization, authentication and access control (including billing and collection of subscription fees). To support roaming, the home-based Wimax service provider makes roaming agreements with other NSPs.
Guest NSP (V-NSP) is an operator that provides roaming services to a WiMAX subscriber. First of all, V-NSP provides AAA for this subscriber, as well as full or partial access to all WiMAX network services. There are various ways to route traffic - through the home network connection or directly through the guest CSN network.
At the physical level in the IEEE 802.16e document, there are not too many differences from IEEE 802.16-2004, but they are quite significant. If you do not go into technical details, the essence of the changes on the physical level is to provide greater flexibility for operating in frequency bands of different widths. In fact, it is about maximally efficient use of the frequency resource. This is very important for mobile subscribers, as the mobile operator can not get a 20 MHz frequency band.

literature
1. V.M.Vishnevsky, A.I. Lyakhov, S.L.Portna, I.V.Shahnovich Broadband wireless networks of information transmission. - Moscow: Technosphere, 2005.
V.Vishnevsky LTE Cellular Technology - Nearly 4G Telecommunications Telecommunications / A. Krasilov, I. Shakhnovich. - ELECTRONICS: Science, Technology, Business, 2009, No. 1. - p. 62-72

СЕКЦІЯ №3. БЕЗПЕКА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Богдан Анастасия Сергеевна
Государственный университет телекоммуникаций
Учебно-научный институт защиты информации
г. Киев

ЧТО ТАКОЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ?

Информация в современном обществе стала одним из основных объектов криминального интереса. Каждый человек сталкивается с ситуациями, когда похищаются, искажаются, незаконно распространяются те или иные сведения, наносящие вред личности, коммерческой деятельности, государству.

В процессе хранения и передачи данных субъекты, не соблюдающие безопасность информационного обмена, могут пострадать из-за нарушений конфиденциальности и целостности информации. Наиболее ощутимый ущерб связан с нарушением конфиденциальности, когда сведения, предназначенные лишь для определенного круга лиц, попадают в посторонние руки.

Информационная безопасность телекоммуникационных систем подвержена угрозам широкого спектра: от вирусного заражения, с которым можно справиться локально, до нормативно-правовых коллизий, требующих работы законодательных и правоохранительных органов власти.

Многообразие угроз для телекоммуникационных систем делится на несколько основных видов:

- Информационные (преднамеренные и случайные);
- Аппаратно-программные (например, «шпионские» средства);
- Радиоэлектронные помехи;
- Физические поломки;
- Организационные и нормативно-правовые.

Одними из основных есть информационные угрозы связаны с промахами и нарушениями при сборе информации, ее обработке, сбоями в технологии передачи данных, что приводит к утечке информации, несанкционированному копированию и искажению (подделке). Может происходить блокирование систем и задержка передачи информации. Безопасность нарушается по невнимательности, либо такие угрозы реализуются преднамеренно. К первому варианту часто относится, например, отправление информации по другому адресу, которое в лучшем случае приводит к ситуации «этот неловкий момент», а в худшем – к финансовому и репутационному краху.

Развитие технологий передачи данных требует постоянного изобретения новых методов, позволяющих сохранить конфиденциальность информации, ее целостность, «уйти от

придирчивых глаз» в глобальной деревне информационной паутины. Для защиты от несанкционированного доступа важно, перед тем как передавать носители информации в посторонние руки, обеспечить правильное удаление конфиденциальных данных, ведь файлы, отправленные в корзину обычным способом, можно восстановить. К наиболее известным традиционным методам, которые обеспечивают безопасность при попытках несанкционированного доступа, относится использование систем идентификации для опознавания тех, кто имеет право работать с той или иной информацией. Необходимо защитить систему надежными паролями, которые требуется периодически менять: это снизит вероятость утечки и перехвата данных.

Литратура:

1) https://studfiles.net/preview/1938199/page:29/
2) *https://camafon.ru/informatsionnaya-bezopasnost/telekommunikatsionnyih-sist*

Хоменко Тетяна Анатоліївна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

СИСТЕМИ МОНІТОРИНГУ ТА КЕРУВАННЯ ПОДІЯМИ БЕЗПЕКИ (SIEM)

З кожним днем зростає складність і кількість різних загроз інформаційної безпеки. Разом з цим збільшується і число систем, покликаних захистити бізнес від цих загроз. У 99% великих компаній функціонує міжмережевий екран, антивірусне рішення і система виявлення вторгнення — це сьогодні необхідний мінімум. Крім того, в мережі працюють бази даних, операційні системи та програмне забезпечення власної розробки. Всі ці підсистеми генерують реєстраційні журнали і різні події. А якщо компанія має кілька філій або віддалених офісів, то потік даних від інформаційних підсистем збільшується в десятки разів!

У підсумку адміністратори отримують сотні тисяч повідомлень від безлічі різноманітних підсистем кожен день. Функціонування кожної з підсистем окремо критично для бізнесу в цілому, тому фахівці змушені аналізувати весь цей потік інформації. Виділити важливі повідомлення стає все складніше, і в результаті цінність окремих рішень для забезпечення безпеки прагне до нуля, а час відновлення інформаційної системи після збоїв катастрофічно зростає.

Максимально ефективно використовувати дані, одержані від сенсорів (серверів) виявлення атак і від міжмережевих екранів атаках (про відображених ними атаках) дозволяє використання системи моніторингу інформаційної безпеки. Система моніторингу ІБ дозволяє звести всі події та інциденти ІБ в єдиній консолі, виконує інтелектуальний аналіз атак та їх наслідків і допомагає адміністраторам виробити контрзаходи. Крім цього, система моніторингу ІБ виконує реєстрацію та зберігання всіх подій інформаційної безпеки, що робить можливим використання отриманого матеріалу в якості доказового при виконанні розслідувань інцидентів та судочинстві.

Основні можливості SIEM-систем:

- Збір інформації про події з різних пристроїв забезпечення інформаційної безпеки і мережевих пристроїв;
- Візуалізацію подій в режимі реального часу;
- Підтримку сигнатурних і «поведінкових» методів виявлення аномалій і атак;
- Можливість створення власних правил кореляції;
- Можливість управління активними мережевими пристроями з метою блокування шкідливого трафіку;
- Прогнозування результатів атаки;
- Аналіз ризику захищаємої системи;
- Автоматичне визначення статусу події (атака, сканування тощо);

- Можливість обробки та аналізу інцидентів безпеки;
- Фокусування уваги на пріоритетних захищаємих вузлах;
- Вбудована система роботи з інцидентами, можливість інтеграції з існуючою;
- Автоматична реакція на інциденти.

Впровадження системи моніторингу подій інформаційної безпеки дозволить компанії досягти наступних переваг:

- забезпечити централізоване управління подіями і інцидентами ІБ
- збільшити швидкість виявлення, розслідування та реагування на інциденти
- управляти інцидентами ІБ
- підвищити ефективність управління ризиками ІБ
- підвищити рівень відповідності політикам і нормативним вимогам

Література:

1. *http://integritysys.com.ua/security/utm/*
2. *https://www.my-itspecialist.com/ru/network_perimeter_security/*

Кисельов Олексій Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

БЕЗПЕКА БАЗ ДАНИХ ТА ЇХ ВРАЗЛИВОСТІ

Атаки на сховища і БД є одними з найнебезпечніших для підприємств і організацій. Згідно зі статистикою компанії infowatch [1], в останні роки кількість витоків даних в світі неухильно зростає, при цьому на 2017 – поч. 2018 року понад тридцять відсотків з них припадають на зовнішніх порушників і більше шістдесяти виконано за участю співробітників організації. Навіть якщо припустити, що в ряді випадків витік включала дані, до яких співробітник має легальний доступ, кожен третій випадок припадав на зовнішню атаку. Обсяг скомпрометованих в світі в результаті витоків записів даних, в тому числі номерів соціального страхування, реквізитів пластикових карт та іншої критично важливої інформації, на кінець 2017 року складав 13,3 млрд записів.[2]

Питання комплексної безпеки БД привертають увагу дослідників, їм щорічно присвячується ряд робіт як в Україні, так і за кордоном. Можна відзначити дослідження, в якому розглядаються підходи до забезпечення конфіденційності, цілісності та доступності СУБД, запобігання, визначення та подолання атак. Пропонуються підходи до забезпечення мандатної і рольового дискреційного доступу до реляційного сервера. З усіх моделей безпеки найзручнішою для користувачів є рольова модель, проте вона найскладніша для адміністрування. За допо- могою мандатної моделі можна створювати багаторівневі системи захисту. Найпростішою моделлю є дискреційна, але вона може вияви- тися надмірно детальною. Методи ідентифікації та аутентифікації користувача (внутрішня,зовнішня,біометрична і парольна). З усіх схем аутентифікації найчастіше використовується парольний захист, зважаючи на дешевизну і простоту. Часто використовується зовнішня аутентифікація за допомогою парольного захисту ОС, оскільки це зручно для користувачів. Досить пошире- ною є аутентифікація за допомогою токенів. Перспективною є біометрична аутентифікація Запроваджуються методи посиленої безпеки СУБД: криптографія, управління безпекою засобами мови SQL. У сучасних СУБД широко використовується прозоре шифрування, оскільки при цьому дані завжди зашифровані, хоча це створює додаткове навантаження на центральний процесор. Окрім цього, при про- зорому шифруванні користувачу не треба змінювати свої програми. Спільне використан- тання симетричних і асиметричних методів шифрування підвищує ефективність СУБД та

зменшує їх завантаженість. Обов'язковою частиною системи без- пеки СУБД є системи резервного копіювання (відновлення) і аудиту. Резервне копіювання і відновлення в сучасних СУБД може здійснюватися через графічний інтерфейс, а також за допомогою команд SQL. Мова SQL відіграє важливу роль у захисті СУБД. За допомогою команд SQL можна виконувати практично всі аспекти за- хисту СУБД. Для ефективного захисту БД в СУБД потрібен комплексний, систематичний підхід, необхідне поєднання різних сервісів безпеки та їх механізмів.

В архітектурному плані [5] виділяють наступні підходи:

- повний доступ всіх користувачів до серверу БД;

- поділ користувачів на довірених і частково довірених засобами СУБД (системи управління БД);

- введення системи аудиту (логів дій користувачів) засобами СУБД;

- введення шифрування даних; винос коштів аутентифікації за межі СУБД в операційні системи і проміжне ПО; відмова від повністю довіреної адміністратора даних.

Список основних вразливостей СУБД не зазнав істотних змін за останні роки. Проаналізувавши засоби забезпечення безпеки СУБД, архітектуру БД, відомі уразливості і інциденти безпеки, можна виділити наступні причини виникнення такої ситуації:

проблемами безпеки серйозно займаються тільки великі виробники;

програмісти баз даних, прикладні програмісти і адміністратори не приділяють належної уваги питанням безпеки;

різні масштаби і види збережених даних вимагають різних підходів до безпеки;

різні СУБД використовують різні мовні конструкції для доступу до даних, організованих на основі однієї і тієї ж моделі;

з'являються нові види і моделі зберігання даних.

Багато уразливості зберігають актуальність за рахунок неуваги або незнання адміністраторами систем баз даних питань безпеки. Наприклад, прості SQL-ін'єкції широко експлуатуються сьогодні по відношенню до різних web-додатків, в яких не приділяється достатньої уваги вхідних даних запитів.

Проте, введення засобів захисту як реакції на загрози не забезпечує захист від нових способів атак і формує розрізнене уявлення про саму проблему забезпечення безпеки. З одного боку, великі компанії можуть виділити достатню кількість коштів забезпечення безпеки для своїх продуктів, з іншого боку, саме з цієї причини є велика кількість різнорідних рішень, відсутнє розуміння комплексної безпеки даних (і її компоненти відрізняються від виробника до виробника), немає загального, єдиного підходу до безпеки сховищ даних і, як наслідок, можливості. Ускладнюються прогнозування майбутніх атак і перспективна розробка захисних механізмів, для багатьох систем зберігається актуальність вже давно відомих атак, ускладнюється підготовка фахівців з безпеки.

Саме розробка програмних засобів перспективної захисту (на випередження зловмисника), забезпечення можливості впровадження такої технології представляються авторам статті найбільш актуальними завданнями на поточному етапі.

Незалежними від даних можна назвати наступні вимоги до безпечної системі БД:

Функціонування в довіреної середовищі.

Під довіреної середовищем слід розуміти інфраструктуру підприємства і її захисні механізми, обумовлені політиками безпеки. Таким чином, мова йде про функціонування СУБД відповідно до правил безпеки, що застосовуються і до всіх інших систем підприємства.

Організація фізичної безпеки файлів даних.

Вимоги до фізичної безпеки файлів даних СУБД в цілому не відрізняються від вимог, що застосовуються до будь-яких інших файлів користувачів і додатків.

Організація безпечної і актуальною настройки СУБД.

Дана вимога включає в себе загальні завдання забезпечення безпеки, такі як своєчасна установка оновлень, відключення невикористовуваних функцій або застосування ефективної політики паролів.

Наступні вимоги можна назвати залежними від даних:

Безпека призначеного для користувача ПО.

Сюди можна віднести завдання побудови безпечних інтерфейсів і механізмів доступу до даних.

Безпечна організація і робота з даними.

Питання організації даних і управління ними є ключовим в системах зберігання інформації. У цю область входять завдання організації даних з контролем цілісності та інші, специфічні для СУБД проблеми безпеки. Фактично це завдання включає в себе основний обсяг залежать від даних вразливостей і захисту від них.

В кінцевому випадку усі системи захисту зловмисники можуть «обійти» тільки через недбалість самих працівників, які не дотримуються регламенту політики безпеки персональних даних, платіжних систем та інших, які мають конфіденційну, службову або таємну інформацію з обмеженим доступом. Шукаючи і використовуючи вразливості СУБД зловмисники можуть навіть за допомогою Google Dorks викрасти особисту інформацію, яку ідентифікує пошукова система, про фізичну чи юридичну особу, згодом використавши це у своїх цілях. І все це через недолугість користувачів. На більш захищені системи винаходять більш руйнівні методи атак.

Література:

1)http://www.tadviser.ru/index.php/

2) irbis-nbuv.gov.ua/.../cgiirbis_64.exe?...

3)http://www.swsys.ru/index.php?page=article&id=4175&lang=

4) https://tproger.ru/articles/db-security-basics/

Чорний Валерій Анатолійович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

КІБЕРЗАГРОЗИ У ХМАРНИХ ТЕХНОЛОГІЯХ

В даний час все більшої популярності набувають «хмарні технології». Це пов'язано з бурхливим розвитком Інтернету і супутніх технологій. На багатьох підприємствах люди працюють у віддаленому режимі, передаючи всю необхідну інформацію через інтернет.

Хмарні технології надають споживачам рішення, повністю готові до роботи. Достатньо володіти будь-яким пристроєм, здатним з'єднатися з інтернетом, і можна отримати доступ до віддаленої бази, яка розташовується на віддаленому сервері.

Хмарні технології відкривають нові можливості для підключення віддалених і сезонних працівників. Збільшуючи кількість персоналу, керівник може як підключати співробітників до хмарного сервісу так і відключати неактивних користувачів.

Розглянемо основні термінології:

Хмарні технології – це технології обробки даних, в яких комп'ютерні ресурси надаються Інтернет користувачеві як онлайн сервіс, одна велика концепція, що включає в себе багато різних понять, що надають послуги.

Хмарний сервіс – послуга надання хмарних ресурсів за допомогою технологій «хмарних обчислень».

Хмарні обчислення (англ. cloud computing) – це програмно-апаратне забезпечення, доступне користувачеві через Інтернет або локальну мережу у вигляді сервісу, що дозволяє використовувати зручний інтерфейс для віддаленого доступу до виділених ресурсів

(обчислювальних ресурсів, програм і даних). Комп'ютер користувача виступає при цьому рядовим терміналом, підключеним до Мережі. Комп'ютери, які здійснюють cloud computing, називаються «обчислювальною хмарою». При цьому навантаження між комп'ютерами, що входять в «обчислювальну хмару», розподіляється автоматично.

Переваги хмарних обчислень

Перевагами хмарних обчислень є те, що користувач має можливість не купувати потужні комп'ютери. Зокрема, і організації можуть відмовлятися від придбання потужних серверів і йти "в хмари". Для розробника – контрольованість усього процесу. У разі виникнення проблеми їм істотно простіше буде змоделювати ситуацію, що викликала помилку, – адже усі дані і так зберігаються в них. Користувач оплачує послугу тільки тоді коли вона йому потрібна, а найголовніше він платить тільки за те, що використовує.

Хмарні технології дозволяють економити на придбанні, підтримці, модернізації ПЗ і устаткування.

Масштабованість, відмовостійкість і безпека – автоматичне виділення і звільнення необхідних ресурсів залежно від потреб додатку. Технічне обслуговування, оновлення ПЗ здійснює провайдер послуг.

Віддалений доступ до даних у хмарі – працювати можна з будь-якої точки на планеті, де є доступ в мережу Інтернет.

Недоліки хмарних обчислень

Розглядаючи переваги "хмарних" обчислень, варто сказати і про недоліки, з якими зв'язаний перехід на "хмари". Найбільш суттєвий з них – загроза інформаційної безпеки. В умовах жорсткої конкуренції, найбільше компанії бояться витоків даних з мережі "хмарного" провайдера внаслідок перехоплення інформації, втрати контролю над даними і додатками, неможливості знищення даних, дій інсайдера на стороні провайдера або інших користувачів "хмари". Для захисту можна використовувати шифрування даних або їх знеособлення. При цьому шифрувати треба не лише ті дані, що зберігаються в провайдера, а й канал зв'язку з ним. Проте доки рішення, які дозволяли б ефективно захищати дані в "хмарі", не вироблені.

Ще одним недоліком можна назвати прив'язку "хмарної" технології до конкретного постачальника послуг, збої на стороні провайдера, вихід з ладу інтерфейсу адміністрування, банкрутство і поглинання оператора. Компанії не даремно побоюються цих подій, оскільки це може принести їх бізнесу значний матеріальний збиток.[1]

На сьогоднішній день проблеми виявлення, розслідування та запобігання кіберзлочинам є надзвичайно актуальними. Впровадження сучасних технологій в економіці, управлінні, кредитово-банківській діяльності, стрімкий розвиток інформаційних і телекомунікаційних технологій на основі використання глобальної інформаційної мережі Інтернет зумовило зростання злочинних проявів у різних сферах діяльності людини.

Одним із аспектів розповсюдження широкого діапазону кіберзлочинів, які включають злочини, що здійснюються з метою отримання фінансової вигоди, злочини, пов'язані з використанням інформації, що знаходиться в комп'ютері, а також злочини, направлені проти конфіденційності, цілісності і доступності комп'ютерних систем, стає небезпека хмарних технологій.

Термін «хмара» (Cloud) широко використовують для позначення різних технологій та послуг в телекомунікаційній індустрії, як абстрактне позначення мережі в системних діаграмах його застосували вперше, а вже потім в Internet, який в теперішній час відіграє фундаментальну роль у хмарних обчисленнях (Cloud computing), оскільки представляє собою платформу, за допомогою якої сервіси хмарних обчислень стають доступними споживачам.

Згідно з визначенням Національного інституту стандартів і технології (NIST) у США, хмарні обчислення – це модель забезпечення повсюдного та зручного доступу на вимогу, через мережу до спільного пулу обчислювальних ресурсів (наприклад, до комунікаційних

мереж, серверів, засобів збереження даних, прикладних програм та сервісів), які можуть бути забезпечені та оперативно надані з мінімальними управлінськими затратами чи зверненням до провайдера послуг. «Хмарою» метафорично називають Інтернет, який приховує всі технічні деталі. Застосовують класифікацію за критерієм надання прав доступу до сервісів та ресурсів адміністративним центром хмари, за яким виділяють чотири типи хмарних обчислень:

1) публічні хмари, які відкриті для широкої публіки;
2) приватні хмари, які розгорнуто на приватному обладнанні та в приватних цілях;
3) гідридні хмари, які є комбінацією двох попередніх типів;
4) суспільні хмари, які характеризуються мульти-адміністративними правами керування, є поєднанням всіх попередніх типів та створюються для дуже специфічних цілей.

В Україні використання систем хмарних обчислень регулюється загальними нормами законів про інформацію та її захист і положеннями приватного права. В свою чергу, у Верховній Раді України 24 березня 2016 року зареєстровано Проект Закону «Про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень», який має виправити ситуацію із розпоряджанням інформацією.

Із прийняттям вказаного проекту можна говорити про гарантії захисту інформації та забезпечення виконання належним чином обов'язку із її зберігання провайдером шляхом запропонованого у вказаному Проекті переліку чисельних істотних умов, які мають міститись у договорі між надавачем хмарних послуг та володільцем інформації або власником системи. Головними із них є: порядок отримання володільцем інформації або власником системи інформації, яка оброблялась в системі хмарних обчислень, у випадку припинення надання хмарних послуг; порядок видалення інформації із системи хмарних обчислень; відповідальність сторін договору.

Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом використовуються засоби захисту інформації, які мають сертифікат відповідності чи позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації. Це означає, що для роботи державних інформаційних ресурсів за допомогою хмарних обчислень або для обробки інформації із обмеженим доступом кожному із осередків розміщення інформаційної інфраструктури системи необхідно бути сертифікованим відповідно законодавства України.

Існує ряд проблеми, пов'язаних з безпекою хмарних обчислень, але ці питання діляться на дві великі категорії: питання безпеки, з якими стикаються під час використання хмарних послуг (організації, які надають програмне забезпечення, платформи, чи інфраструктуру як послуги через використання хмарних технологій) і питання безпеки, з якими стикаються їх клієнти (компанії або організації, які розгортають додатки або зберігають дані на хмарі). Відповідальність йде в обох напрямках, тобто: постачальник повинен гарантувати, що їх інфраструктура знаходиться в безпеці і що дані та додатки клієнтів захищені, в той час як користувач повинен вживати заходи, щоб зміцнювати їх застосування, використовувати надійні паролі і перевірку автентичності.

Користувач стає залежним від провайдера хмари та може втратити контроль над інформацією. В такому випадку гостро постає питання порядку витребування інформації у незаконного володільця й відшкодування завданої шкоди за допомогою загальних засобів захисту цивільних прав.

Широке використання віртуалізації в реалізації хмарної інфраструктури спричиняє проблеми безпеки для клієнтів або орендарів публічного хмарного сервісу. Віртуалізація змінює відношення між ОС і базовим обладнанням – будь то обчислення, зберігання чи мережі. Це вносить додатковий шар – віртуалізації – що сам по собі повинен бути правильно налаштований та закріплений. Певні проблеми мають можливе рішення – компромісне

програмне забезпечення віртуалізації, або «гіпервізор». У той час як ці проблеми мають здебільшого теоретичний характер, вони все ж існують.

Коли організація вибирає для зберігання даних або розгортання додатків публічному хмарі, вона втрачає можливість мати фізичний доступ до серверів з інформацію. В результаті, конфіденційні дані не зазнають ризику інсайдерських атак. Згідно з недавнім звітом від Cloud Security Alliance, інсайдерські атаки треті за величиною загрози в області хмарних обчислень. Таким чином, постачальники хмарних послуг повинні забезпечити, ретельні перевірки для співробітників, що мають фізичний доступ до серверів в центрі даних. Крім того, центри обробки даних повинні постійно контролювати підозрілу активність.

Для того, щоб зберегти ресурси, скоротити витрати, та зберегти ефективність, провайдери хмарних послуг часто зберігають більше одного разу дані клієнта на тому ж сервері. В результаті, існує ймовірність того, що особисті дані одного користувача можуть бути доступні іншим користувачам (можливо, навіть конкурентам). Для вирішення таких складних ситуаціях, постачальники хмарних послуг повинні забезпечувати правильну ізоляцію даних і логічні сегрегації зберігання.

Отже, хмарні обчислення – наступний етап інформаційного розвитку людства. В Україні досі залишається відкритим процес формування нормативно-правової бази врегулювання відносин з приводу їх використання. Досі для появи на теренах нашої держави послуг з надання хмарних сервісів вистачало лише договірного регулювання, однак для їх вдосконалення і подальшого поширення в українське законодавство мають бути внесені зміни з обов'язковим врахуванням розвитку хмарних технологій.[2]

Література:

1) http://academicfox.com/lektsiya-1-osnovni-ponyattya-hmarnyh-tehnolohij/

2) http://mdu.in.ua/Nauch/Konf/2017/zbirnik_kiberbezpeka.pdf

Загиней Антон Юрійович

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

ВРАЗЛИВОСТІ МАРШРУТИЗАТОРІВ GPON

У цій статті показані основні принципи роботи системи з використанням технології GPON. Дві вразливості, які використовували хакери для здійснення атак.04.05.2018 року було здійснено атаку на маршрутизатори GPON з використанням двох вразливостей.

GPON - представник сімейства пасивних технологій оптичних мереж доступу PON.

Суть технології PON (passive optical network) полягає в тому, що між приймально-передавальним модулем центрального вузла OLT (optical line terminal) і віддаленими абонентськими вузлами ONT (optical network terminal) створюється повністю пасивна оптична мережа, що має топологію дерева. У проміжних вузлах дерева розміщуються пасивні оптичні розгалужувачі (splitters) - компактні пристрої, які не потребують електроживлення та обслуговування. Один приймально-передавальний модуль OLT дозволяє передавати інформацію безлічі абонентських пристроїв ONT. Число ONT, підключених до одного OLT, може бути настільки великим, наскільки дозволяє бюджет потужності і максимальна швидкість приймально-передавальної апаратури.

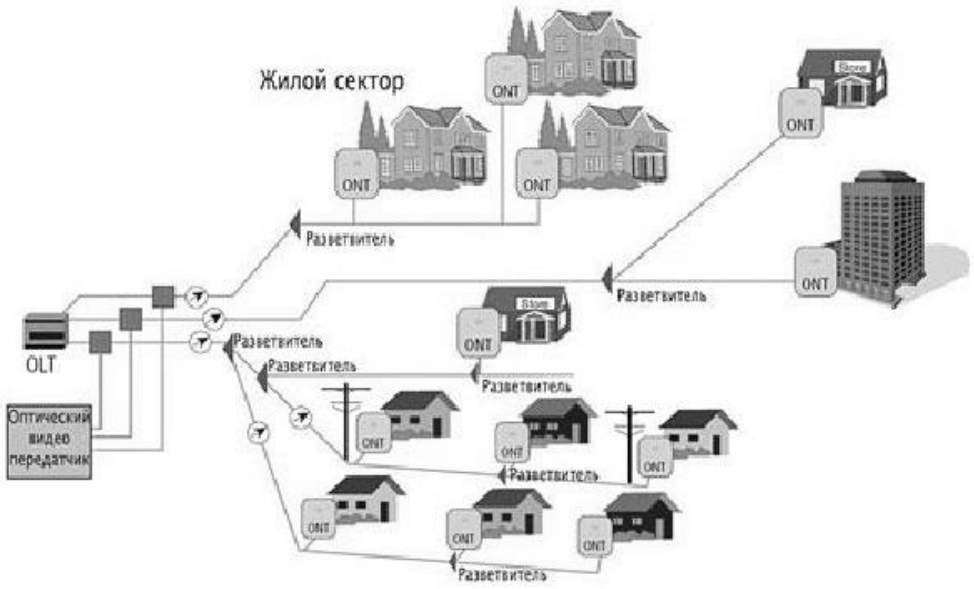


Рисунок 1

Основні технології GPON

- Принципи GPON - мультиплексування даних. GPON використовує Wavelength Division Multiplexing (WDM) технологію, для забезпечення 2-х спрямованої роботи в 1 оптичному кабелі.
- GPON Downlink. Кадр фіксованої довжини 125 мкс. Розподіл трафіку на основі GEM-PORT з функцією контролю (обмеження смуги).
- GPON Uplink. Послідовність і час доставки пакетів від кожного ONU контролюється OLT.
- Різні конфігурації GPON.
- Ослаблення потужності в технології GPON. Наприклад, обладнання Huawei GPON підтримує тип Class B+ з чутливістю -28dB, що дає впевнений прийом на відстані 20 км.

Переваг для провайдерів від використання GPON надзвичайно багато:

1. Не потрібний аналоговий телефон і кабельне телебачення з дорогими мідними кабелями.
2. Не потрібно тримати обладнання в будівлях і оплачувати оренду місця.
3. За електроенергію буде платити користувач, а не провайдер як це було раніше.
4. Абонент не зможе замінити кінцеве обладнання на своє, також є можливість прослідкувати та фільтрувати трафік для кожного абонента окремо, це дає змогу розгрузити власне обладнання з чорними списками и збільшити швидкість передачі даних.

У більшості випадків ця технологія зустрічається в країнах Азії. Найпопулярнішою компанію, яка випускає маршрутизатори з технологією GPON є Dasan.

В кінці квітня 2018 року анонімні дослідники оприлюднили матеріал, в якому розповіли про виявлення двох «дір» в системі безпеці роутерів Dasan, які мали технологію GPON. Виявлена вразливість стосувалась більше мільйона пристроїв в південно-корейській компанії.

Перша вразливість (CVE-2018-10561) дає можливість обійти механізм аутентифікації. Для виконання будь-яких операцій в web-інтерфейсі достатньо просто

добавити рядок «?images/» до URL-сторінки (наприклад, «/diag.html?images/» або «/GponForm/diag_FORM?images/»). Якщо виконати команди такого типу, то пристрій перезавантажиться. Вразливість присутня в типовому HTTP-сервері, який приміняють в різноманітних моделях домашніх GPON-маршрутизаторів.[2]

Друга вразливість (CVE-2018-10562) дозволяє, окрім загальних команд в web-інтерфейсі виконувати будь-які команди в контексті операційної системи пристрою. Вразливість викликана відсутністю необхідних перевірок, під час виконання операцій ping і traceroute в формі /diag.html. Ці операції виконуються через запуск однакових команд з передачею вказаних користувачем характеристик. Так як вхідні дані не перевіряються необхідним чином, з'являється можливість через передачу рядка типу «id; 192.168.1.1» в полі IP-адреси запустити будь-яку команду на пристрої. Цікаво, що про цю вразливість згадувалось в коментарях рік тому. В мережі можна знайти публічні експлойти для проведення CSRF-атак, датовані 2015 року.[2]

04.05.2018 співробітники компанії Netlab 360 повідомили про серію атак, які були здійсненні на маршрутизатори цього типу, використовуючи вищезазначені вразливості. Найбільше постраждали користувачі Казахстану, В'єтнаму та Мексики. За початковими даними для атаки доступні більше мільйона проблемних пристроїв, які приймають з'єднання до web-інтерфейсу через реальний IP.[2]

Хакери запустили ботнет, який сканує і намагається використовувати вразливі пристрої. Ботнет керується з сервера, який розташований у В'єтнамі. За перші 5 днів до групи ботнетів які використовують вразливості GPON долучилося безліч сервісів.

Компанія VPN Mentor випустила патч, який може запобігти та унеможливити атаки на маршрутизатори. Проте слід зазначити, що проблеми не специфічні для конкретного виробника пристроїв і проявляються на широкому спектрів домашніх маршрутизаторів для пасивних оптичних мереж GPON. Багато пристроїв, які були встановленні провайдерами використовуючи GPON-систему випускалися по OEM-контрактам під власними брендами і вже не підтримуються.[1]

Насправді ситуація яка склалася є надзвичайно небезпечною, адже хакери можуть використати отриманий нелегальний доступ до маршрутизаторів, наприклад, для здійснення DDos-атак. За попередніми підрахунками 1 млн. гігабітних пристроїв дає до 1 петибіта роздільної здатності і якщо хакери це використають, то це нанесе фатальну шкоду для всієї мережі. Звичайно, випущена прошивка для певних пристроїв зменшить кількість використаних пристроїв, також слід зазначити, що не всі пристрої, які використовують технологію GPON піддалися атакам, з тих чи інших причин.

Ця історія з маршрутизаторами можна стати хорошим прикладом для інших компаній та систем, про те що безпека повинна завжди залишатися на найвищому рівні і в майбутньому наслідки будуть все масштабнішими і масштабнішими. Постійна перевірки системи в цілому і окремих компонентів, ось дієвий спосіб протидії майбутнім атакам та загрозам. Багато фахівців провідних компаній, а також анонімних користувачів тестують, як обладнання, так і програмне забезпечення, їх взаємодія з розробниками дієвий спосіб залишати систему в безпечному стані.

Література

1) http://isearch.kiev.ua/uk/searchpractice/science/1412--as-internet-technology-gpon;
2) https://opennet.ru/opennews/art.shtml?num=48550;
3) https://lenta.ru/news/2018/05/04/dasan/.

Кукшин Дарія Вікторівна
Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації
м. Київ

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ

Соціальні мережі давно вже стали невід'ємною частиною нашого життя. Вони допомагають нам спілкуватися один з одним і обмінюватися повідомленнями, фотографіями, аудіо- та відео-файлами. У кожного є сторінка в соціальній мережі, де можна розмістити різну інформацію про себе, а, також, дізнатися більше про своїх друзів, знайомих та різних людей, з якими потім можна познайомитись

В соціальних мережах користувачі розміщують різні персональні дані про себе, наприклад: ПІБ, дата народження, та навіть інформацію про улюбленого співака або, яку музику ви слухаєте. Такий великий обсяг різних даних потрібно оберігати, бо вона у вільному доступі і кожен може прочитати, а потім і використовувати цю інформацію. У зв'язку з тим, що є ризик взлому аккаунтів в соціальних мережах, а потім зловмисники можуть використовувати ваші персональні дані. І від цього не застрахована жодна мережа, томи ми, користувачі, повинні самі захищати свої персональні дані, коли ми користуємося соціальними мережами.

Одним з найактуальніших завдань безпеки в цьому контексті є забезпечення конфіденційності, тобто, надання своїх персональних даних тільки заздалегідь визначеному колу осіб у рамках соціальної мережі (наприклад, тільки друзям). Це право дається тільки користувачу, і він сам вирішує, яку інформацію він робить загальнодоступною, а до якої обмежити доступ.

Також комп'ютерні шахраї зламують аккаунти для використання у власних цілях. Вони діють дуже обережно, щоб користувач не відразу запідозрив, що щось не так. В більшості випадків такі «зламані» сторінки використовують для вступу у різні групи, додавання коментарів або лайків. Це дуже зручно і так проводиться монетизація чужого аккаунту, бо більшість користувачів не перевіряє, в які спільноти вони вступили, та і перевіркою коментарів і лайків у соціальних мережах взагалі ніхто не займається.

Зараз послуга вступу до різних груп та додавання лайків та коментарів масово пропонується реальним користувачам. Але так ви нічого не зможете продати, бо хакери запрошують в такі спільноти замовників нецільову аудиторію, а розсилка спаму від невідомих спільнот розлючує людей, що не є плюсом для іміджу компанії.

Існує два найпоширеніших методів монетизації аккаунтів:

1. Розсилка спаму на стінку аккаунта, в особисті повідомлення друзям, тощо. Спам розсилається у вигляді промоакцій та рекламних повідомлень.
2. Розсилка особистих повідомлень з проханням проголосувати або просто допомогти. В них повідомляється, що така допомога буде коштувати недорого, а на практиці виходить по-іншому.

Отже, щоб ваш аккаунт не виявився в руках зловмисників, потрібно дотримуватися декількох базових рекомендацій, так званої мереженої гігієни.

Так, до загальних механізмів безпеки, які не прив'язані до соціальних мереж, відноситься, наприклад, використання захищеного протоколу взаємодії з Web-серверами. Тобто, при вході і перебуванні в соціальній мережі повинен використовуватися лише протокол https. Це гарантує безпечну передачу інформації у мережі (але при цьому знижується швидкість передачі даних), у тому числі зв'язки логін – пароль.

Необхідно стежити і регулярно очищати дані про профіль користувача соціальної мережі, що залишається браузером у вигляді файлів або відповідних записів на комп'ютері. У деяких випадках такі дані можуть використовуватися шкідливим програмним забезпеченням для несанкціонованого отримання персональних відомостей (наприклад, тієї ж зв'язки логін – пароль).

Персональні дані на сторінці в соціальних мережах потрібно розміщувати з розумом. Не потрібно виставляти інтимну інформацію, відверті фото, дані про вашу сім'ю. Це все для того, щоб не потрапити в зону ризику і не привертати увагу шахраїв.

Варто періодично змінювати паролі, використовуючи якомога більше символів, щоб ускладнити автоматичний підбір. Слід вигадати складний пароль мінімум з 8 символів, з урахуванням регістру (користуватись великими і малими літерами), також слід увімкнути двофазну авторизацію через телефон (до аккаунту в особистих налаштуваннях додається телефон, і при вводі логіну та паролю сайт відправляє код через SMS, який додатково потрібно ввести).

Не залишайте номер свого мобільного на жодному з сайтів, коли розміщуєте інформацію про себе. Його легко відслідкувати, просто використавши пошук по фото. Використовуйте це правило, якщо не хочете, щоб номер вашого телефону дізналися шахраї. Вам можуть приходити SMS-повідомлення різного змісту, або навіть вони можуть телефонувати Вам і вимагати грошей. Таким методом користуються телефонні шахраї, які обманом вимагають гроші від простих людей, які мали необережність залишити свій номер телефону в спільному доступі.

Не використовуйте в соціальних мережах геолокацію. Так зловмисники можуть дізнатися точну вашу адресу проживання, і це допоможе квартирним злодіям обстежити та оцінити ваше помешкання. Таким чином людина, сама того не розуміючи, повідомляє шахраям всю інформацію про те, де і як вона живе. Так злодії обирають собі наступну жертву. Отже, так через соціальні мережі можна привабити до себе навіть і квартирних злодіїв.

Остерігайтесь переходити за посиланнями, які вам надсилають на пошту і в соціальні мережі. Кожне з них може бути використане для зламу вашої сторінки. Також такі посилання можуть призвести до взлому вашого персонального комп'ютера, або хакери так можуть переносити різні віруси.

Зрештою, до одного із дієвих механізмів безпеки необхідно віднести установку на ваш персональний комп'ютер антивірусів і інших засобів захисту. Але не варто також забувати про мобільні пристрої, з яких останнім часом багато користувачів заходять в соцмережі. Ці пристрої локально зберігають персональні дані, отримані із соцмереж, та схильні до дії шкідливого програмного забезпечення.

На жаль, мережева гігієна, як і будь-яка інша, не зможе повністю захистити ваш аккаунт від вірусного захворювання. Навіть якщо враховувати, що соціальні мережі захищені безпечними протоколами, на сьогодні не існує стовідсоткових способів захисту облікового запису. Це, у першу чергу, пов'язано з тим, що соціальна мережа – це непідконтрольне нам середовище, і захистити її можуть тільки її співробітники за допомогою додаткових внутрішніх систем безпеки.

До того, як ваш аккаунт буде взломаний, майже неможливо виявити його слабкості, але вже після цього можна змінити логін і пароль, що зменшить доступ зловмисників до ваших персональних даних. В соціальній мережі набагато легше вирішувати проблеми по факту їх появи, ніж намагатися передбачити можливі варіанти атаки, бо ми не можемо покращити міри обережності стороннього середовища.

Як зрозуміти, що аккаунт було взломано? Перерахуємо основні ознаки взломаного аккаунта, щоб користувачі могли своєчасно змінити свої контактні дані. Також рекомендуємо змінити пароль не лише від аккаунта в соцмережі, а й від скриньки електронної пошти.

Основні ознаки взломаного аккаунта в соцмережі:

- Друзі пишуть Вам, що Ви були online, коли Ви впевненні, що в зазначений час Ви не заходили до Інтернету;
- З Вашого аккаунту почалась розсилка дивних листів та посилань;

- Ви виявляєте у себе в аккаунті спільноти, в які не вступали і друзів, яких не додавали;
- Ви заходите до себе в аккаунт, але ваш пароль не підходить.

Таким чином, існують лише базові поради щодо запобіжних заходів, дотримуючись яких ви зможете, якщо не повністю убезпечити, то хоча б максимально ускладнити несанкціонований доступ до ваших персональних даних.

Зараз почали використовувати соціальні мережі для різних видів інтернет-шахрайства. Тому, щоб протистояти такій небезпеці, потрібно знати, з чим маємо справу.

І перший вид такого інтернет шахрайства - фішинг. Це вид інтернет-шахрайства, мета якого полягає в отриманні доступу до персональних даних користувача – паролів, логінів тощо. В процесі цього виду хакер використовує фішинговий лист, який він надсилає в особисті повідомлення користувачу, де є прохання проголосувати за щось або просто прохання перевести гроші на допомогу. Наївний користувач переходить по посиланню в такому листі та вводить персональні дані, які потім використовує зловмисник. Але це не один сценарій. В іншому - користувач заходить на даний фішинговий сайт і відразу виходить. При таких діях починає працювати спеціальний скрипт, який визначає версію вашої операційної системи та використовуваного браузера. Виходячи з одержаних даних, встановлюється екстплойт за допомогою якого отримується правка файлу HOSTS, встановлюється і активізується троян, який може зчитати всі дані користувачів з ПК.

Як захиститися від фішингу в соціальних мережах? По-перше, листи, які прийшли від невідомих користувачів, не потрібно навіть читати, а відразу відправляти в «спам» і повідомляти про це адміністрації сайту. Але не потрібно всі листи відправляти туди, якщо користувач брав участь в конкурсах, і організатори можуть надіслати вам повідомлення, але переходити по посиланням дуже обережно. Потрібно пам'ятати, що адміністрація не буде просити у користувача пароль, бо він у неї і так є. Також адміністрація не буде просити вислати SMS-повідомлення на якийсь номер.

Ще один тип загроз, що перейшов до соцмереж, - програми для крадіжки паролів. Вони впроваджують частини коду в ваш комп'ютер, щоб викрасти ваші дані для регістрації до того, як вони будуть відправлені на сервер. Після цього зловмисник починає використовувати ваші дані, то він почне також відправляти посилання знайомим та друзям жертви, то кількість постраждалих буде рости, як снігова куля.

Існує ще один вид загроз – фармінг, який більш небезпечний, ніж фішинг. Спочатку з'явився фішинг, а потім, в результаті еволюції, фармінг. Що ж представляє із себе цей вид інтернет – шахрайства? Фармінг – це замасковане перенаправлення користувача–жертви на фальшивий IP-адрес.

В чому ж криється відмінність фішинга від фармінга? В обох випадках становищу жертви не позаздриш. Користувача перенаправляють з красивого справжнього сайту на красивий фальшивий сайт. Але якщо у випадку з фішингом назва сайту змінюється, то у випадку з фармінгом назва сайту залишається та сама, змюється тільки IP-адреса, тобто, якщо сайт знаходиться в Україні, то його двійник буде знаходитись, наприклад, в Японії. Навіть найуважніший користувач не в змозі відрізнити, коли потрапляє на фармінг-сайт, а коли – на справжній, якщо у нього, звичайно, немає змоги перевіряти IP-адреси сайтів. Якщо адреси двох сайтів ідентичні, то можна починати бити на сполох.

Отже, захист персональних даних в соціальних мережах – справа рук самого користувача. Тому краще сто разів подумати, перед тим, як викласти якусь інформацію про себе або фотографію. Ніхто не може гарантувати того, що саме Ваші дані не будуть використовуватися зловмисниками в особистих цілях.

Література:

- *Захист персональних даних в соціальних мережах [Електронний ресурс] – Режим доступу: http://www.vaas.gov.ua/news/zaxist-personalnix-danix-v-socialnix-merezhax/*
- *Як захистити персональні дані в мережі – поради спеціалістів [Електронний ресурс] – Режим доступу : http://universe.zp.ua/?p=4505*
- *Способы защиты персональных данных в социальных сетях [Електронний ресурс] – Режим доступу : http://www.praima.ru/node/351*
- *Виды защиты информации в социальных сетях [Електронний ресурс] – Режим доступу : https://sites.google.com/site/socialnyeseti94/zasita-informacii-v-socialnyh-setah/vidy-zasity-informacii-v-socialnyh-setah*

Пилипенко Р.А.

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

ТЕНДЕНЦІЇ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Розглянуто ключові переваги IT-індустрії як двигун глобального економічного зростання. Перераховано переваги від запровадження IT-сектора у економіках та вказані конкретні прибутки держав світу.

IT-індустрія є двигуном глобального економічного зростання і надає ряд ключових переваг:

- Сьогодні IT-індустрія безпосередньо забезпечує роботою 9 млн. високооплачуваних кваліфікованих співробітників у більш ніж 4 тис. компаній в усьому світі. Крім того, цей сектор економіки створює зайнятість ще для 21 млн. IT-фахівців у різних сферах діяльності - від консалтингу до вантажних автоперевезень. Число робочих місць в IT-індустрії в цілому за період з 2014 по 2016 рік зросла на 40%, а в галузі програмного забезпечення - на 76%.
- IT-індустрія приносить до бюджетів своїх країн понад 700 млрд. дол податкових надходжень на рік. Ці податкові доходи від діяльності, пов'язаної з інформаційними технологіями, зросли за 2014-2016 роки на 37% і допомагають фінансувати життєво важливі державні служби і надавати державні пільги, в тому числі забезпечують громадську безпеку, роботу шкіл і транспортної системи. Таким чином, можна зробити висновок, що зростання IT-індустрії вигідний для держави і суспільства в цілому.
- Вклад IT-індустрії у світову економіку складає майже 1 трлн. дол на рік, у тому числі 330 млрд. дол надходять від галузі виробництва комп'ютерного обладнання, 250 млрд. дол - від галузі «тиражного» програмного забезпечення і ще 420 млрд. дол - від галузі IT-послуг.

Завдяки більш високим темпам зростання порівняно з традиційними галузями економіки IT-індустрія може забезпечити більш значні переваги: ‹створення нових робочих місць, збільшення податкових надходжень і розвиток економіки. Чим швидше це зростання, тим більші економічні переваги він приносить. У даній роботі ми постараємося охарактеризувати тенденції подальшого розвитку інформаційних технологій, іншими словами, ми спробуємо вирішити складне завдання - зазирнути у світ майбутнього вже сьогодні.

Література:

1. *Гриценко В.І., Паньшін Б.М. Інформаційна технологія: Питання розвитку та застосування. Київ: Наукова думка, 2002*

Мальгина Екатерина Вячеславовна

Государственный университет телекоммуникаций

Учебно-научный институт защиты информации

г. Киев

КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ ФИШИНГА?

Суть фишинга (вишинга, вэйлинга и пр.) состоит в так называемой социальной инженерии и при этом целью фишинг-атаки является не компьютер, а человек, работающий на нём. Даже в случае если действия осуществляются по взлому программ, данные, необходимые злоумышленнику, извлекаются не из «мозгов» компьютера, а из мозга человека.

В чём цель социального инженера?

Цель «социального инженера» заключается в том, чтобы вынудить пользователя компьютера (планшета, смартфона и даже банкомата) по собственной воле произвести некое действие или поделится той информацией, которую нужно хранить в тайне. В этом плане их деятельность схожа с работой различных наперсточников, гадалок и других «воров на доверии» из оффлайн жизни.

Квинтэссенция питательной среды, на которой расцветает данный вид афер, отражена в названии книжки одного из столпов Web-дизайна, С.Круга: «Не заставляйте меня думать!». Всевозможные технологические хитрости, предназначенные для того, чтобы упростить жизнь обычному пользователю и «сделать ему красиво», вместе с объективными недочетами разработчиков программного обеспечения и дизайнеров оставляют большое количество лазеек для злоумышленников, что позволяет им достичь своей цели и постоянно улучшаться в способах ее достижения. При этом наблюдается постоянный рост трудности таких атак и тенденция к переходу от «стрельбы по площадям» к целевым атакам за счет применения данных, полученных из соц. сетей.

Как защитится от фишинг атак?

Для того чтобы уменьшить вероятность попадания на фишинг удочку, следует помнить старенькую поговорку: на заборе много чего пишут, а за ним дрова лежат. Любое предложение о предоставлении важной информации следует внимательно и тщательно проверять, не забывая о том, что бесплатный сыр бывает лишь в мышеловке.

1. В первую очередь нужно постоянно быть уверенным в том, с кем вы общаетесь в сети. По возможности проверять полученную информацию по другому каналу связи. Понимать, что в нашей реальной онлайн жизни практически никогда нет никакой реальной срочности в том, чтобы сделать что-то прямо сейчас и здесь, как вас стараются заставить.
2. Будьте внимательны при получении сообщений электронной почты от незнакомых отправителей и сообщений требующих, а иногда просящих перейти по внешней гиперссылке.
3. Заведите себе привычку постоянно проверять через адресную строку в вашем браузере на том ли веб-сайте вы вводите свой пароль (обычно подделывается и доменное имя. т.е. оно очень похоже на свой оригинал, отличие может быть только в одной букве, к примеру microsoft.com может превратиться в maicrosoft.com)
4. Используйте последние версии браузеров и лицензионного антивирусного ПО
5. По возможности используйте безопасные браузеры, скаченные с официальных сайтов разработчиков
6. Следите за тем, что бы при входе на веб-сайты банков было установлено особое защищенное интернет соединение https
7. В случае если у вас есть сомнение, и вы думаете что вы подверглись фишинг атаке, обязательно и незамедлительно поменяйте пароль вашего аккаунта и

обратитесь в службу безопасности банка или другой организации данные от которой получили фишинг мошенники.

Но самое главное что нужно держать в голове и помнить всегда: ваш ПАРОЛЬ – ТОЛЬКО ВАШ, ни одна фирма, организация или интернет сайт не будут спрашивать у вас вашего пароля. Пароль необходим вам исключительно для получения доступа к определенному сервису и знать его должны лишь вы.

Хоть интернет и виртуален, но он на столько сильно проник в нашу с вами жизнь, что вред от фишинг атаки может быть вполне материальным, будьте осторожнее!

Щебланин Александр Юрьевич
Государственный университет телекоммуникаций
Учебно-научный институт защиты информации
г.Киев

ОСНОВНЫЕ МЕТОДЫ ШИФРОВАНИЯ. БАЗИСЫ КРИПТОГРАФИИ

Криптография как наука появилась много сотен лет назад, на протяжении длительного периода времени методы шифрования информации становились все лучше и лучше. Именно благодаря ученым развивающим криптографию информация находится в безопасном состоянии. Для начала, что же такое криптография, это наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, а также невозможности отказа от авторства [1].

Одним из древних и ключевых методов шифрования был «шифр Цезаря». Суть шифра - каждый символ текста заменяется на некоторый другой, причём одинаковые символы заменяются одинаково. Если данный символ - k-тый в N-символьном алфавите, то он заменяется (k + C) mod N - ым символом алфавита. Нумерация символов начинается с нуля. Зашифруем слово ЯМА, предположим ключ равен 2, тогда Я сдвигается на две буквы алфавита вперед и получаем букву Б, проделав такие манипуляции с каждой буквой получаем шифр БОВ [2]. Шифр Цезаря вместе со всеми его вариантами перебрать очень легко, в ключе Цезаря всего 25 вариантов при 26 буквах в алфавите и его как раз можно перебрать полным перебором, что является легкой задачей для современных компьютеров.

Потом появился шифр «Вижнера», который основан на методе Цезаря. В данном случае ключ задается не в виде числа, а в виде слова. Есть слово ВЕДРО и ключ БАГБА, учитывая правила шифрования, Б это первая буква, получается В сдвигается на одну букву и получаем Д. После шифрования получаем сообщение ГЕЖСО. Ключ в данной ситуации будет подбираться сложнее, но все равно возможно [3].

Каждый современный шифр тем или иным способом базируется на двух принципах — подстановки и перестановки. Сейчас их использование намного более сложное, но сами базовые принципы остались прежними.

Очень важным является Шифрование публичным ключом. Алгоритм шифрования, применяющийся сегодня в различных модификациях буквально во всех компьютерных системах. Есть два ключа: открытый и секретный. Открытый ключ — это некое очень большое число, имеющее только два делителя, помимо единицы и самого себя. Эти два делителя являются секретным ключом, и при перемножении дают публичный ключ. Например, публичный ключ — это 1961, а секретный — 37 и 53. Открытый ключ используется для того, чтобы зашифровать сообщение, а секретный — чтобы расшифровать. Без секретного ключа расшифровать сообщение невозможно [4].

Мир криптографии постоянно развивается и никогда не стоит на месте, еще есть большое количество других интересных и по своему полезных методов шифрования информации.

Литература:
1.Криптография: Базовые знания о науке шифрования [Электронный ресурс] / -
2.Шифр Виженера [Электронный ресурс] / - режим доступа: http://crypto.hut2.ru/vigener.html
3.Введение в криптографию и шифрование [Электронный ресурс] / - режим доступа: https://habr.com/company/yandex/blog/324866/
4. 10 популярных кодов и шифров [Электронный ресурс] / - режим доступа: https://tproger.ru/translations/10-codes-and-ciphers/

Вакуленко Ольга Сергеевна
Государственный университет телекоммуникаций
Учебно-научный институт защиты информации
г. Киев

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ОТКРЫТОЙ WI-FI СЕТИ И ЕЕ ОТЛИЧИЯ ОТ КОРПОРАТИВНОЙ

В 2к18 нет человека, пользующегося интернетом и ни разу не подключившемся к открытой точке доступа выхода в интернет. Причин этому может быть множество, но они не столь важны, как последствия такого подключения. В данном тезисе будут рассмотрены основные уязвимости открытой Wi-Fi сети, а также способы нейтрализации этих уязвимостей со стороны пользователя сети; отличия корпоративной сети от открытой.

Открытая Wi-Fi сеть.

Обычный Wi-Fi, который раздается в кафе, торговых центрах, метро, аэропортах или же в любом другом заведении схожего рода, зачастую не оснащен никакими защитными функциями, что делает сеть более удобной в использовании. Сеть, подобного типа, не ограничивает действия пользователя, но также дает возможность злоумышленнику воспользоваться этой неограниченностью и получить доступ к ряду уязвимостей Wi-Fi сети.

Основные угрозы безопасности при работе с открытым Wi-Fi [1],[2]:

- Считывание (перехват и анализ) интернет-трафика: при наличии подходящего программного обеспечения, можно «внушить» адаптеру Wi-Fi, что он должен принимать все пакеты вне зависимости от указанных в сетевых пакетах IP-адресов. В этом случае злоумышленник может считывать весь трафик, подходящий через точку доступа, при этом оставаясь в тени, т.к. сам ничего не передает.
- Перехват cookie-файлов: с помощью соответствующего програмного обеспечения злоумышленник может организовать сетевую атаку с использованием протокола ARP и перехватить сеансовые cookie-файлы, которые идентифицируют авторизировавшегося на каком-либо сайте. Благодаря таким cookie-файлам вам не требуется вводить пароль каждый раз, когда вы хотите авторизироваться. Специальные программы извлекают из трафика все сеансовые cookie-файлы и выводят их на экран, после чего злоумышленник может войти на ваши текущие сеансы.
- Подмена точки доступа: Из любого устройства злоумышленник создает точку доступа Wi-Fi с любым именем, если в вашем списке сохраненных Wi-Fi сетей есть точка доступа с таким именем, то ваше устройство подключается к сети злоумышленника автоматически, а он в свою очередь считывает в своей поддельной сети все передаваемые по ней данные.

- Взлом механизма шифрования: вариантов множество, одним из довольно распространенных есть тот, где злоумышленник перенаправляет с защищенного сайта на его незащищенную версию, после чего имеет возможность узнать пароль или прослушать весь трафик.
- Прямая атака хакера: атака злоумышленником компьютер, подключенный к незащищенной точке доступа вредоносным программным обеспечением.

Способы защиты со стороны пользователя сети [2],[]:

- Использование технологии VPN для доступа к сети интернет;
- Использование только защищенных протоколов;
- Отказ от передачи конфиденциальных или персональных данных по протоколам, не защищенным стойкими алгоритмами шифрования;
- Отказ от использования интернет-банкинга через незащищенные сети;
- Использование полностью настроенного брандмауэра;
- Выключение адаптера Wi-Fi, когда не требуется подключения к сети;
- Удаление сохраненных сетей Wi-Fi из списка в настройках устройства, оставляя там только домашние и рабочие.
- При возможности переподключение к сети с включенным WPA/WPA2- шифрованием.

Корпоративная Wi-Fi сеть:

Wi-Fi сеть, используемая определенным предприятием; радует глаз наличием администратора безопасности.

Способы защиты со стороны администратора сети [3]:

- Контроль доступа;
- Аутентификация пользователей;
- Аутентификация устройств;
- Шифрование трафика;
- Система предотвращения вторжений в беспроводную сеть;
- Система обнаружения чужих устройств и возможности их активного подавления;
- Мониторинг радиоинтерференции и DoS-атак;
- Мониторинг уязвимостей в беспроводной сети и возможности аудита уязвимостей;

Вывод:

Просматривать местность на наличие подозрительных личностей или не иметь конфиденциальной информации вам решать, я выбираю использование 3G и домашнего Wi-Fi.

Литература:

1. *Райтман М.А. Искусство легального, анонимного и безопасного доступа к ресурсам интернета.*
2. *https://habrahabr.ru/company/eset/blog/66086/*
3. *.https://habrahabr.ru/company/pentestit/blog/265697/*

Щебланин Александр Юрьевич
Государственный университет телекоммуникаций
Учебно-научный институт защиты информации
г.Киев

РЕШЕНИЕ ПРОБЛЕМЫ УТЕЧКИ ИНФОРМАЦИИ С ПОМОЩЬЮ DLP СИСТЕМ

Вопрос защиты информации в корпоративных сетях очень актуален в наши дни. Критическая информация о компании может стоить большую сумму денег, и ее утечка может нести серьезные деструктивные действия со стороны оппонентов или же определенных формирований. Примером утечки информации в корпоративных сетях является случай в 2017 году, когда группа хакеров под названием Tsar Team опубликовала в Сети более 25 тысяч фотографий и личную информацию пациентов литовской клиники пластической хирургии. В каждой сети может сформироваться утечка данных, из-за случайных действий сотрудников, или же из-за целенаправленных действий инсайдеров и хакеров использующих уязвимости информационной сети. Хорошим решением данной проблемы является DLP система.

DLP (Data Loss Prevention) система - это программный продукт, созданный для предотвращения утечек конфиденциальной информации за пределы корпоративной сети. Строится эта система на анализе потоков данных, выходящих за пределы корпоративной сети. В случае активации определенной сигнатуры и определения передачи конфиденциальной информации система либо блокирует такую передачу, либо посылает уведомление должностному лицу службы защиты информации компании [1].

DLP-системы позволяют контролировать все каналы сетевой коммуникации компании. Защита от утечки информации достигается за счет того, что на все компьютеры сотрудников ставятся программы-клиенты, которые собирают информацию и передают ее на сервер. Порой информация собирается через шлюз, с использованием SPAN-технологий. Информация анализируется, после чего системой или должностным лицом принимаются решения по инциденту.

Предотвращение утечки данных реализуется за счет внедрения механизмов: контроля протоколов, социальных сетей и блогов, портов, анализа рисунков, архивов, транслита, логирования действий администраторов системы, записи отчетов в локальные хранилища, оповещений, просмотра истории инцидентов и многого другого.

Данная система нуждается в постоянном администрировании и анализе инцидентов, по этому требуется квалифицированный персонал для поддержки. Пункты которые нужно соблюдать для успешной работы системы:

1. Корректно настроить правила безопасности;
2. Актуализировать правила безопасности с определенной периодичностью;
3. Продумать алгоритм реагирования на инциденты;
4. Проверить работу режима блокировки;
5. Проверить, введен ли режим коммерческой тайны [2].

Примеры данной системы от различных производителей: Security ZGate, Info Watch Traffic Monitor, Symantec Data Loss Prevention, Search Inform Контур безопасности, Falcon Gaze Secure Tower. Цены на данный продукт варьируются от 500 грн до 5000 грн, так же есть бесплатные версии. Для крупных компаний программа стоит дороже.

Литература:

1. Выбираем DLP-систему для средней организации [Электронный ресурс] / - режим доступа: https://habrahabr.ru/post/141000/

2. Нечеухин О. Как заставить DLP-систему работать [Электронный ресурс] / - режим доступа: https://kontur.ru/articles/1798]

Макарченко Александр Сергеевич
Государственный университет телекоммуникаций
Учебно-научный институт защиты информации
г.Киев

СПОСОБЫ ЗАЩИТЫ ОТ DDOS-АТАКИ

DDoS (Distributed Denial of Service - "распределенный отказ в обслуживании") атаки относятся к так называемым виртуальным методам терроризма. Их цель – вывести из строя сервер, подключенный к сети Интернет, путем посылки на него огромного количества запросов. В результате либо сервер, либо канал связи, им используемый, становится перегруженным. Это приводит к неработоспособности находящихся на атакуемом сервере ресурсов. При этом реальные пользователи «упавшего» сайта не могут получить к нему доступ — всё это влечет за собой финансовые убытки.

Суровая правда такова, что многие сайты может положить любой желающий, воспользовавшись атакой Slowloris, наглухо убивающей Apache, или устроив так называемый SYN-флуд с помощью фермы виртуальных серверов, поднятых за минуту в облаке Amazon EC2. Все наши дальнейшие советы по защите от DDoS своими силами основываются на следующих важных условиях.

Так какие же есть способы защиты от DDoS-атаки?

1. Мощные сервера

Чтобы свести DDoS-атаки сайта на нет и защитить его, необходимо иметь мощные серверы, широкие каналы связи. В этом случае атака просто пройдет незамеченной, так как сервер попросту обработает все входящие запросы. Средства блокировки слишком частых запросов с одного адреса также являются эффективным методом защита от DDoS-атак сайта.

2. Отказаться от Windows Server

Практика подсказывает, что сайт, который работает на винде, в случае DDoS обречен. Причина неудачи кроется в виндовом сетевом стеке: когда соединений становится очень много, то сервер непременно начинает плохо отвечать. Не понятно, почему Windows Server в таких ситуациях работает настолько отвратно, но случалось такое не раз и не два. По этому все ниже наведённые способы защиты от DDoS-атак в случае, когда сервер крутится на Linux.

3. Расстаться с Apache

Второе важное условие — отказ от Apache. Если у вас стоит Apache, то как минимум поставьте перед ним кеширующий прокси — nginx или lighttpd. Apache’у крайне тяжело отдавать файлы, и, что еще хуже, он на фундаментальном уровне уязвим для опаснейшей атаки Slowloris, позволяющей завалить сервер чуть ли не с мобильного телефона. Но если вы не хотите заниматься лишней работой, то проще взять HTTP-сервер, неуязвимый для Slowloris на уровне архитектуры кода. Поэтому все дальнейшие способы основываются на предположении, что на фронтенде используется nginx.

Что делать, если пришел DDoS? Традиционная техника самообороны — почитать лог-файл HTTP-сервера, написать паттерн для grep (отлавливающий запросы ботов) и забанить всех, кто под него подпадет. Эта методика на удачу. Ботнеты бывают двух типов, оба опасны, но по-разному. Один целиком приходит на сайт моментально, другой — постепенно. Первый убивает все и сразу, зато в логах появляется весь полностью, и если вы их progrepаете и забаните все IP-адреса, то вы — победитель. Второй ботнет укладывает сайт нежно и осторожно, но банить вам его придется, возможно, на протяжении суток. Любому администратору важно понимать: если планируется бороться grep’ом, то надо быть готовым посвятить борьбе с атакой пару дней.

4. Анализируйте ошибки

Проанализируйте объем трафика, время ответа сервера, количество ошибок. Для этого смотрите логи. В nginx время ответа сервера фиксируется в логе двумя переменными: request_time и upstream_response_time. Первая — это полное время выполнения запроса, включая задержки в сети между пользователем и сервером; вторая сообщает, сколько бэкенд (Apache, php_fpm, uwsgi…) выполнял запрос. Значение upstream_response_time

чрезвычайно важно для сайтов с большим количеством динамического контента и активным общением фронтенда с базой данных, им нельзя пренебрегать.

5. Отслеживайте количество запросов в секунду

Также посмотрите на число запросов в секунду. По сравнению с нормальным для этого времени дня уровнем количество запросов в секунду может как падать, так и расти. Растут они в случае, если пришел крупный ботнет, а падают, если пришедший ботнет обрушил сайт, сделав его полностью недоступным для легитимных пользователей, и при этом ботнет статику не запрашивает, а легитимные пользователи запрашивают. Падение количества запросов наблюдается как раз за счет статики. Но, так или иначе, мы ведем речь о серьезных изменениях показателей. Когда это происходит внезапно — пока вы пытаетесь решить проблему своими силами и если не видите ее сразу в логе, лучше быстро проверьте движок.

6. Лимитируем ресурсы (размеры буферов)

Про что нужно помнить в первую очередь? Каждый ресурс имеет лимит. Прежде всего это касается оперативной памяти. Поэтому размеры заголовков и всех используемых буферов нужно ограничить адекватными значениями на клиента и на сервер целиком.

7. Настраиваем тайм-ауты

Ресурсом является и время. Поэтому следующим важным шагом должна стать установка всех тайм-аутов. Сразу вопрос: какие параметры буферов и тайм-аутов правильные? Универсального рецепта тут нет, в каждой ситуации они свои. Но есть проверенный подход. Нужно выставить минимальные значения, при которых сайт остается в работоспособном состоянии (в мирное время), то есть страницы отдаются и запросы обрабатываются. Это определяется только тестированием — как с десктопов, так и с мобильных устройств.

Литература:

1. *https://xakep.ru/2012/12/29/16-antiddos-recipes/#toc03.*
2. *http://timeweb.com/ru/community/articles/sposoby-zashchity-ot-ddos-ataki-1*

Сокол Антон Васильович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ВПЛИВ BLOCKCHAIN НА ІНФОРМАЦІЙНУ БЕЗПЕКУ

З моменту своєї появи в 2009 році, концепція блокчейн розширила своє початкове використання в якості біткоіни на багато інших напрямків. За своєю природою ця розподілена база даних надає прекрасну платформу для управління криптовалюта. Але її особливості привернули увагу фахівців, що займаються широким спектром інших додатків. Можливо, найбільший інтерес був пов'язаний з безпекою. Блокчейн пропонує більш безпечні транзакції, захист від певних хакерських атак і навіть, певною мірою, позбавляє від необхідності паролів.

Що таке блокчейн?

Блокчейн (blockchain) - це розподілена база даних, що складається з строкових блоків і розроблена таким чином, щоб уникнути подальших модифікацій. Після того як дані були опубліковані в ній, використовуючи надійну техніку проставляння часу і складної посилання на попередній блок, вважається, що вже неможливо відкотити назад і внести якісь зміни в запис. Блокчейн став безцінним інструментом, що ідеально підходять для забезпечення безпеки, але він також використовується для таких завдань, як зберігання і підтвердження даних - метод, який в даний час використовується для інтелектуального

аналізу даних (дата-Майнінг). Блокчейн - це результат багаторічних досягнень в криптографії та інформаційної безпеки.

Ми розглянемо три варіанти систем:

централізований з довіреним центром

централізований з недовіреним центром

децентралізований варіант з використанням доказу роботи

Централізований blockchain з довіреним центром

Якщо у нас є довірений центр, то ми просто доручаємо йому через певний проміжок часу (або ж через певний набір транзакцій) формувати новий блок, забезпечуючи його не тільки хеш-сумою, а й своїм електронним підписом. Кожен клієнт системи має можливість перевірити, що всі блоки в ланцюжку згенеровані довіреним центром і ніким іншим. У припущенні, що довірений центр не скомпрометований, можливості модифікації журналу зловмисником немає.

Використання технології blockchain в цьому випадку є надмірною. Якщо у нас є довірений центр, можна просто звертатися до нього з метою підписати кожну транзакцію, додавши до неї час і порядковий номер. Номер забезпечує порядок і неможливість додавання (видалення) транзакцій з ланцюжка, електронний підпис довіреної центру - неможливість модифікації конкретних транзакцій.

Централізований blockchain з недовіреним центром

Цікавий випадок, коли виділений центр не є довіреним. Точніше, не є повністю довіреним. Ми йому довіряємо в плані фіксації транзакцій в журналі, але хочемо бути впевненими, що виділений центр не перегенерірует весь ланцюжок блоків, видаливши з неї непотрібні йому більш транзакції або додавши потрібні.

Для цього можна використовувати, наприклад, такі два методи.

Перший метод з використанням додаткового довіреної сховища. Після створення чергового блоку центр повинен відправити в довірена і незалежне від даного центру сховище хеш-код від нового блоку. Довірена сховище не повинно приймати ніяких змін до хеш-кодами вже створених блоків. В якості такого сховища можна використовувати і децентралізовану базу даних системи, якщо така є. Розмір що зберігається може бути невеликим порівняно із загальним обсягом журналу.

Другий можливий метод полягає в доповненні кожного блоку міткою часу, згенерованої довіреним центром тимчасових міток. Така мітка повинна містити час генерації мітки і електронний підпис центру, обчислену на підставі хеш-коду блоку і часу мітки. У разі, якщо «недовірений» центр захоче перегенеріровать частина ланцюжка блоків, буде спостерігатися розрив в мітках часу.

Варто зазначити, що цей метод не гарантує, що «недовірений» центр не буде генерувати відразу два ланцюжки блоків, доповнюючи їх коректними мітками часу, а потім не підмінить одну інший.

Децентралізований blockchain

Найбільший інтерес для нас (і - найменший для компаній, що продають blockchain-рішення) являє децентралізована система blockchain без виділених центрів генерації блоків. Кожен учасник може взяти набір транзакцій, які очікують включення в журнал, і сформувати новий блок. Більш того, в системах типу BitCoin такий учасник (будемо його

назвати «Майнер», від англ. To mine - копати) ще й отримає премію у вигляді певної суми та / або комісійних від прийнятих в блок транзакцій.

Але не можна просто так взяти і сформувати блок в децентралізованих системах. Надійність таких систем ґрунтується саме на тому, що новий блок не можна сформувати швидше (в середньому) ніж за певний час. Наприклад, за 10 хвилин (BitCoin). Це забезпечується механізмом, який отримав назву доказ роботи.

Блокчейн в сервісі безпеки

Деякі експерти почали аналізувати потенціал блокчейна щодо сервісів, пропонованих DNS-серверами. В силу непорушності і децентралізації блокчейна, якби ця технологія використовувалася для заміни системи доменних імен, то атаки типу «відмова в обслуговуванні» (DDoS-атаки) стали б неможливі.

Більш загальне застосування (і це вже реалізовано) - це використання блокчейн в криптографії. Адже це дуже логічний спосіб використання даної технології, враховуючи, що вона дозволяє передавати інформацію дуже безпечним способом. Вона також використовується для запобігання маніпуляції з даними. Оскільки природа блоків незмінна, використовуючи послідовне хешування разом з криптографією в децентралізованої структурі, ми можемо побудувати систему, якій буде практично неможливо маніпулювати. Інформаційна безпека, безсумнівно, йде по шляху адаптації технології блокчейна в не настільки віддаленому майбутньому. Принципова відмінність в технологічному підході дозволяє вийти за межі кінцевих пристроїв, включаючи безпеку цифровий «особистості» користувача, передачу інформації і захист критичної інфраструктури. Це дуже складні перетворення, але ми вже бачимо перші результати такого підходу.

Безпека блокчейна піддається перевірці

З технічної точки зору, будучи розподіленої і «взаємозалежної» базою даних, блокчейн являє собою міцну скелю. Втім, в залежності від доступності блоку, він може бути не настільки інтегрований, як може здатися. Для уточнення: існує величезна різниця між публічними і приватними блокчейнами. У той час як публічні блокчейни не мають обмеження на те, хто може отримати доступ до даних або здійснювати транзакції, в приватних блокчейнах ці операції доступні тільки для певного кола осіб.

Перші забезпечують прозорість, а другі надають більш високі рівні контролю, але тільки з боку певних адміністраторів. В обох випадках ми можемо знайти діри безпеки, часто побічно пов'язані з технологією (наприклад, чорний ринок криптовалюта). Блокчейн - це все ж поки що розвивається технологія, так що для її доведення до досконалості пройдуть ще довгі роки. Як і будь-яка технологія подібного типу, вона стикається із змінним технологічним контекстом: поява квантових обчислень, зміни в законодавстві, суперкомп'ютери ... Але очевидно, що блокчейн скоро буде відігравати провідну роль в сфері інформаційної безпеки.

Література:

1. https://habrahabr.ru/post/335994/
2. https://www.securitylab.ru/blog/company/PandaSecurityRus/342639.php

Таранюк Владислав Олександрович

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації
м. Київ

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

У сучасному суспільстві у зв’язку з входженням у світовий інформаційний простір швидкими темпами впроваджуються новітні досягнення комп’ютерних і телекомунікаційних технологій.

Так, вже створені локальні й регіональні обчислювальні мережі, великі території охоплені мережами мобільного зв’язку та Інтернет-простором. Системи телекомунікацій активно впроваджуються у фінансові, юридичні, промислові, торгові й соціальні галузі. У зв’язку з цим швидко зростає інтерес до проблем збереження й захисту інформації.

Тривалий час методи захисту інформації розроблялися тільки державними органами, а їхнє впровадження розглядалося як виняткове право певної держави. Проте в останні роки збільшилися спроби несанкціонованого доступу до конфіденційної інформації, а проблеми захисту інформації виявилися в центрі уваги багатьох вчених і спеціалістів різних країн.

Основними об'єктами забезпечення інформаційної безпеки України в загальнодержавних інформаційних і телекомунікаційних системах є:

- інформаційні ресурси, що містять державну таємницю та іншу інформацію обмеженого доступу;
- засоби та системи інформатизації (засоби обчислювальної техніки, інформаційно-обчислювальні комплекси, мережі та системи), програмні засоби (операційні системи, системи керування базами даних, інше загальносистемне та прикладне програмне забезпечення), автоматизовані системи керування, системи зв'язку та передачі даних, що здійснюють приймання, обробку, зберігання та передачу інформації обмеженого доступу, їхні інформативні фізичні поля;
- технічні засоби та системи, що обробляють відкриту інформацію, але розміщені в приміщеннях, де обробляється інформація обмеженого доступу;
- приміщення, призначені для проведення закритих переговорів, під час яких озвучується інформація обмеженого доступу.

Основними загрозами інформаційної безпеки України в загальнодержавних інформаційних і телекомунікаційних системах є:

- діяльність спеціальних служб іноземних держав, злочинних угруповань, організацій і груп, протизаконна діяльність окремих осіб, спрямована на одержання несанкціонованого доступу до інформації та здійснення контролю за функціонуванням інформаційних і телекомунікаційних систем;
- вимушене використання під час створення та розвитку інформаційних і телекомунікаційних систем імпортних програмно- апаратних засобів через об'єктивне відставання вітчизняної промисловості;
- порушення встановленого регламенту збору, обробки та передачі інформації, навмисні дії та помилки персоналу інформаційних і телекомунікаційних систем, відмови технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах;

Саме на вирішення питань ефективного захисту інформації, як від зовнішніх, так і від внутрішніх загроз, направлено створення комплексної системи захисту інформації в автоматизованих системах підприємств, установ та організацій.

Комплексна система захисту інформації (далі – КСЗІ) – це сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку й несанкціонованого доступу.

Головною метою створення КСЗІ є досягнення максимальної ефективності захисту за рахунок одночасного використання всіх необхідних ресурсів, методів і засобів, що виключають несанкціонований доступ до інформації, та створення умов обробки інформації

відповідно до чинних нормативно-правових актів України у галузі захисту інформації: Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації» та «Про захист персональних даних».

Комплексна система захисту інформації складається з організаційних та інженерно-технічних заходів. Зміст організаційних заходів полягає у розробці посадових інструкцій для користувачів та обслуговуючого персоналу, створенні правил адміністрування інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів, розробці планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації, навчанні правилам інформаційної безпеки користувачів тощо.

Щодо інженерно-технічних заходів, то це сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захищеності інформації, який необхідно забезпечити.

На сьогодні у Вінницькому апеляційному адміністративному суді проводяться роботи з впровадження комплексної системи захисту інформації, зокрема триває процес детального обстеження приміщення суду з метою розробки плану подальших дій щодо налагодження стабільного процесу функціонування КСЗІ у суді.

Отже, можна сказати, що потреба у створенні комплексної системи захисту інформації наразі досить актуальна, адже дає можливість організації побудувати цілісну систему інформаційної безпеки та унеможливити несанкціонований доступ сторонніх осіб до конфіденційної інформації.

Література:

1. http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive-zavdannya-sogodennya/
2. https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review

Бердник Олена Василівна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м.Київ

ПІДХОДИ ДО ОЦІНЮВАННЯ ЕФЕКТИВНСОТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ПРОНИКНЕННЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Розглянуто методики тестування стану захищеності інформаційних систем, адже проблема забезпечення необхідного рівня захищеності інформації в автоматизованих та інформаційно-телекомунікаційних системах залишається досить актуальною з розгляду умов інформаційної боротьби.

Інформаційні системи з кожним днем отримують все більшого розповсюдження та розвитку, інтегруються практично у всі сфери людської діяльності. Поруч із значними перевагами впровадження і розвитку інформаційних систем, існують і недоліки їх використання, а саме зростання кількості загроз безпеці інформаційних ресурсів.

Проблема забезпечення необхідного рівня захищеності інформації в автоматизованих та інформаційних системах залишається актуальною, особливо за умови інформаційної боротьби. Її науково-обґрунтоване вирішення проблеми визначається рішенням науково-технічної задачі, яка полягає у створенні моделей оцінювання необхідного та досягнутого рівня захищеності інформаційних систем, а також у розробці методів оцінювання ефективності систем захисту інформації.

Нині серед міжнародних стандартних і рекомендованих методик, які описують процес оцінки захищеності варто виділити наступні:

– OSSTMM (Open Source Security Testing Methodology Manual). Методика розроблена асоціацією ISECOM. Описано комплексний підхід до тестування захищеності на основі практичних методів подолання систем захисту.

– Стандарт PTES (Penetration Testing Execution Standard). Створено каталог сценаріїв атак і методів подолання систем захисту.

– Методологія OWASP (Open Web Application Security Project). Проект OWASP акумулює знання із забезпечення захисту Web-додатків.

– Методологія BSI Penetration Testing Model Служби захисту інформації Німеччини, де описано не тільки методологію, але й необхідні вимоги до процесу тестування.

– Information Systems Security Assessment Framework (OISSG). Розглянуто питання інформаційної безпеки, а також надано опис оцінювання безпеки апаратного і програмного забезпечення.

– NIST Guideline on Network Security Testing. Надано стандартні функції, які обов'язково включають до систем захисту інформації.

– ISACA Switzerland – Testing IT Systems Security With Tiger Teams.

– Cybersecurity Vulnerability Assessment Methodologies (Cybersecurity VAMs).

– При проведенні пошуку уразливостей для оцінки стану захищеності слід виділити декілька етапів:

- збір та аналіз інформації про об'єкт, що потребує захисту;
- розробка плану проникнення та вибір програмного та (або) апаратного забезпечення для реалізації атак;
- безпосередній тест на проникнення до інформаційної системи та спроби отримання доступу до інформації, що потребує захисту;
- складання звіту про результати тестування та розробка рекомендацій щодо усунення виявлених уразливостей.

Система захисту інформації, окрім безперервного забезпечення безпеки інформаційної системи, включає в себе постійний аналіз для випереджаючих вдосконалення методів захисту захищеності інформаційної системи на всіх її рівнях. Таким чином виникає необхідність використання системного підходу, шляхом об'єднання методик із різними підходами для підвищення якості інформаційної безпеки, інтегральної оцінки та підвищення ефективності управління інформаційними системами. Тож розглядається питання, що пов'язані з розробкою актуальної наразі методики тестування стану захищеності із адаптивним підходом до вибору об'єктів та складу систем захисту інформації.

Література:

1. Cisco исследовала основные тенденции в сфере информационной безопасности на украинском рынке [Електронний ресурс] – Режим доступу: http://www.pcweek.ua/themes/detail.php?ID=153526

2. Безпека інформації у інформаційно-телекомунікаційних системах . Матеріали міжнародної науково-практичної конференції. Київ – 2017. Вип.18. -91с.

Кисіль Владислав Андрійович
Державний університет телекомунікацій,
Навчально-науковий інститут захисту інформації

м.Київ

СИСТЕМА ЗАПОБІГАННЯ ВТОРГЕНЬ В БЕЗДРОТОВІЙ МЕРЕЖІ

Розглянуто аналіз систем запобігання вторгнень в бездротовій мережі WIPS та переваги їхнього застосування. Також проведено порівняння з технологією запропонованою компанією Cisco адаптивною системою запобігання вторгнень Cisco wIPS..

Актуальність застосування системи запобігання вторгнень пояснюється насамперед зростанням зацікавленості зловмисників до бездротових локальних мереж та, як наслідок, збільшенням варіантів та кількості можливих атак на ці мережі. Системи WIPS дозволяють виявити та знешкодити дії зловмисників ще на початковому етапі їх активності

Бездротова система запобігання вторгнень WIPS – це програмна, апаратна чи апаратно-програмна система мережної безпеки, призначена для моніторингу бездротової активності і визначення та запобігання спробам внутрішніх і зовнішніх мережевих вторгнень. Здійснюючи свій аналіз на канальному і фізичному рівнях мережевої моделі OSI, цей інструмент дозволяє організаціям успішно ідентифікувати і захищати свої мережі від несанкціонованих точок доступу, атак на бездротові мережі і атак типу «відмова в обслуговуванні».

Провідний виробник мережевого обладнання компанія Cisco запропонувала власний варіант даної технології – адаптивну систему запобігання вторгнень для безпровідних мереж.

Технології WISP та Cisco wIPS .забезпечують особливості виявлення та стримування (підключення смартфонів, DoS-атак, неавторизовані підключення, атаки на протокол WEP та MAC-спуфинг). Але технологія компанії Cisco забезпечує більш широкий спектр, в ній також присутні:

– автоматичне виявлення MAC-адреси;

– виявлення місця знаходження Non-WiFi передавачів, мостів, точок доступу;

– виявлення місця знаходження DoS-атак на фізичному рівні.

Нова функціональність, що виникає завдяки інфраструктурно інтегрованій архітектурі адаптивної системи Cisco wIPS, дає можливість адміністраторам наступні можливості:

1. Адаптивна система wIPS будується на моніторингу радіоефіру із застосуванням аналізу мережевого трафіку і аномалій в точках доступу та контролерах, аналізу в реальному часі ресурсів пристроїв в конфігурації мережі для виявлення загроз і контролю продуктивності.

2. Завдяки інтеграції в інфраструктуру безпровідної локальної мережі адаптивна система wIPS виходить за рамки пасивного моніторингу і здатна проникати в інфраструктуру для усунення загроз безпеки і проблем продуктивності в реальному часі.

3. Адаптивна система wIPS здатна використовувати точки доступу в мережі для визначення місця розташування шкідливих пристроїв та їх нейтралізації.

Отже, потреба використання системи запобігання вторгнень в бездротовій мережі оправдовується необхідністю забезпечення безпеки даних мережі. А запропонована компанією Cisco адаптивна система wIPS має ряд вдосконалень, що забезпечує більш точне і ретельне виявлення загроз.

Література:

1. Безпека інформації у інформаційно-телекомунікаційних системах . Матеріали міжнародної науково-практичної конференції. Київ – 2017. Вип.18. -91с

2. Cisco исследовала основные тенденции в сфере информационной безопасности на украинском рынке [Електронний ресурс] – Режим доступу: http://www.pcweek.ua/themes/detail.php?ID=153526

Кравцов Олександр Анатолійович

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації
м. Київ

ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ PORT-KNOCKING ДЛЯ ОРГАНІЗАЦІЇ БЕЗПЕКИ СЕРВІСУ ОБМЕЖЕНОГО ДОСТУПУ

Будь-який відкритий порт на веб-сервері представляє потенційну небезпеку. Зловмисники можуть сканувати сервер на відкриті порти за допомогою ПЗ nmap, дізнаватись версії запущених сервісів та їх найменування і здійснювати атаки на уразливі сервіси. Крім цілеспрямованих атак на сервіси зловмисники можуть застосовувати атаку на SSH, Telnet, FTP та HTTP-форми авторизації методом «грубої сили» (англ. bruteforce) . Такий тип атаки створює додаткове навантаження на сервер і без спеціального ПО, наприклад, fail2ban, яке блокуватиме невдалі спроби логіну, неможливо здійснити превентивні заходи для захисту сервера. Вибіркове блокування IP-адрес зловмисників в IPTABLES або перенесення сервісу на інший порт буде лише тимчасовим рішенням.

Якщо відмовитись від деяких сервісів немає ніякої можливості, а підвищити безпеку системи все ж необхідно, можна використати програму knockd, яка дозволяє закрити взагалі всі порти, зберігши при цьому можливість роботи з усіма популярними сервісами, такими як SSH, FTP, HTTP і т.д.

Ідея knockd проста і геніальна. Наприклад, користувач хоче встановити зв'язок з іншим комп'ютером через SSH. Для цього на віддаленій машині повинен бути постійно відкритий порт 22. Knockd дозволяє за допомогою iptables закрити 22 порт для зовнішнього світу і відкрити в потрібний момент тільки потрібному IP. Як knockd визначає, коли відкрити порт і кому конкретно надати доступ?

У перекладі з англійської «to knock» - стукати. Щоб knockd впізнав «хазяїна» і відкрив потрібний порт потрібно «постукати» в заздалегідь обумовлені порти в заздалегідь обумовленій послідовності. Наведений нижче приклад конфігурації knockd добре ілюструє відкриття і закриття SSH:

```
[options]
        logfile = /var/log/knockd.log
[openSSH]
        sequence = 700,800,900 seq_timeout = 5 command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT tcpflags = syn
[closeSSH]
        sequence = 900,800,700 seq_timeout = 5 command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT tcpflags = syn
```

В секції options потрібно вказати, куди зберігати логи підключень, в секції openSSH – умови для відкриття необхідного порту та сам порт в параметрах до команди IPTABLES, а в секції closeSSH – умови для закриття порту.

Якщо користувач спробує відкрити на віддаленій машині спочатку порт 700, потім 800, а потім 900, то knockd створить для фаєрвола нове правило, яке відкриває 22й порт для IP користувача. Після роботи користувач повинен закрити 22й порт, «постукавши» в зворотньому порядку: 900, 800, 700. Тепер про те, як «постукати». Зрозуміло, вручну відкривати будь-які порти не потрібно. Для зручності користувача існує команда knock. Приклад використання:

```
knock 127.0.0.1 700 800 900
```

Як перший аргумент вказується адреса сервера з knockd, всі інші аргументи є номерами портів, в які потрібно «постукати».

Примітки:

Для встановлення knockd на Ubuntu Server LTS 16.04 потрібно виконати команду в терміналі:

sudo apt-get install knockd.

Конфігурація knockd на більшості серверних дистрибутивів Linux знаходиться за адресою /etc/knockd.conf. Після внесення змін в конфігурацію необхідно перезапустити демон knockd:

sudo /etc/init.d/knockd restart

Якщо потрібно налаштувати knockd для інших сервісів, потрібно openSSH, closeSSH в конфігурації замінити до прикладу на openFTP, closeFTP. Для повного розуміння принципу роботи knockd та більш детального налаштування (відкриття доступу для діапазону IP, відкриття доступу на певний час) бажано знати основи правил IPTABLES.

Література:

1. *Інтернет-ресури liberatum.ru, habrahabr.ru, wikipedia.org.*

Андрущенко Ярослав Вячеславович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

WHAT IS SECURITY INTELLIGENCE AND WHY DOES IT MATTER TODAY?

In the introduction to this series, I asserted that people have many questions about security intelligence, then made the bold promise to answer six of the most pressing ones. Let's start by gaining a common understanding of security intelligence.

In a recent post, I proposed the following definition of security intelligence that I feel encapsulates where the industry is headed: *"Security intelligence is the real-time collection, normalization, and analysis of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise. The goal of Security Intelligence is to provide actionable and comprehensive insight that reduces risk and operational effort for any size organization."*

Breaking Down the Key Elements:

"Real-time"

Viewing time-stamped historical data or pouring over logs won't cut it. You need a view of what's happening right now, across your entire network.

"Collection, normalization and analysis"

This is where context and intelligence rule. Gather data from every relevant device and system in your network. Normalize it so you can compare activity across different devices and locations. Apply analytics and correlate activity and rule out the false positives that are the bane of every security analyst's world. Then present the results, clearly and simply, and put every relevant piece of information at your fingertips or eyeballs. Use every bit of data (Big Data anyone?) to enrich your view of security incidents, because context drives insight and discovery. Look, you might have already been breached and the evidence could be right in front of you, but you'll never see it if your solution can't intelligently correlate, analyze and present information to you.

"The IT security and risk posture of an enterprise"

Your ability to secure your data, intellectual property, IT assets and more from malicious outsiders and insiders, while maintaining reliable and efficient business operations. A crucial

element of protecting your brand and reputation, this can only be accomplished by collecting and analyzing the most comprehensive set of data generated across the organization.

"Actionable and comprehensive insight"

Collecting and analyzing all the relevant data in your network is a good start, but data (logs, query results, etc.) by themselves are worthless. (How many times have *you* experienced alert overload?) A security intelligence solution must make sense of your data and help you quickly research and remediate incidents.

"Reduces risk and operational effort"

(Enough said.)

"For any size organization"

Security intelligence isn't just for those with big budgets, staff and lots of patience. Today's modern security intelligence solution has evolved from the dinosaurs known as first-gen SIEM offerings. These products required major upfront implementation work and actually added to your ongoing headcount needs, rather than easing them. Today it's just the opposite – which means security intelligence is within the reach and budget of virtually any organization. I'll discuss this further in my next post in this series.

Security Intelligence Solution

Security intelligence solutions have evolved from a number of technologies you may be familiar with. In short, security intelligence builds on the data collection capabilities and compliance benefits of log management, the correlation, normalization and analysis capabilities of SIEM (security information and event management), the network visibility and advanced threat detection of NBAD (network behavior anomaly detection), the ability to reduce breaches and ensure compliance provided by risk management, and the network traffic and application content insight afforded by network forensics. Yet what distinguishes a modern Security Intelligence solution is that it's not a gift basket of discrete technologies wrapped together with duct tape, or worse, PowerPoint. It's a truly integrated solution built on a common codebase, with a single data management architecture and a single user interface.

Why Does Security Intelligence Matter

As for why it matters, I could discuss the increased prevalence and sophistication of advanced persistent threats. But instead, I thinkDavid Ingall of BGL Group (a leading UK insurance broker) puts it best:

"The move to the QRadar Security Intelligence Platform has been a real eye opener for us and has helped us to concentrate our efforts on the most important issues. Even without significant tuning, it has improved how we deal with security intelligence and it will form a core part of our infrastructure as we move forward."

Євтушенко Вікторія Максимівна

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м.Київ

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ ДЕРЖАВИ

В статті розглядається умови створення захисту інформаційного простору в Україні та за кордоном. Розглянуто основні проблеми захисту інформаційного простору в Україні. Запропоновано враховувати власний погляд на сучасні напрямки вирішення питань забезпечення інформаційної безпеки в Україні

Характерною ознакою інформаційної досконалості постіндустріальних країн є витіснення національної готівки у країни з менш досконалим інформаційним станом і, як результат, нееквівалентний обмін товарами і послугами. Водночас пріоритетними напрямками інформаційної діяльності на внутрішньому ринку є антимонопольна протидія, національне заощадження невідтворюваних ресурсів (передусім енергетичних та

екологічних), постійна структурна перебудова ринку праці і відповідний життєвий рівень громадян, які створюють і споживають інформацію.

Питання пов’язані з виявленням проблем щодо захисту інформаційного простору держави в сучасних умовах є актуальними. Тенденцію до надання пріоритетної ролі інформаційній безпеці наочно демонструють резолюції Генеральної асамблеї ООН: «Роль науки і техніки в контексті міжнародної безпеки, роззброєння та інших, пов’язаних з цим сфер» № 53/576 (1998 р.); «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» № 54/49 (1999 р.); № 55/28 (2000 р.); № 60/45 (2005 р.) [1].

Відомо що Генеральна Асамблея ООН ще у 2001 р. на 56-й сесії акцентувала поняття «Інформаційна та мережева безпека», що означає захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації і створення надійного джерела постачання обладнання, послуг та інформації. Інформаційна безпека того часу охоплювала захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. Уже у ті часи передбачалося, що недостатній захист життєво важливих інформаційних ресурсів і інформаційних і телекомунікаційних систем несе загрозу міжнародній безпеці.

Умови створення захисту інформації припускають застосування апаратні и програмні платформи зі складу довіреної програмно-апаратного середовища. Розглядається можливість комп'ютерних систем, виконувати те ж самепрограмне забезпечення у так називаній віртуальній машині. Прикладом віртуальної машини є Java, здатна працювати на платформах. Для реалізації віртуальної машини потрібно програмне забезпечення, про яке говорять як про кросплатформенне. Сукупниість технічних і програмних засобів, організаційних заходів, що сворюють розвиток систем спецільглшл призначення в захищеному виконані, що відповідають вимогам інформаційної безпеки, це співшдношення вимог інформаційної безпеки в сучасних умавах інфлрмацвйного противоборства.

В Україні існують необхідні закони, укази і внутрішні розпорядження різних структур, які є базою для організації кіберзахисту. Прийнята доктрина інформаційної безпеки України [2], затверджена указом президента. У державі створено ряд структур і підрозділів, які беруть участь у забезпеченні інформаційної безпеки держави. Дані структури займаються удосконаленням законодавства, вивченням і сертифікацією технічних засобів, забезпеченням захисту обчислювальних систем органів державної влади, розслідуванням виявлених кібер атак і прийняттям заходів для їх припинення.

В Україні існують компанії і фахівці з інформаційної безпеки, що займаються розробкою і впровадженням систем інформаційної безпеки. Спільна робота таких компаній і держави роблять можливим створення якісних і доступних технічних рішень для забезпечення захисту громадян державою. Не зважаючи на це ряд фахівців вважають, що основними причинами захисту інформаційного простору України є [3,4]:

- слабка інтегрованість України у світове інформаційне поле;
- недостатня кваліфікованість й активність її інформаційних служб;
- негативні наслідки міжпартійних відносин;
- некомпетентність працівників державних органів і установ;
- вплив на засоби масової інформації організованої злочинності;
- мафіозних структур;
- недосконаліть технічного захисту інформаційного простору України.

Ці решення будуть контролюватися і регламентуватися державою. Такі рішення забезпечать зв'язок державних структур з грамодянами. Також вони дозволять встановлювати списки заблокованих програм, WEB-сайтів та інтернет-вузлів, здійснюючи державний контроль над небажаним програмним забезпеченням і інтернет-ресурсами.

Які перші кроки у напрямку вирішенні питань забезпечення інформаційної безпеки можна розглядати:

1.Створення загальнодержавної системи інформаційної безпеки, складовими якої є системи криптографічного та технічного захисту інформації. Обов'язковою умовою створення цієї системи є розробка відповідної нормативної бази.

2.Розвиток та вдосконалення системи сертифікації систем та засобів захисту інформації, програмних та апаратно-програмних засобів.

3.Здійснення державного контролю за станом інформаційної безпеки в системах зв'язку, і в першу чергу в тих, що функціонують в інтересах управління держави

4.Відтворення системи органів контролю за станом інформаційної безпеки на підприємствах та контроль за їх діяльністю з боку держави.

5.Створення сприятливих умов для підприємств, організацій та налагодження виробництва вітчизняних засобів захисту інформації.

6.Створення системи підготовки наукових кадрів в галузі захисту інформації.

7.Вдосконалення системи підготовки та перепідготовки кадрів для роботи в сфері інформаційної безпеки

8. Врегулювання відносин в галузі використання Internet, і в першу чергу забезпечення безпеки державних інформаційних ресурсів.

Література:

1. *Исследование компании GfK об использовании глобальной сети Интернет к Украине: [Електронний ресурс]. – Режим доступу: http://www.gfk.ua/imperia/md/content/gfkukraine/presentations/111119_blogfest.pdf*
2. *Указ Президента України «Про Доктрину інформаційної безпеки України» від 8 липня 2009 року. – № 514/2009. - [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/9570.html*
3. *Морушко О. Проблеми захисту інформаційного простору держави в сучасних умовах- [Електронний ресурс]. – Режим доступу: http://ena.lp.edu.ua/bitstream/ntb/24671/1/13-40-41.pdf*
4. *Губерський Л. В., Макаренко Є. А. та ін. Інформаційна політика України: європейський контекст. – К. : Либідь, 2007.*

Прус Кирило Володимирович

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м.Київ

НОВІТНІ ЗАСОБИ ЗАХИСТУ КОМП'ЮТОРНИХ МЕРЕЖ

Розглянуто новітні засоби забезпечення інформаційної безпеки в телекомунікаційних системах та мережах. А саме: Quad9, *TDSSKiller, Malwarebytes Anti-Rootkit Beta, Norton Power Eraser, CHKRootkit, GMER. Ці програми допоможуть захистити мережі компаній, державних установ, підприємств, приватних осіб (груп), тощо.*

Перш за все, хотілося б розглянути такий сервіс як Quad9. Quad9 - це безкоштовний пакет доменних імен, який автоматично блокує шкідливі веб-сайти**.**

Система доменних імен Quad9 (DNS) - це безкоштовна служба безпеки, розроблена компанією IBM Security у співпраці з некомерційними дослідницькими органами, що займаються інформаційним пакетом, та Глобальним Cyber Alliance - з останньою групою, до якої входять деякі правоохоронні та державні установи. Це допомагає захистити користувачів від поширених вірусів і покращує продуктивність системи шляхом автоматичного блокування доступу до веб-сайтів, які, як відомо, є зловмисними.

Як працює Quad9*?* Quad9 забезпечує безпеку для запитів DNS, системи, яку комп'ютер використовує для перекладу IP-адрес для знаходження веб-сайтів.

Конфігурації DNS за замовчуванням можуть бути небезпечними на рівні підприємства, і вони найчастіше є метою розподілених атак на відмову в обслуговуванні.

Quad9 призначений для забезпечення додаткового рівня захисту. Служба допомагає захистити користувачів від кібер-атак, автоматично блокуючи веб-сайти, які, як відомо, крадуть особисту інформацію, заражають користувачів шкідливим програмним забезпеченням або здійснюють шахрайську діяльність.

Це робить це шляхом маршрутизації DNS запитів через безпечну мережу серверів у всьому світі. Він спирається на загрозу інтелекту, зібраної з підбору компаній, що займаються кібербезпекою, для забезпечення оцінки ризиків в реальному часі кожного веб-сайту, який ви відвідуєте, і блокує доступ до будь-якого, на якому можливе зараження.

Система забезпечує підвищену безпеку для фізичних осіб, ділових користувачів та їх клієнтів через мережі, пристрої, цифрові активи та продукти IoT.

Навіщо вибирати Quad9? Розробники Quad9 кажуть, що він пропонує більш високий рівень безпеки, ніж його конкуренти.

Служба блокує в середньому 30 000 веб-сайтів на день, перевіряючи їх на базі даних IBM X-Force, яка містить понад 40 мільярдів веб-сторінок, а також зображень та додаткових розвідувань, що надаються більш ніж 18 партнерами з безпеки віртуальної безпеки.

Quad9 також може мати перевагу в захисті приватності в Інтернеті. Вона не зберігає або не використовує будь-яку особисту інформацію від своїх користувачів, на відміну від інших служб DNS, які фіксують інформацію про веб-сайти, які ви відвідуєте, на вашому пристрої та про своє місцезнаходження.

Він також обіцяє зберегти швидкість доступу, який користувачі Інтернету очікували, маючи точку присутності у більш ніж 70 місцях у 40 країнах, коли вона буде запущена, загалом вона очікує подвоїтись протягом наступних 18 місяців.

Більшість людей використовують стандартного інтернет-провайдера, а не переходять на альтернативного постачальника, але перехід на Quad9 - це досить простий процес.

Як налаштувати Quad9? Ви можете налаштувати Quad9 за допомогою простої зміни конфігурації існуючої служби DNS.

Просто змініть налаштування DNS на своєму пристрої або маршрутизаторі, щоб вказати на IP-адресу 9.9.9.9, номер, з якого Quad9 малює своє ім'я.

Точна конфігурація залежатиме від вашої конфігурації мережі. Quad9 надає детальні вказівки щодо встановлення за допомогою посібників YouTube для Mac OS і Windows .

Користувачі, які потребують додаткової допомоги з процесом onboarding можуть надіслати електронною поштою компанії на support@quad9.net .

Наступні інноваційні засоби будуть спрямовані на забезпечення захисту інформації проти руткітів. Руткіт - це шкідлива програма, призначена для отримання зловмисниками прав суперкористувача на пристрої без відома жертви.

Руткіти можуть проникнути на ваш комп'ютер непоміченими, щоб перехоплювати системні функції, якщо у вас немає інструмента проти руткітів, який може виявити підозрілу поведінку.

Ризик руткітів можна пом'якшити, встановивши сучасне антивірусне програмне забезпечення та брандмауери, але кращий захист забезпечує додавання спеціального руткіт-сканера та видалення. Тут ми розглянемо деякі з кращих інструментів на ринку.

TDSSKiller - це безкоштовний анти-руткітний інструмент, розроблений російським виробником програмного забезпечення Kaspersky Lab. Програмне забезпечення аналізує систему та містить резюме результатів або більш просунутий звіт, якщо ви хочете. Потім він може видалити будь-які руткіти, які він знаходить.

Ця утиліта безкоштовна і завершує сканування приблизно через 15 секунд. Він також дозволяє вибрати, які області комп'ютера сканувати. Він може працювати без нагляду і в нормальному, і в безпечному режимі на Microsoft Windows.

Malwarebytes Anti-Rootkit Beta - це окремий продукт, призначений для виявлення та видалення руткітів на комп'ютерах Windows. Інструмент виконує глибокий сканування комп'ютера для будь-яких підозрілих дій.

Він сповіщає вас, коли виявляє загрозу, і пропонує їх видалити. Сканування повторюється, поки не буде загрози. Сканування вимагає часу, але він глибоко виконує пошук для вбудованих руткітів. В даний час це в бета-версії, отже, ім'я, що означає, що немає ніякої гарантії, що воно не призведе до помилок.

Norton Power Eraser - це ще один безкоштовний інструмент для видалення загрози для Windows, який доповнює стандартне антивірусне програмне забезпечення. Щоб запустити сканування в режимі руткітів, перед його запуском потрібно перезавантажити комп'ютер.

Програмне забезпечення перевіряє результати за списком довірених і зловмисних програм і позначає будь-яку останню для видалення. Сканування настільки агресивне, що це може спричинити шкоду нешкідливим файлам, однак пошкодження може бути скасовано, відновлюючи вилучене виявлення.

CHKRootkit - є єдиним інструментом у нашому списку, який працює на Linux. Програма шукає локальні системи для ознак підозрілої діяльності та перевіряє наявність відомих файлів руткітів, сканування серверів для компромісів.

Програма потім надсилає системному адміністратору електронний лист із докладною інформацією про будь-які загрози, які він виявляє. Інструмент доступний безкоштовно, але нові випуски не є настільки правильними, як деякі з інструментів Windows, які ми рекомендуємо.

GMER - це безкоштовний інструмент для виявлення руткітів для Windows, розроблений компанією Avast. Програмне забезпечення є легким і не вимагає перезавантаження системи, але це доводить ретельне сканування, яке виявляє глибоко вбудовані загрози.

Тим не менш, це нелегко використовувати, і інтерфейс є різким. Користувачам потрібно зрозуміти результати, які він виробляє, оскільки він може позначати потенційні ознаки руткітів, які фактично використовуються законні додатками, які не слід видаляти. Якщо ви хочете отримати більш простий інструмент, вам, можливо, краще обслуговувати один з інших в нашому списку.

Література:

1. *Best anti-rootkit tools:* https://www.computerworlduk.com/galleries/security/best-anti-rootkit-tools-3672860/
2. *What* is Quad9?: https://www.computerworlduk.com/security/what-is-quad9-3672365/

Хворостяний Родіон Віталійович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

АЛГОРИТМИ АСИМЕТРИЧНОГО ШИФРУВАННЯ ТА ЇХ ВИКОРИСТАННЯ ПІД ЧАС ЗАХИСТУ ІНФОРМАЦІЇ

Асиметричні алгоритми шифрування дозволяють забезпечувати шифрування інформації, що направляться йому необмеженою кількістю відправників. Крім того, використання цих алгоритмів дозволяє проводити автентифікацію учасників обміну інформацією та здійснювати контроль цілісності переданої інформації.

Загальний принцип роботи асиметричних алгоритмів полягає в наступному:

- учасник інформаційного обміну генерує пари ключів. При цьому дані, зашифровані одним із ключів, можуть бути розшифровані тільки іншим ключем. Один із цих ключів є відкритим (загальнодоступним), інший — закритим (секретним). Секретний ключ учасник зберігає в себе, а відкритий поширює всім бажаючої відправляти йому шифровані повідомлення. Відкритий ключ - це функція, за допомогою якої відправник може зашифрувати своє повідомлення, але ні він сам, ні хто-небудь інший не може дешифрувати це повідомлення, використовуючи відкритий ключ. Для дешифрування повідомлення (тобто здійснення зворотної операції — обчислення значення аргументу за значенням функції) необхідно знати деякий параметр зазначеної функції, що, по суті, і є закритим ключем;

- відправник повідомлення шифрує інформацію відкритим ключем і передає її одержувачеві по каналах зв'язку;

- одержувач дешифрує повідомлення, використовуючи свій закритий ключ.

Найпоширеніші алгоритми асиметричного шифрування:

- RCA. Алгоритм розроблено в 1977 році. Використовує відкриті ключі, що забезпечують перетворення інформації «тільки в одну сторону» (шифрування) за рахунок фактори- зації (розкладання на множники) великих чисел;

- ECC (Elliptic Curve Cryptography). Односпрямованість перетворень (шифрування) забезпечується в цьому методі складністю математичних обчислень, пов'язаних з еліптичними кривими.

Електронний цифровий підпис є електронним еквівалентом власноручного підпису. Він використовується не тільки для автентифікації відправника повідомлення, але й для перевірки цілісності повідомлення. При використанні цифрового підпису для автентифікації відправника повідомлення застосовуються відкритий і закритий ключі. Процедура схожа на здійснювану в асиметричному шифруванні, але в цьому випадку закритий ключ служить для шифрування, а відкритий - для дешифрування. Алгоритм застосування електронного цифрового підпису складається з ряду операцій:

- генерується пара ключів: відкритий і закритий;

- відкритий ключ передається зацікавленій стороні (одержувачеві документів, підписаних стороною, яка сгенерувала ключі);

- відправник повідомлення шифрує його своїм закритим ключем і передає одержувачеві по каналах зв'язку;

- одержувач дешифрує повідомлення відкритим ключем відправника.

Суть у тім, що створити зашифроване повідомлення, при розшиф- ровці якого відкритим ключем виходить вихідний текст, може тільки власник закритого ключа, тобто відправник повідомлення. Використовувати для цього відкритй ключ неможливо.

Разом з електронним цифровим підписом звичайно застосовуються хеш-функції. Вони служать для того, щоб крім автентифікації відправника, яка забезпечується електронним цифровим підписом, гарантувати, що повідомлення не має перекручувань, і одержувач одержав саме те повідомлення, що підписав і відправив йому відправник.

Хеш-функція - це процедура обробки повідомлення, в результаті дії якої формується рядок символів (дайджест повідомлення) фіксованого розміру. Найменші зміни в тексті повідомлення приводять до зміни дайджесту при обробці повідомлення хеш-функцією. Таким чином, будь- які зміни, внесені в текст повідомлення, відіб'ються на дайджесті.

Алгоритм застосування хеш-функції

- перед відправленням повідомлення обробляється за допомогою хеш-функції. В результаті отримують його стислий варіант (дайджест); саме повідомлення при цьому не

змінюється - отриманий дайджест шифрується закритим ключем відправника (підписується електронним цифровим підписом) і пересилається одержувачу разом з повідомленням;

- одержувач розшифровує дайджест повідомлення відкритим ключем відправника;

- одержувач обробляє повідомлення тою ж хеш-функ- цією, що й відправник, і отримує його дайджест; якщо дайджест, надісланий відправником, і дайджест, отриманий в результаті обробки повідомлення одержувачем, збігаються, роблять висновок, що у повідомлення не було внесено змін.

Шумлянська Аліна Олександрівна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

Інформаційна безпека держави — це стан її захищеності, при якому спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам.

Відповідно до законодавства України поняття "інформаційна безпека" має таке визначення:*"стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації."*

Інформаційна безпека держави характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) по відношенню до небезпечних (дестабілізуючих, деструктивних, суперечних інтересам країни тощо), інформаційним впливам, причому як до впровадження, так і до вилучення інформації.

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

Поняття інформаційних технологій (ІТ) включає в себе широкий обсяг дисциплін і сфер діяльності і стосується технічних засобів обробки і передачі даних (чи інформації).

В англійській мові поняття безпеки ІТ має два значення. Поняття *функціональної безпеки* (англ. *safety*) означає, що система коректно і у повному обсязі реалізує *ті і лише ті* цілі, що відповідають намірам її власника, тобто функціонує відповідно до існуючих вимог. Поняття власне *інформаційної безпеки* (англ. *security*) стосується безпечності процесу технічної обробки інформації і є властивістю функціонально безпечної системи. Така система повинна унеможливлювати несанкціонований доступ до даних та запобігати їхній втраті у разі виникнення збоїв.

Говорячи про інформаційну безпеку, часто мають на увазі інформаційну безпеку в найзагальнішому сенсі, як комплекс заходів, покликаний зменшити число ймовірних шкідливих сценаріїв чи розмір збитків, яких може зазнати підприємство у разі розголошення конфіденційної інформації. З цієї точки зору інформаційна безпека — це економічний параметр, який повинен враховуватися у роботі підприємства, а інформацію (або дані) можна розглядати як певний товар або цінність, що підлягає захисту, а відтак вона має бути доступною лише для авторизованих користувачів чи програм.

Інформаційна безпека організації — цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Інформаційна безпеки особистості характеризується як стан захищеності особистості, різноманітних соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору.

Для характеристики основних властивостей інформації як об'єкта захисту часто використовується модель CIA:

- Конфіденційність (англ. *confidentiality*) — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем
- Цілісність (англ. *integrity*) — означає неможливість модифікації неавторизованим користувачем
- Доступність (англ. *availability*) — властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час.

Література:

1. -майбутнє та інформаційне право / [В. Брижко, В. Цимбалюк, Ю. Базанов]; за ред. доктора економічних наук, професора, члена-кореспондента АПрН України М. Швеця. – [2-е вид., доп.]. – К. : НДЦПІ АПрН України, 2006. – 234 с.

2. Макаренко Є.А. Європейська інформаційна політика [Текст]: [монографія] / Є.А. Макаренко. – К.: Наша культура і наука, 2000. – 368 с.

3. Про Концепцію Національної програми інформатизації [Електронний ресурс]: Закон України: [від 04.02.1998 р. № 75/98-ВР]. – режим доступу: www.rada.gov.ua; www.bod.kiev.ua

Чабан Богдан Валетнинович
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

КАТЕГОРИИ АТАК

Во время работы компьютерных систем часто возникают различные проблемы. Некоторые – по чьей-то оплошности, а некоторые являются результатом злоумышленных действий. В любом случае при этом наносится ущерб. Поэтому будем называть такие события атаками, независимо от причин их возникновения.

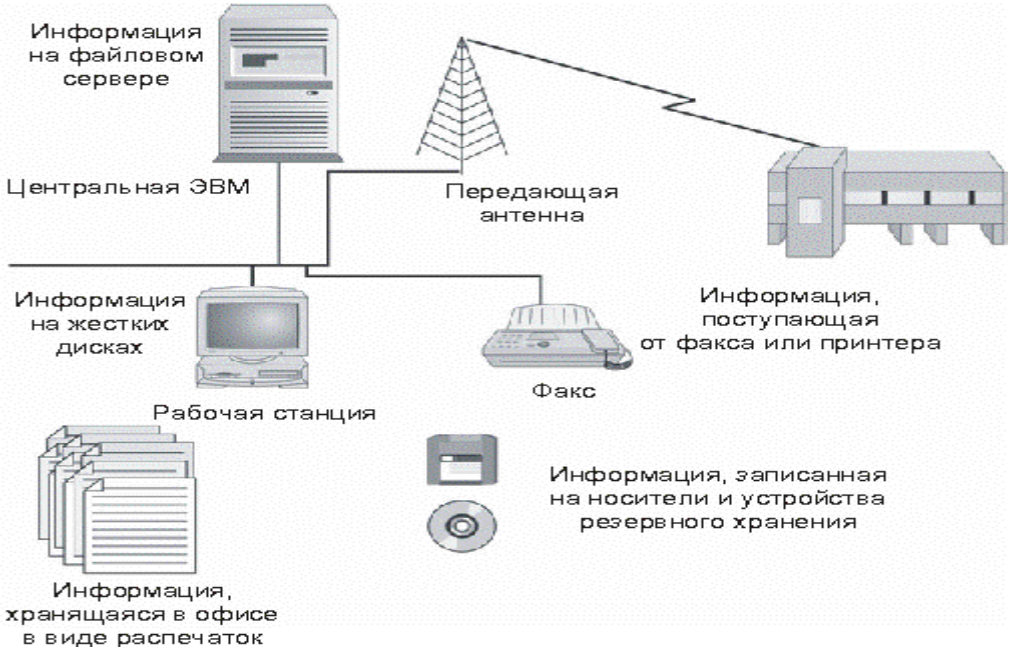
Существуют четыре основных категории атак:

1. Атаки доступа.
2. Атаки модификации.
3. Атаки на отказ в обслуживании.
4. Атаки на отказ от обязательств.

Определение атаки доступа

Атака доступа – это попытка получения информации злоумышленником, для просмотра которой у него нет разрешений, и которая направлена на нарушение конфиденциальности информации. Для осуществления данной атаки необходима информация и средства для ее передачи.

Рис. 1. Атака доступа возможна везде, где существуют информация и средства для ее передачи



К атакам доступа можно так же отнести подсматривание, подслушивание и перехват.

• Подсматривание – это просмотр файлов или документов для поиска интересующей злоумышленника информации.

• Подслушивание – когда кто-то слушает разговор, участником которого он не является (часто при этом он использует электронные устройства).

• Перехват – захват информации в процессе ее передачи к месту назначения.

Прежде, чем разобраться, как выполняются атаки доступа, давайте разберемся, где хранится информация в электронном виде.

А хранится она:

• на рабочих станциях;
• на серверах;
• в портативных компьютерах;
• на флоппи-дисках;
• на компакт-дисках;
• на резервных магнитных лентах.

Последние четыре пункта мы рассматривать не будем, т.к. злоумышленник может их просто украсть. С первыми двумя дело обстоит иначе. При легальном доступе к системе злоумышленник будет анализировать файлы, просто открывая один за другим. При несанкционированном доступе, взломщик постарается обойти систему контроля и получить доступ к нужной информации. Сделать это не сложно. Необходимо установить в компьютерной системе сетевой анализатор пакетов (sniffer). Для этого взломщик должен повысить свои полномочия в системе или подключиться к сети. Анализатор настроен на захват любой информации, проходящей по сети, но особенно – на пользовательские идентификаторы и пароли.

Подслушивание выполняется и в глобальных компьютерных сетях типа выделенных линий и телефонных соединений. Однако такой тип перехвата требует наличия соответствующей аппаратуры и специальных знаний. В этом случае наиболее удачным местом для размещения подслушивающего устройства является шкаф с электропроводкой.

А с помощью специального оборудования квалифицированный взломщик может осуществить перехват в системах оптико-волоконной связи. Однако, что бы добиться успеха, он должен поместить свою систему в линии передачи между отправителем и

получателем информации. В интернете это выполняется посредством изменения разрешения имени, в результате чего имя компьютера преобразуется в неправильный адрес. Трафик перенаправляется к системе атакующего вместо реального узла назначения. При соответствующей настройке такой системы отправитель так и не узнает, что его информация не дошла до получателя.

Определение атаки модификации

Атака модификации – это попытка неправомерного изменения информации. Она направлена на нарушение целостности информации и возможна везде, где существует или передается информация.

Существует три вида атаки модификации – это замена, добавление и удаление.

• Замена – замена существующей информации направлена как против секретной, так и общедоступной информации.

• Атака добавления – добавление новых данных.

• Атака удаления означает перемещение существующих данных.

Все три вида атаки модификации используют уязвимые места систем, например, «бреши» в безопасности сервера, позволяющие заменить домашнюю страницу. И даже в этом случае необходимо основательно поработать во всей системе, чтобы воспрепятствовать обнаружению. Т.к. транзакции нумеруются последовательно, и удаление или добавление неправильных операционных номеров будет замечено.

В случае, если атака модификации производится при передаче информации, то необходимо сначала выполнить перехват интересующего трафика, а затем внести изменения в информацию перед ее отправкой к пункту назначения.

Атаки на отказ в обслуживании

Атаки на отказ в обслуживании (Denial-of-service, DoS) – это атаки, запрещающие легальному пользователю использование системы, информации или возможностей компьютеров. Другими словами, эта атака «Вандализм», т.к. злоумышленник В результате DoS-атаки обычно не получает доступа к компьютерной системе и не может оперировать с информацией.

• DoS-атака, направленная против информации – уничтожает, искажает или переносит в недоступное место последнюю.

• DoS-атака, направленная на приложения, обрабатывающие или отображающие информацию, или на компьютерную систему, в которой эти приложения выполняются – делают невозможным решение задач, выполняемых с помощью такого приложения.

• Общий тип DoS-атак (отказ в доступе к системе) ставит своей целью вывести из строя компьютерные системы, в результате чего сама система, установленные на ней приложения и вся сохраненная информация становится недоступной.

• Отказ в доступе к средствам связи заключается в выведении из строя средств связи, которые лишают доступ к компьютерным системам и информации.

• DoS-атаки, нацеленные непосредственно на компьютерную систему, реализуются через эксплоиты, использующие уязвимые места операционных систем или межсетевых протоколов. С помощью этих «брешей» атакующий посылает в приложение определенный набор команд, который оно не в состоянии правильно обработать, в результате чего приложение выходит из строя. Перезагрузка восстанавливает его работоспособность, но на время перезагрузки работать с приложением становится невозможно.

Определение атаки на отказ от обязательств

Атака на отказ от обязательств направлена против возможности идентификации информации, или дать неверную информацию о реальном событии либо транзакции.

К данному виду атаки относятся:

• Маскарад – это выполнение действий под видом другого пользователя или другой системы.

• Отрицание события – это отказ от факта совершения операции.

• DoS-атаки против интернета – это атака на серверы корневых имен интернета.

Світіна Ольга Сергіївна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ДЖЕРЕЛА ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Джерела загроз інформаційній безпеці розуміються як вихідні підстави (причини) небезпечного впливу на життєво важливі інтереси особистості, суспільства і держави в інформаційній сфері.

За типом *джерела* загрози підрозділяються на такі, що мають *соціальний* і

природний характер. Загрози соціального характеру проявляються в процесі взаємодії між соціальними спільнотами (групами), а природні загрози - взаємодії соціальних груп з навколишнім природним середовищем.

Залежно від *характеру прояву* небезпечного впливу на об'єкти інформаційної безпеки джерела загроз можуть носити зовнішній або внутрішній характер.

До *зовнішніх джерел* загроз інформаційної безпеки відносяться:

• діяльність іноземних політичних, економічних, військових, розвідувальних та інформаційних структур, спрямована проти інтересів Російської Федерації в інформаційній сфері;

• прагнення ряду країн до домінування і ущемлення інтересів Росії у світовому інформаційному просторі, витіснення її з зовнішнього і внутрішнього інформаційних ринків;

• загострення міжнародної конкуренції за володіння інформаційними технологіями та ресурсами;

• діяльність міжнародних терористичних організацій;

• збільшення технологічного відриву провідних держав світу і нарощування їх можливостей щодо протидії створенню конкурентоспроможних російських інформаційних технологій;

• діяльність космічних, повітряних, морських і наземних технічних та інших засобів (видів) розвідки іноземних держав;

• розробка низкою держав концепцій інформаційних війн, які передбачають створення засобів небезпечного впливу на інформаційні сфери інших країн світу, порушення нормального функціонування інформаційних і телекомунікаційних систем, збереження інформаційних ресурсів, отримання несанкціонованого доступу до них.

До *внутрішних джерел* загроз інформаційної безпеки відносяться:

• недостатня економічна міць держави і недостатнє фінансування заходів щодо забезпечення інформаційної безпеки;

• критичний стан вітчизняних галузей промисловості;

• відставання від провідних країн світу за рівнем інформатизації всіх видів людської діяльності (державного управління, промисловості, кредитно-фінансової сфери, освіти, охорони здоров'я, сфери послуг та побуту громадян);

• недостатня розробленість нормативної правової бази, що регулює відносини в інформаційній сфері, а також недостатня правозастосовна практика;

• несприятлива криміногенна обстановка, що супроводжується тенденціями зрощування державних і кримінальних структур в інформаційній сфері, отримання кримінальними структурами доступу до конфіденційної інформації, посилення впливу організованої злочинності на життя суспільства;

• недостатня координація діяльності щодо формування та реалізації єдиної державної політики в галузі забезпечення інформаційної безпеки Російської Федерації;

• нерозвиненість інститутів громадянського суспільства і недостатній державний контроль за розвитком інформаційного ринку Росії;

• зниження ефективності системи освіти і виховання, недостатня кількість кваліфікованих кадрів у галузі забезпечення інформаційної безпеки;

• недостатня активність федеральних органів державної влади, органів державної влади суб'єктів в інформуванні суспільства про свою діяльність, у роз'ясненні прийнятих рішень, у формуванні відкритих державних ресурсів і розвитку системи доступу до них громадян.

Література:

1. *Інформаційні технології в юридичній діяльності під редакцією П.У Кузнецова.*
2. *Інформаційна безпека України в умовах євроінтеграції. Авторів В.А Лілкан, Ю.Е. Максименко, В.М. Желіховський.*
3. *Підручник - Забезпечення інформаційної безпеки держави.*

Кучер Владислав Ігорович

Держаний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

СТЕГАНОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ОБ'ЄКТІВ МУЛЬТИМЕДІА

Питання збереження конфіденційності інформаційних потоків під час їх зберігання та передачі каналами зв'язку, стоїть на провідній позиції у процесі забезпечення інформаційної безпеки особистості, суспільства та держави. На сьогодні найбільш поширеними технологіями захисту інформації є процедури поєднанням криптографічних та стеганографічних методів (комбіновані).

Відповідно до обраного типу контейнера визначається метод приховування інформаційних потоків.

Приховування даних у просторовій області.

Загальний принцип таких алгоритмів полягає у заміні надлишкової, малозначної частини зображення бітами секретного повідомлення. Для витягу повідомлення необхідно знати алгоритм, по якому воно розміщувалося у зображенні.

1) Метод заміни найменш значущого біту.

Метод заміни найменш значущого біту - найбільш розповсюджений метод серед методів даного класу. НЗБ несуть у собі найменше інформації. Як відомо, людина, у більшості випадків, не може розрізнити інформацію у даних бітах. При чому в чорно-білому зображенні (в якому кожен піксель кодується одним байтом) об'єм вбудованих даних може займати до 1/8 об'єму зображення-контейнера. Популярність даного методу обумовлена його простотою та можливістю приховувати доволі великі об'єми даних. В більшості випадків цей метод працює із растровими зображеннями, представленими у форматі без компресії даних (GIF, BMP).

2) Метод псевдовипадкового інтервалу.

Даний підхід полягає у псевдовипадковому розподілення бітів повідомлення по зображенню-контейнеру, внаслідок чого відстань між двома вбудованими бітами визначається псевдовипадково. Цей підхід ефективний у випадку, коли об'єм повідомлення набагато менший за контейнер. Недоліком такого методу є те, що біти повідомлення розподіляються по контейнеру у тому ж порядку, що і у самому повідомленні.

3) Метод псевдовипадкової перестановки.

Основою цього методу є генератор псевдовипадкових чисел (ПВЧ), який формує певну псевдовипадкову послідовність індексів $j_1, j_2 \ldots j_k$ і *k-й* біт повідомлення зберігається у пікселі із індексом j_k .

Функція перестановки має бути псевдовипадковою і мати достатньо великий набір індексів, щоб жоден індекс не повторився жодного разу і не відбулося «перетину».Цей метод забезпечує рівномірний розподіл інформаційних бітів по контейнеру. Імовірність перетину зменшується із зменшенням співвідношення (довжина повідомлення)/(довжина контейнера).

4) Метод блочного приховування.

При використанні даного методу зображення-контейнер розбивають на блоки, що не перетинаються між собою. Для кожного блоку визначають певний біт парності. В кожному блоці приховують один секретний біт. Якщо визначений біт парності не відповідає секретному біту, проводять інвертування НЗБ блоку, доки біт парності не буде, по суті, секретним бітом.

Цей метод, як і всі попередні, має низьку стійкість до викривлень, але він має свої переваги – існує можливість модифікувати такий піксель у блоку, щоб статистика контейнера була змінена якомога менше.

5) Метод заміни палітри.

Ще один метод приховування даних у зображенні – зміна палітри кольорів. Палітра кольорів зображення зберігається у вигляді списку пар індексів (i, A_i) який визначає відповідність між індексом i та його вектором кольору. Кожному пікселю зображення ставиться у відповідність певний індекс у таблиці. Оскільки порядок кольорів у палітрі не важливий для відновлення зображення, конфіденційна інформація може бути прихована шляхом перестановки кольорів у палітрі.

Приховування даних у частотній області зображення.

Найпоширеніші методи приховування даних у частотній області використовують вейвлет-перетворення та дискретно-косинусне перетворення (ДКП). Це пояснюється широким їх розповсюдженням у технологіях компресії цифрових зображень.

1) Метод відносної заміни величин коефіцієнтів ДКП.

При використанні даного методу зображення розбивається на блоки 8х8 пікселів. До кожного з блоків застосовується ДКП, в результаті чого отримується матриця коефіцієнтів ДКП 8х8. Кожен блок призначений для приховування одного біту даних. Приховування проводиться заміною одного коефіцієнту у блоку.

2) Метод Бенгама-Мемона-Ео-Юнга.

Даний метод є модифікацією попереднього. Основною зміною є той факт, що при використанні даного методу секретна інформація приховується не в усіх блоках зображення, а тільки в обраних блоках (найбільш підходящих).

3) Метод Фрідріх.

Згідно цього методу, який по суті є комбінацією двох алгоритмів, секретні дані вбудовуються в низькочастотні та середньочастотні коефіцієнти ДКП. Каскадне використання цих двох алгоритмів може дати непогані результати відносно стійкості стеганографічної системи до різних атак.

4) Методи розширення спектру.

Система зв’язку є системою із розширеним спектром, коли:

· Полоса частот, яка використовується при передачі, значно ширша за необхідну для передачі повідомлення, за рахунок чого співвідношення сигнал/шум є доволі низьким, і повідомлення важко знайти у каналі (особливо розрізнити органам чуття людини);

· Розширення спектру відбувається за допомогою, так званого, розширюючого сигналу, який не залежить від інформації, що передається. Присутність енергії сигналу в усіх частотних діапазонах робить радіосигнал стійким до завад, а інформацію, що знаходиться у контейнері - стійкою до її видалення.

· Відновлення первинної інформації відбувається шляхом зіставлення отриманого сигналу та синхронізованої копії кодового(розширюючого) сигналу [1].

Приховування даних у аудіосигналах

Особливий розвиток отримали стеганографічні методи приховування інформації у аудіосередовищі.

1) Кодування найменш значущих бітів (часова область).

Даний метод є найпростішим серед методів приховування даних у аудіосигналах. Його суть полягає у заміні НЗБ у кожній точці вибірки із сигналу, представленого у двійковій послідовності. Використання даного методу обумовлює високу пропускну здатність каналу, платою за що є добре чутний низькочастотний шум. Дану проблему можна вирішити використанням записів, на яких і так присутній певний шум, наприклад, звук стадіону на живому концерті. Але, як і у аналогічних методах приховування інформації у нерухомих зображеннях, заповнені контейнери є вразливими до сторонніх впливів окрім випадків, коли секретна інформація вбудована із внесенням надлишковості. Однак, останнє при збільшенні стійкості каналу зменшує швидкість передачі даних.

2) Метод фазового кодування (частотна область).

Основною ідеєю методу фазового кодування є заміна фази вихідного звукового сегменту на деяку опорну фазу, характер зміни якої і відражає повідомлення, яке необхідно приховати. При правильному використанні даний метод є найефективнішим для приховування даних у аудіосигналах, оскільки, доки модифікація фази достатньо мала, наявність повідомлення може бути абсолютно не відчутно на слух (не враховуючи використання спецтехніки).

3) Метод розширення спектра (часова область).

Даний метод майже ідентичний до методу приховування даних у нерухомих зображеннях шляхом розширення спектру. Тобто, секретне повідомлення розподіляється по частотам несучого сигналу рівномірно, так щоб співвідношення сигнал(повідомлення)/шум у каналі було дуже низьким і не виникло підозр щодо наявності повідомлення. Сигнал-контейнер, в даному випадку, обирається набагато більший за секретне повідомлення.

4) Приховування даних із використанням ехо-сигналу.

Даний метод вбудовує повідомлення у аудіосигнал-контейнер шляхом введення у нього ехо-сигналу. Дані приховуються зміною параметрів ехо-сигналу: початкової амплітуди, швидкості затухання та зсуву. Коли зсув між оригінальним сигналом та ехо-сигналом зменшується, починаючи з певного значення, ССЛ стає нездатною виявити різницю між двома сигналами, а ехо-сигнал сприймається лише як додатковий резонанс. Цей метод непростий у реалізації, тому що це значення зсуву дуже важко визначити. Воно значною мірою залежить від якості початкового сигналу і, само собою, від слухача.

Приховування даних у відео даних

Стеганографічні методи приховування рідше всього використовуються у відеоданих, так як даний файл складається з динамічних зображень (фреймів) та звукової доріжки. Для цих цілей найчастіше використовуються контейнери у форматах MPEG – 2, MPEG – 4 та AVI. Варто також зазначити, що досі не використовується в якості контейнерів одночасно аудіо доріжки та фрейми.

На сьогодні існує три методи для приховування інформації у відеоданих , а саме:

Метод вбудовування на рівні коефіцієнтів – біти приховуваного повідомлення вбудовуються в коефіцієнти ДКП. Для зменшення внесених змін використовують додатковий спеціальний сигнал. В зв’язку з обмеженням бітової швидкості, при вбудовування змінюється лише 10-12% коефіцієнтів ДКП. При використанні даного методу приховувана інформація зберігається при фільтруванні, зашумленні (адитивним шумом) і дискретизації.

1) *Метод вбудовування інформації на рівні бітової площини* - цей метод відрізняється високою пропускною здатністю і легкими обчисленнями. Але є й істотний недолік: інформація, вбудована таким чином, може бути легко видалена. При повторному

накладенні послідовності біт якість відео погіршиться незначним чином, а приховувана інформація буде знищена.

2) *Метод вбудовування інформації за рахунок енергетичної різниці між коефіцієнтами* - в снові цього методу лежить диференціальне вбудовування енергії. Цей метод може використовуватись для багатьох алгоритмів стиснення, не тільки для MPEG. Інформація вбудовується шляхом видалення декількох коефіцієнтів ДКП.

Висновки

Стеганографічні системи захисту інформаційних потоків, під час їх зберігання та передачі займають провідній позиції у процесах забезпечення інформаційної безпеки. У роботі проведено аналіз існуючих стеганографічних методів.

Літаратура

1. *Юдін О.К., Конахович Г.Ф., Корченко О.Г. Захист інформації в мережах передачі даних: Підручник. – К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009.*
2. *Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография //теория и практика/Г.Ф. Конахович, А.Ю. Пузыренко.—Киев: МК-Пресс. – 2006.*
3. *Моденова О. В. Стеганография и стегоанализ* в видеофайлах //Прикладная дискретная математика. Приложение. – 2010. – №. 3.

Перепелиця Ліна Сергіївна

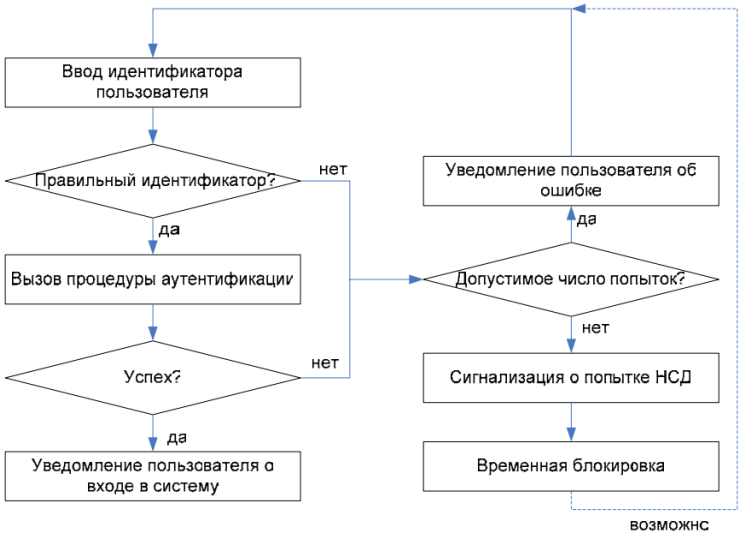
Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ. МЕТОДЫ АУТЕНТИФИКАЦИИ

Под ***идентификацией*** принято понимать присвоение субъектам доступа уникальных идентификаторов и сравнение таких идентификаторов с перечнем возможных. В свою очередь, ***аутентификаци***я понимается как проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Тем самым, задача идентификации – ответить на вопрос «кто это?», а аутентификации - «а он ли это на самом деле?».



Базовая схема идентификации и аутентификации

Приведённая схема учитывает возможные ошибки оператора при проведении процедуры аутентификации: если аутентификация не выполнена, но допустимое число попыток не превышено, пользователю предлагается пройти процедуру идентификации и аутентификации еще раз.

Всё множество использующих в настоящее время методов аутентификации можно разделить на 4 большие группы:

1.Методы, основанные на знании некоторой секретной информации.

Классическим примером таких методов является парольная защита, когда в качестве средства аутентификации пользователю предлагается ввести пароль – некоторую последовательность символов. Данные методы аутентификации являются наиболее распространёнными.

2.Методы, основанные на использовании уникального предмета.

В качестве такого предмета могут быть использованы смарт-карта, токен, электронный ключ и т.д.

3.Методы, основанные на использовании биометрических характеристик человека.

На практике чаще всего используются одна или несколько из следующих биометрических характеристик:

- отпечатки пальцев;
- рисунок сетчатки или радужной оболочки глаза;
- тепловой рисунок кисти руки;
- фотография или тепловой рисунок лица;
- почерк (роспись);
- голос.

Наибольшее распространение получили сканеры отпечатков пальцев и рисунков сетчатки и радужной оболочки глаза.

4.Методы, основанные на информации, ассоциированной с пользователем.

Примером такой информации могут служить координаты пользователя, определяемые при помощи GPS. Данный подход вряд ли может быть использован в качестве единственного механизма аутентификации, однако вполне допустим в качестве одного из нескольких совместно используемых механизмов.

Широко распространена практика совместного использования нескольких из перечисленных выше механизмов – в таких случаях говорят о ***многофакторной аутентификации***

Особенности парольных систем аутентификации

При всём многообразии существующих механизмов аутентификации, наиболее распространённым из них остаётся парольная защита. Для этого есть несколько причин, из которых мы отметим следующие:

- Относительная простота реализации.

Действительно, реализация механизма парольной защиты обычно не требует привлечения дополнительных аппаратных средств.

- Традиционность.

Механизмы парольной защиты являются привычными для большинства пользователей автоматизированных систем и не вызывают психологического отторжения – в отличие, например, от сканеров рисунка сетчатки глаза.

В то же время для парольных систем защиты характерен парадокс, затрудняющий их эффективную реализацию: стойкие пароли мало пригодны для использования человеком. Действительно, стойкость пароля возникает по мере его усложнения; но чем сложнее пароль, тем труднее его запомнить, и у пользователя появляется искушение записать неудобный пароль, что создаёт дополнительные каналы для его дискредитации.

Маслова Юлія
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ОСНОВНІ ЗАГРОЗИ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Загрози інформаційній безпеці — сукупність умов і факторів, що створюють небезпеку життєвоважливим інтересам особистості, суспільства і держави в інформаційній сфері. Основні загрози інформаційній безпеці можна розділити на такі групи:

- загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;
- загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);
- загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації;
- загрози праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і достоїнства і т. ін.

Фактори загроз за видовою ознакою поділяються на:

- політичні;
- економічні;
- організаційно-технічні.

Під політичними факторами загроз інформаційній безпеці розуміють:

- зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;
- інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, та розповсюджують інформацію з метою здобуття односторонніх переваг;
- становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;
- знищення колишньої командно-адміністративної системи державного управління, а також системи забезпечення безпеки;
- порушення інформаційних зв'язків унаслідок утворення на території колишнього СРСР нових держав;
- прагнення пострадянських країн до більш тісного співробітництва із закордонними країнами в процесі проведення реформ на основі максимальної відкритості сторін;
- низька загальна правова та інформаційна культура сторін.
- перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур — виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;
- критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;
- розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними організаційно-технічними факторами загроз інформаційній безпеці є:

- недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки;

- недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;
- широке використання у сфері державного управління та кредитно-фінансової сфери незахищених від витоку інформації імпортних технічних та програмних засобів для зберігання, обробки та передавання інформації;
- зростання обсягів інформації, яка передається відкритими каналами зв'язку;
- загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері

Глобальні фактори загроз інформаційній безпеці:

- недружня політика іноземних держав у галузі глобального інформаційного моніторингу, розповсюдження інформації, розповсюдження інформації та нових інформаційних технологій;
- діяльність іноземних розвідувальних та спеціальних служб;
- діяльність іноземних політичних та економічних структуру, спрямована проти інтересів держави;
- злочинні дії міжнародних груп, формувань та окремих осіб.

Регіональні фактори загроз інформаційній безпеці:

- використання інформаційної інфраструктури колишнього СРСР для передавання конфіденційної інформації;
- невідповідність інформаційного забезпечення державних та суспільних інститутів сучасним вимогам управління економічними, політичними та соціальними процесами;
- відставання від розвинених країн світу з темпів та масштабів розробки та впровадження нових інформаційних технологій;
- недопустимо високий рівень технологічної залежності держави від зарубіжних держав у зв'язку з широким використанням імпортних засобів обчислювальної техніки, систем телекомунікації, зв'язку та інформаційних технологій;
- розвиток зарубіжних технічних засобів розвідки, та промислового шпигунства, що дозволяє одержати несанкціонований доступ до конфіденційної інформації, у тому числі такої що складає державну таємницю;
- зростання злочинності в інформаційній сфері;
- використання старих методів та засобів захисту національних інформаційних мереж, широке розповсюдження комп'ютерних вірусів, призначених для ураження систем управління та зв'язку;
- відсутність ефективної системи забезпечення цілісності, незмінності та схоронності нетаємної інформації, у тому числі такої, що є інтелектуальною власністю.

Локальні фактори загроз інформаційній безпеці:

- перехоплення електронних випромінювань;
- застосування підслуховуючих пристроїв або закладок;
- дистанційне фотографування;
- розкрадання носіїв інформації та промислових відходів;
- копіювання носіїв інформації з подоланням заходів захисту;
- незаконне приєднання до апаратури та ліній зв'язку;
- упровадження та використання комп'ютерних вірусів і т. ін.

Література

1. *«Стратегія забезпечення кібернетичної безпеки України» (від 15.03.2016 № 96/2016)*
2. *«Стратегія національної безпеки України» (в редакції від 12 лютого 2007 року № 105/2007)*

3. *Бурячок, В. Л. ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА: СОЦІОТЕХНІЧНИЙ АСПЕКТ/ В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. – Київ: ДУТ, 2015. – 287 с.*

Протасенко Костянтин Костянтинович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ОРГАНІЗАЦІЙНО-РОЗПОРЯДЧЕ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ СЛУЖБИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті розглянуто співвідношення служби захисті інформації в автоматизованих системах і служби інформаційної безпеки, запропоновано визначення служби інформаційної безпеки та окреслено основні організаційно-розпорядчі документи, що регламентують функціонування служби інформаційної безпеки підприємства, установи, організації.

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб [1], що у свою чергу суттєво підвищує значення спеціалістів із захисту інформації.

Зазначені спеціалісти на підприємствах, в установах та організаціях входять до складу служби захисту інформації (далі – СЗІ), створення якої регламентовано Типовим положенням про службу захисту інформації в автоматизованій системі (НД ТЗІ 1.4-001-2000), в якому також визначаються завдання, функції, структура, повноваження СЗІ, а також організації її робіт із захисту інформації впродовж всього життєвого циклу автоматизованих систем (далі – АС).

Зважаючи на те, що *захист інформації* – це діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС в цілому [2], а *інформаційна безпека* – це захищеність інформації та інфраструктури, яка її підтримує від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації й підтримуючої інфраструктури [3], можна встановити, що інформаційна безпека є більш ширшим поняттям ніж захист інформації

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають. З метою забезпечення інформаційної безпеки на підприємствах, в установах, організаціях доцільно створювати службу інформаційної безпеки (далі – СІБ), яка складатиметься із спеціалістів СЗІ та спеціалістів інформаційної безпеки.

Нормативно закріплене визначення поняття «служба інформаційної безпеки» в Україні відсутнє, тому можна запропонувати таке визначення:

служба інформаційної безпеки – це організаційно-технічна одиниця системи забезпечення інформаційної безпеки, яка реалізує певні задачі, спрямовані на протидію загрозам інформаційній безпеці.

Підставою для створення СІБ є наказ (розпорядження) керівника підприємства, установи, організації, яким затверджується:

1)положення про СІБ;

2)склад СІБ;

3)інструкції співробітників СІБ.

Контроль за виконанням такого наказу (розпорядження) доцільно покласти на керівника підприємства, установи, організації.

Положення про СІБ є нормативним документом підприємства, установи, організації, що регламентує роботу служби, в якому визначаються завдання, функції, структура СІБ, повноваження та відповідальність співробітників СІБ, її взаємодія з іншими підрозділами підприємства, установи, організації та зовнішніми організаціями.

Положення про СІБ може бути складено у вигляді:

- доповнення до Положення про службу захисту інформації в автоматизованих системах – на підприємствах, в установах, організаціях, де наказом керівника затверджено положення про службу захисту інформації, створеної відповідно до НД ТЗІ 1.4-001-2000.

  У такому разі, в доповненні доцільно викласти:

  - завдання і функції спеціалістів СІБ, які не зазначені у положенні про службу захисту інформації;
  - структуру СІБ, розширену у порівнянні зі СЗІ;
  - взаємодію СІБ з іншими підрозділами підприємства, установи, організації та зовнішніми організаціями;
- окремого документа, складеного на базі положення про СЗІ – на підприємствах, в установах, організаціях, де не було створено СЗІ та прийнято рішення про створення СІБ.

З метою забезпечення кібербезпеки, організації та здійснення ефективної боротьби із кіберзагрозами, кібершпигунством, кібертероризмом та кіберзлочинністю, забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, до складу СІБ доцільно включити спеціалістів із кіберзахисту. Завдання та функції таких спеціалістів викладені у розділі 4 Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96/2016.

Особи відповідальні за зберігання матеріальних носіїв інформації здійснюють свою діяльність відповідно до вимог Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою Кабінету Міністрів України від 18.12.2013 № 939, Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затвердженої постановою Кабінету Міністрів України від 19.10.2016 № 736, та інших нормативно-правових актів.

У залежності від обсягів і особливостей завдань СІБ до її складу можуть входити спеціалісти різного фаху:

- спеціалісти з питань захисту інформації від витоку технічними каналами;

- спеціалісти з питань захисту каналів зв’язку і комутаційного обладнання, налагодження і керування активним мережевим обладнанням;

- спеціалісти з питань адміністрування засобів захисту, керування базами даних захисту;

- спеціалісти з питань захищених технологій обробки інформації»

- спеціалісти з кіберзахисту;

- особи відповідальні за зберігання матеріальних носіїв інформації;

- спеціалісти, відповідальні за встановлення та експлуатацію інженерно-технічних засобів охорони та інші.

За посадами співробітники СІБ поділяються на такі категорії (за рівнем ієрархії):

- керівник СІБ;
- заступник керівника СІБ (у разі необхідності);
- адміністратори захисту АРМ (безпеки БД, безпеки систем, документів тощо);
- системні адміністратори;
- інженери з кіберзахисту;
- інженери з експлуатації інженерно-технічних засобів охорони;
- фахівці із захисту матеріальних носіїв інформації;
- інші спеціалісти СІБ.

СІБ може бути штатним підрозділом підприємства, установи, організації, безпосередньо підпорядкованим керівнику, який відповідає за забезпечення безпеки інформації, або структурною (штатною або позаштатною) одиницею підрозділу служби безпеки підприємства, установи, організації, в разі їх наявності.

Штатність чи позаштатність СІБ на підприємстві, установі, організації визначається рішенням керівництва підприємства, установи, організації відповідно.

Структура СІБ, її склад і чисельність визначається фактичними потребами підприємства, установи, організації для виконання вимог політики безпеки інформації та затверджується керівництвом. Чисельність і склад СІБ мають бути достатніми для виконання усіх завдань з інформаційної безпеки підприємства, установи, організації.

Інструкції спеціалістам СІБ складаються за прийнятою на підприємствах, установах, організаціях формою та, як правило, містять:

- загальні положення;
- обов'язки спеціаліста;
- права спеціаліста;
- відповідальність спеціаліста.

СІБ здійснює свою діяльність щодо реалізації основних організаційних та організаційно-технічних заходів зі створення і забезпечення функціонування комплексних систем захисту інформації та комплексів технічного захисту інформації у відповідності з планами робіт. Підставою для розроблення планів робіт є:

- план захисту інформації в АС, що є сукупністю документів, згідно з якими здійснюється організація захисту інформації на всіх етапах життєвого циклу АС;
- план технічного захисту інформації (далі – ТЗІ) підприємства, установи, організації, що повинен містити такі документи:
  - перелік розпорядчих, організаційно-методичних, нормативних документів з ТЗІ, а також вказівки щодо їхнього застосування;
  - інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту;
  - інструкції, що встановлюють обов`язки, права та відповідальність персоналу;
  - календарний план ТЗІ.

Календарний план може мати такі розділи:

- організаційні заходи;
- контрольно-правові заходи;
- профілактичні заходи;
- інженерно-технічні заходи.
- робота з кадрами.

До планів включаться наступні основні заходи:

- разові (одноразово виконувані, необхідність у повторенні яких виникає за умови повного перегляду прийнятих рішень з захисту інформації);

- постійно виконувані (заходи, що потребують виконання безперервно або дискретно у випадковий чи заданий час);
- періодично виконувані (з заданим інтервалом часу);
- виконувані за необхідності (заходи, що потребують виконання під час здійснення або виникнення певних змін в АС чи зовнішньому середовищі).

За результатами виконання планів СІБ готуються звіти про забезпечення безпеки інформації на підприємствах, в установах, організаціях, які регулярно (наприклад – щоквартально) подаються керівництву.

У звітах відображається стан інформаційної безпеки на підприємствах, в установах, організаціях, із зазначенням досягнутих показників і виявлених недоліків, робиться висновок і надаються пропозиції щодо покращення стану інформаційної безпеки.

Матеріально-технічну базу для забезпечення діяльності СІБ складають засоби захисту інформації, програмне забезпечення, технічне та інженерне обладнання, засоби вимірювань і контролю, відповідна документація, а також інші засоби та обладнання, які необхідні для виконання СІБ покладених на неї завдань.

СІБ фінансується за рахунок:
- коштів, що виділяються на підприємствах, в установах та організаціях на утримання органів управління;
- прибутку підприємств і організацій та інших коштів за рішенням керівництва;
- коштів, отриманих за виконання СІБ договірних робіт та надання послуг;
- інших джерел фінансування, не заборонених законодавством України.

На підставі викладеного вище, зважаючи на необхідність захисту інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, незалежно від форми, у якій вони перебувають, у подальших дослідженнях за темою статті доцільно розглянути нормативно-правові та інші питання щодо створення, організації та забезпечення функціонування служби інформаційної безпеки підприємства, установи, організації.

Література:

1. *Стратегія кібербезпеки України затверджена Указом Президента України від 15 березня 2016 року № 96/2016[Електронний ресурс] – Режим доступу: http://zakon4.rada.gov.ua/laws/show/96/2016*
2. *НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102106&cat_id=46556&ctime=1344502446343*
3. *Берко А.Ю., Висоцька В.А., Рішняк І.В. МЕТОДИ ТА ЗАСОБИ ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОЇ [Електронний ресурс] / Берко А.Ю., Висоцька В.А., Рішняк І.В. – Режим доступу: http://www.nbuv.gov.ua/old_jrn/natural/Vnulp/Komp-systemy/2007_591/14.p*

Алексейчук Олена Дмитрівна
Державний Університет Телекомунікацій
м. Київ

SOCIAL ENGINEERING IN INFORMATIONAL SECURITY OF BANKING SPHERE

The relativity of human factor to social engineering in information security is investigated. Human vulnerabilities, concerning the human factor to information security, which may lead to an illegal method of obtaining information, are presented.

Широко визнано, що співробітники банківських організацій часто є слабкою ланкою в захисті своїх інформаційних активів. Соціальна інженерія не отримала достатньої уваги з точки зору впливу людського фактору.

Людський фактор має великий вплив на успіх і невдачу щодо забезпечення та захисту підприємств, послуг, систем та захисту інформації. Якщо безпека системи упускається розробником, IT-система стає вразливою, і може бути експлуатована зловмисником. Зловмисники, які атакують, використовуючи соціальну інженерію, намагаються отримати конфіденційну інформацію, націлюючись на уразливості людей - тобто, слабкі сторони в організації завдяки особливостям і поведінці людей.

Соціальна інженерія - це метод управління людьми без використання технічних засобів. Метод заснований на використанні слабкості людського фактора і вважається дуже руйнівним.

Мета даної статті - аналіз людського фактору в області інформаційної безпеки, аналіз того, як інформація розуміння безпеки може стати основним інструментом подолання цих недоліків.

Людські чинники

Людські та організаційні чинники можуть бути пов'язані з інформаційною безпекою.

Фактори, що впливають на безпеку комп'ютера з точки зору соціальної інженерії діляться на дві категорії, а саме людський фактор і організаційний фактор. Людські чинники є важливіші за інші чинники. Вони поділяться на наступні групи:

- фактори, які відносяться до управління, а саме організація робочого місця, робоче завантаження працівника;
- фактори, пов'язані з кінцевим користувачем - помилки в роботі персоналу.

Далі ми зосередимося на чотирьох людських факторах, які мають серйозні наслідки для впливу на поведінку користувачів

1. Нестача мотивації зарплата, немає кар’єрного зростання

Багато організацій вважають, що співробітників необхідно мотивувати на безпечну поведінку з інформаційними активами, і керівництво повинно бути в змозі визначити, що мотивує їх персонал.

2.Недолік обізнаності

Недолік обізнаності пов'язаний з відсутністю загальних знань про про захист інформації та можливі атаки на неї. Загальні приклади відсутності обізнаності можуть бути наступними: користувачі не знають, як визначити шпигунські програми і шпигунське ПЗ і як важливо вказувати надійний пароль. Вони не можуть захистити себе від крадіжки особистих даних, а також як контролювати доступ інших користувачів до їх комп'ютера.

3. Переконання

Прикладами ризикованого переконання є наприклад, наступні: вважається, що установка антивірусного програмного забезпечення вирішує проблеми щодо захисту інформації.

4. Безграмотне користування технологіями захисту

Навіть найкраща технологія не може досягти успіху у вирішенні проблем інформаційної безпеки без безперервного людського співробітництва та ефективного використання цієї технології. Загальні приклади неналежного використання технологій захисту полягає в наступному: створення несанкціонованої реконфігурації систем, доступ до паролів, отримання несанкціонованої інформації. Ризики в області комп'ютерної безпеки можна класифікувати декількома способами: перевищення привілеїв, помилки та упущення, відмова в обслуговуванні, соціальна інженерія, несанкціонований доступ, розкрадання особистих даних, фішинг, шкідливі програми і несанкціоновані копії.

У якості висновку слід зазначити, що основним недоліком у сфері запобігання негативним проявам соціальної інженерії є відсутність системної роботи щодо її виявлення та подолання. Було чітко визначено людські фактори, що викликають проблеми безпеки і

представлено пропозиції щодо способів їх подолання. Наслідком цього є те, що інформаційна безпека є ключем до пом'якшення загроз безпеки, викликаних людською уразливістю. Організації повинні розвивати і підтримувати культуру, в якій цінують позитивну поведінку в області безпеки, щоб безпека починалася і закінчувалася кожною людиною, яка пов'язана з їхньою інфраструктурою, бізнесом і їх послугами.

Література:

1. *"Искусство обмана"/ Кевин Митник, 2014.-360 с.*
2. *Социальная инженерия и социальные хакеры/ Кузнецов Максим Валерьевич, Симдянов Игорь Вячеславович, 2007.-20 с.*
3. *"Искусство вторжения"/ Кевин Д. Митник, Вильям Л. Саймон, 2005.-78 с.*

Писаренко Павло Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (КІБЕРЗАХИЩЕНОСТІ) В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ ПРИ ВПРОВАДЖЕНІ ТА НАДАННІ ІННОВАЦІЙНИХ ПОСЛУГ

Оповідь ведеться про поняття інновації та інноваційної діяльності в телекомунікаційних системах і мережах, а також про забезпечення кіберзахищенності послуг цієї діяльності, важливість цього на сучасному ринку продуктів та ресурсів інтелектуальної діяльності. Розглядається концепція авторського права як спосіб захистити конфіденційність інтелектуальної власності, при цьому залишивши її доступною для широкого окола споживачів.Цифровий підпис.

Відповідно до міжнародних стандартів інновація визначається як кінцевий результат інноваційної діяльності, втілений у вигляді нового або вдосконаленого продукту чи технологічного процесу, який використовується в практичній діяльності або в новому підході до соціальних послуг. Необхідною ознакою інновації є науково-технічна новизна та виробниче її використання. Ринок новацій визначається як сукупність об'єктів інтелектуальної власності, яка характеризується цілісністю і володіє якістю новизни порівняно з попередніми новаціями. Основним товаром ринку є продукт інтелектуальної діяльності.

Кіберзахищеність інноваційних послуг гарантує максимально ефективне використання наявних та безпечне залучення додаткових інвестиційних ресурсів. Вона передбачає формування умов для збільшення можливостей створення і комерціалізації інновацій, використання науково- технологічного потенціалу та є результатом цілеспрямованої діяльності щодо впровадження інноваційної моделі розвитку.

Головними об’єктами кіберзахисту в даному випадку є запобігання компрометації інформації сторонніми фізичними (юридичними) особами, при цьому збереження доступності відповідної інформації для цільової аудиторії.

Одним із аспектів, яким однозначно не слід нехтувати є захист прав та інтересів суб'єктів інноваційної діяльності.

Фізична особа, яка винайшла якийсь твір або продукт насамперед повинна використати авторське право на свою продукцію. Головною проблемою є крадіжка інноваційних ідей. Саме для запобігання цього потрібно авторське право. Наступний шлях – придбання патенту (охоронний документ, що засвідчує пріоритет, авторство і право власності на винахід (корисну модель).Також потрібна торгівельна марка, яка відрізняє товари і послуги учасників об'єднання підприємств

Суб'єктами авторського права є автори творів, їх спадкоємці та особи, яким автори чи їх спадкоємці передали свої авторські майнові права. Об'єктами авторського права є

твори у галузі науки, літератури і мистецтва: літературні письмові твори (книги, брошури, статті); виступи, лекції, промови, проповіді та інші усні твори; комп'ютерні програми, бази даних;музичні твори з текстом і без тексту тощо;

У сучасному кіберпросторі своєрідним аналогом підпису є ЕЦП, який у кожного документу унікальний, тобто при модифікації документу, або самого підпису, скомпрометованість буде одразу ідентифікована із 100% вірогідністю. ЕЦП забезпечує неможливість автора відмовитися від цього документу, а також вказує, що це саме його власність.

Література:

1. *Зима, В. Безпека глобальних мережевих технологій / В. Зима, А. Молдовян, Н. Молдовян – СПб, 2000.*
2. *Семенов Г. Цифровий підпис. / / Відкриті системи .- 2002. № 07-08.*
3. *Біячуев Т.А. Безпека корпоративних мереж / під ред. Л. Г. Осовецкого. - СПб: СПб ГУ ІТМО, 2004.*

Ковтун Юлія Олександрівна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

КИБЕРБЕЗОПАСНОСТЬ – БИЧ СОВРЕМЕННОСТИ

"Кибербезопасность невозможно купить — ее можно только построить."
Михаил Шелемба, генеральный директор "Датагруп"

В наше время, все чаще мы слышим о том, что уровень киберприступности растет с каждым днем всё быстрее, что специалистов в области кибербезопасности нет. Но при этом, каких-то решительных действий по изменению ситуации не происходит. В данной работе рассмотрена проблема кибербезопасности, а так же возможные пути ее решения.

Каждый из нас, хотя бы раз, видел пёстрые заголовки газет и/или статей о том, что хакеры взломали банковскую систему и сняли крупную сумму денег, что критически важные государственные объекты были подвержены кибератаке и так далее. Что же это такое, эта кибератака? ***Кибератака*** (хакерская атака) в узком смысле – покушение на информационную безопасность компьютерной системы. **[1]**

Зачастую, в таких статьях еще и определяют виновных: государство, "внешние агрессоры", неготовность и т.п. К кибератаке невозможно подготовится. Это явление спонтанное, у него нет четкого графика. И как видим, сейчас практически во всех госучреждениях создаются группы по реагированию на инциденты. Стоит отметить, что пока засекут атаку и примут определенные меры по их устранению, может пройти много драгоценного времени. Ведь с каждой минутой, та или иная организация, терпит колоссальные убытки.

И в итоге получается стандартная схема: организацию атакуют, отдел реагирования на инциденты начинает панически пытаться устранить угрозу, а информация, или другие ценные активы, утекают в руки преступников. И, в основном, схема не меняется. Еще, наверное, ни разу не слышали, чтобы в газетах написали: "На Х-организацию была осуществлена сильная кибератака, но система безопасности выстояла под ударом и группой реагирования уже установлен алгоритм действия преступников и приняты меры по устранению полученных и новонайденных уязвимостей". Такой исход был бы в некоторой степени даже утопией.

Для того, чтобы выявить проблему, нужно знать, что означает понятие кибербезопасности. ***Кибербезопасность*** — это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к

управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя **[2].** Что является причиной того, что кибератаки так часто достигают своей цели, и получают необходимую жизненно важную информацию, если вообще не выводят из строя критически важные системы. Причиной можно назвать тех специалистов и руководители, которые хотят всё и сразу. Если мы приняли закон, он должен сразу же работать. Если мы хотим уберечь свои активы от кибератаки, нам должны предоставить программу/систему/компьютер, которые это сделают за нас. И желательно как можно дешевле, и чтобы "всё в одном". Мы же не хотим тратить больше денег и времени.

Ничего сразу не делается. Перед тем, как начать строить нашу систему кибербезопасности, нам нужны действительно грамотно написанные законы, стандарты и требования. Брать на вооружение общепринятые, и создавать свои, которые не будут идти наперерез им, но будут иметь свою "изюминку". Мы ведь говорим о кибербезопасности.

Далее нам нужен проект или, другими словами, план. Он будет ответом на простой вопрос – "Что мы хотим?".

Следующим этапом выступает подбор персонала. Персонала, который будет регулировать работу и состояние всей системы. Улучшать ее, менять необходимые элементы без потери ее работоспособности в период модернизации. Такие специалисты, должны быть профессионалами своей деятельности, можно даже сказать, влюблены в нее. Нельзя построить действенную систему защиты, если относится к этой работе халатно. Для эффективной работы, нужно мощное "железо". Компьютеры и сервера, системы телекоммуникаций, которые идут в ногу со временем. Но не стоит забывать о главном принципе – адекватность и оправданность вложенных средств.

И последним по счету, но не по значению этапом будет постройка системы защиты. Всевозможные программы и устройства, с умом и толком подобранные и правильно настроенные и введенные в эксплуатацию. Очень важно, чтобы персонал имел навыки не только работы с современными продуктами по кибербезопасности, но и умел создать альтернативу. Создать программу (устройство), которое, пусть и будет выполнять те же функции, но будет делать это "по-своему". Можете быть уверенными, что даже если у вас установлена самая лучшая программа по безопасности, злоумышленники уже знаю, как она работает и где ее изъяны.

Следуя этим простым этапам, любая организация сможет создать действенную систему кибербезопасности. Но в первую очередь, на высшем уровне должен быть реализован именно первый этап – подготовлены и приняты достойные законы, стандарты и требования. Которые будут учитывать все аспекты и будут универсальными, а не только направлены на одну из сфер жизнедеятельности страны (организации) и/или период времени.

Список использованной литературы:

1. Кибератака. [Электронный ресурс]: - Режим доступа - https://www.securitylab.ru/news/tags/%EA%E8%E1%E5%F0%E0%F2%E0%EA%E0/

2. Кибербезопасность [Электронный ресурс]: (статья) - Режим доступа - http://www.itu.int/net/itunews/issues/2010/09/20-ru.aspx

Кисельов Олексій Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

МЕТОДЫ ПРЕДОТВРАЩЕНИЯ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

С появлением информационных технологий и внедрением в них своих персональных данных, а также любых сведений, все больше становится актуальным вопрос утечки конфиденциальной информации и предостережение этого. Если раньше распространение информации можно было достаточно эффективно контролировать административными мерами, предоставляя физический доступ к ней только для ограниченного числа лиц, то в эпоху всеобщей информатизации контролировать доступ к информации и тем более ее перемещение становится сложнейшей задачей. Поэтому всё острее встаёт проблема инсайдеров и утечек конфиденциальной информации. Причем это актуально как и для владельцев бизнеса, различных спецслужб, государственных учреждений, которые кооперируют множеством информацией с ограниченным доступом, так и для рядовых пользователей интернета.

Для того чтобы решить проблему с инсайдерами и НСД, было решено создать технологию предотвращения утечки конфиденциальной информации - **Information Leak Protection.** Это так же обусловлено тем, что большая часть традиционных средств защиты, таких как антивирусы, межсетевые экраны и системы аутентификации не способны обеспечить эффективную защиту от внутренних нарушителей. Целью такого рода нарушителей (инсайдеров) является передача информации за пределы компании с целью дальнейшего несанкционированного использования - продажи, опубликования ее в открытом доступе и т.д.

В рамках создания таких систем решаются задачи:

- предотвращения утечек конфиденциальной информации по основным каналам передачи данных:
- исходящий веб-трафик (HTTP, FTP, P2P и др.)
- исходящая электронная почта, внутренняя электронная почта
- системы мгновенного обмена сообщениями, сетевая и локальная печать
- контроля доступа к устройствам и портам ввода-вывода, к которым относятся: дисководы, CD-ROM, USB - устройства, инфракрасные, принтерные (LPT) и модемные (COM) порты.

Говоря о таких системах мы имеем ввиду такие технологии, как: **DLP** *(Data Loss Prevention)* и **IPC** *(Information Protection and Control).*

DLP *(Data Loss Prevention)* - технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек.

Необходимость защиты от внутренних угроз была очевидна на всех этапах развития средств информационной безопасности. Однако первоначально внешние угрозы считались более опасными. В последние годы на внутренние угрозы стали обращать больше внимания, и популярность DLP-систем возросла. У DLP-системах зазвичай використовуються три методи ідентифікації: імовірнісний, детерміністський і комбінований. Системи, засновані на першому методі, здебільшого використовують лінгвістичний аналіз контенту і «цифрові відбитки» даних. Такі системи прості в реалізації, але недостатньо ефективні і характеризуються високим рівнем помилкових спрацьовувань. Системи, що використовують детермінований підхід (мітки файлів), дуже надійні, але їм не вистачає гнучкості. Комбінований підхід поєднує обидва методи з аудитом середовища зберігання та обробки даних, що дає можливість досягти оптимального вирішення проблеми захисту конфіденційності інформації..Є два основні підходи аналізу контенту. Перший підхід базується на фільтрації контенту, тобто змістовного наповнення інформації. Це означає, наприклад, що при перевірці на секретність стандартних офісних документів у форматі .doc система спочатку переведе їх у текстовий формат, а потім,

використовуючи заздалегідь підготовлені дані, винесе по цьому тексту вердикт. Контекстна фільтрація використовує принципово іншу схему: система перевіряє контекст, в якому передається інформація: витягує мітки файлу, дивиться на його розмір або аналізує поведінку користувача, тобто сигнатуру.

Information Protection and Control **(IPC)** — технология защиты конфиденциальной информации от внутренних угроз. Решения класса IPC предназначены для защиты информации от внутренних угроз, предотвращения различных видов утечек информации, корпоративного шпионажа и бизнес-разведки. Термин IPC соединяет в себе две основные технологии: шифрование носителей информации на всех точках сети и контроль технических каналов утечки информации с помощью технологий Data Loss Prevention (DLP). **Технология IPC** является логическим продолжением технологии DLP и позволяет защищать данные не только от утечек по техническим каналам, то есть инсайдеров, но и от несанкционированного доступа пользователей к сети, информации, приложениям и в тех случаях, когда непосредственный носитель информации попадает в руки третьих лиц. Это позволяет не допускать утечки и в тех случаях, когда инсайдер или не имеющий легального доступа к данным человек получает доступ к непосредственному носителю информации.

Дополнительные задачи систем класса IPC

- предотвращение передачи вовне не только конфиденциальной, но и другой нежелательной информации (обидных выражений, спама, эротики, излишних объёмов данных и т.п.);
- предотвращение передачи нежелательной информации не только изнутри наружу, но и снаружи внутрь информационной системы организации;
- предотвращение использования работниками Интернет-ресурсов и ресурсов сети в личных целях;
- защита от спама;
- защита от вирусов;
- оптимизация загрузки каналов, уменьшения нецелевого трафика;
- учет рабочего времени и присутствия на рабочем месте;
- отслеживание благонадёжности сотрудников, их политических взглядов, убеждений, сбор компромата;
- архивирование информации на случай случайного удаления или порчи оригинала;
- защита от случайного или намеренного нарушения внутренних нормативов;
- обеспечение соответствия стандартов в области информационной безопасности и действующего Законодательства.

Седлецький Денис Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ЗАХИСТ КОРПОРАТИВНОЇ МЕРЕЖІ

Кожна організація турбується про безпеку своєї інформації, оскільки її розголошення може нанести збитки, як фінансові, так і репутаційні, привести до небажаних наслідків. Найслабшою ланкою в забезпеченні інформаційної безпеки є людина, яка може виступати джерелом і цілеспрямованих, і випадкових загроз. Отже, забезпечення безпеки внутрішньої корпоративної мережі є вкрай важливим аспектом побудови захищеної інфраструктури.

Впродовж останніх кількох років у технічних новинах все більше переважають статті про витоки даних, проблеми інформаційної безпеки, різноманітні вразливості. У минулому році було виявлено досить критичні вразливості: вразливість KRACK, знайдена в протоколі

безпеки WPA2, що впливає на більшість сучасних маршрутизаторів Wi-Fi; Meltdown і Spectre, до яких вразливі майже всі сучасні процесори, і, звичайно, різні витоки даних, які впливають навіть на величезні компанії. Пропоную кілька порад, що допоможуть забезпечити безпеку офісної корпоративної мережі.

1. Створення посібнику «BYOD»

BYOD (**B**ring **Y**our **O**wn **D**evice, укр. принеси свій власний пристрій) – організаційна політика, що передбачає використання персональних пристроїв для роботи в корпоративній мережі. Впроваджується з метою заощадження коштів на дорогих апаратних засобах та наданні свободи працівникам, які часто працюють поза офісом або вдома.

Проте така політика може призвести до великої кількості проблем безпеки. Використання ноутбука у особистих цілях та для роботи може призвести до появи вірусів у офісній мережі. Це також означає повну довіру до знань співробітників у сфері кібербезпеки.

Для вирішення цих питань, необхідно створити посібник «BYOD», в якому вказати, що можна робити, а що ні. Переконайтеся, що визначено хоча б основні функції безпеки, які повинні використовуватись на підключених до Інтернету пристроях, такі, як VPN та антивірус.

2. Використання брандмауеру та обмеження доступу

Більшість підприємств мають корпоративний брандмауер і обмежують доступ працівників, визначаючи, які конкретні комп'ютери та веб-сайти можуть бути пропущені через брандмауер. Це є важливим кроком у забезпеченні безпеки офісної мережі. Більше того, деякі брандмауери оснащені вбудованим VPN, забезпечуючи ще більший захист за допомогою шифрування.

Підприємствам, які ще не використовують VPN, рекомендується встановити VPN в свою офісну мережу для використання в якості бар’єру безпеки між ПК та сервером. Завдяки такому підходу комп’ютер використовуватиме зашифрований тунель під час доступу до сервера. Існують безкоштовні варіанти, але великі підприємства повинні використовувати платний широкосмуговий VPN, щоб забезпечити оптимальний захист.

3. Щоденне оновлення антивірусу

Як і більшість речей в житті, регулярне обслуговування є вкрай важливим для того, щоб тримати все в порядку. Щоденне антивірусне оновлення призведе до зниження ризику спаду рівня вашої захищеності, включаючи навіть такі аспекти, як відключення автоматичних оновлень і виникнення нових загроз, які не охоплюються вашим поточним захистом.

4. Обмеження доступу до сервера

Сервери можуть бути розподілені і виконувати окремі функції для кожного відділу у організації, тому кожен комп'ютер і обліковий запис кожного співробітника повинні мати доступ лише до відповідних частин сервера.

Також необхідно вчасно відключати облікові записи колишніх співробітників, щоб обмежити шанс хакерів отримати несанкціонований доступ через неактивний обліковий запис, або захиститись від потенційного зловмисника в особі колишнього працівника, який здійснює зловмисну діяльність в офісній мережі.

5. Впровадження «білих списків»

Хоча підприємства можуть обмежувати доступ до певних файлів на сервері, вони також повинні розглянути можливість заборони доступу для зовнішніх непідтверджених пристроїв: ноутбуків, планшетів та ін.

Це означатиме, що працівники зможуть переглядати інформацію на сервері зі свого офісного ПК, але якщо вони використовуватимуть інший пристрій, він отримає доступ лише до гостьового Wi-Fi і не матиме абсолютно ніякого доступу до сервера, якщо він не затверджений офісним менеджером або IT-адміністратором. Це ще один крок до захисту даних, збережених на офісному сервері.

6. Блокування сайтів

Обмеження використання працівниками Інтернету може не тільки захистити офісну мережу від вірусів та шкідливого вмісту, розміщеного на деяких веб-сайтах, а і допомогти підвищити швидкість доступу в Інтернет.

Існує багато способів блокувати потенційно шкідливі веб-сайти, але найпоширенішим є використання можливостей маршрутизатора, блокування окремих IP-адрес, створення фільтрів брандмауера. Кожен брандмауер має власні налаштування, але більшість веб-сайтів можуть бути заблоковані за допомогою фільтрації.

Джерела:
IT-ресурс «Computerworld UK». URL: https://computerworlduk.com/
IT-ресурс «Cisco». URL: https://www.cisco.com/

Чорний Валерій Анатолійович
Державний Університет Телекомунікацій
Навчально-науковий інститут захисту інформації
м.Київ

СУЧАСНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Засоби захисту інформації - це сукупність інженерно-технічних, електричних, електронних, оптичних та інших пристроїв і пристосувань, приладів і технічних систем, а також інших речових елементів, які використовуються для вирішення різних завдань із захисту інформації, в тому числі попередження витоку і забезпечення безпеки захищеності інформації.

Загальна комп'ютеризація і новий розвиток інформаційних технологій призвели до того, що інформаційна безпека стає обов’язковою. Дії, які можуть призвести до спотворення, несанкціонованому використанню або навіть руйнації інформаційних ресурсів керованої системи розуміються, як загроза безпеки інформації. Для цього вченні розробили багато засобів захисту інформації.

У своїх протиправних діях, зловмисники намагаються знайти джерела конфіденційної комп'ютерної інформації, які давали б їм найбільш достовірну інформацію в великих обсягах з мінімальними витратами його одержання. За допомогою багатьох прийомів, різноманітних фокусів і коштів підбираються шляхи й підходи до таких джерел. Під джерелом інформації мається на увазі матеріальний об'єкт, у якого є певні дані, котрі представляють конкретний інтерес для зловмисників чи конкурентів.

На сьогоднішній день комп’ютерні генії розробили нову сучасну технологію — технологію захисту в комп'ютерних інформаційних системах й у мережах її передачі. Для реалізація цієї технології здійснюється потреба в збільшенні витрат і зусиль. Однак це дозволяє уникнути значних втрат і шкоди, які можуть виникнути при реальному здійсненні загроз.

Засоби для створення інформаційної безпеки:

Системний підхід базується на побудові системи захисту, що означає оптимальне поєднання взаємозалежних організаційних програмних,. апаратних, фізичних та інших властивостей.

Принцип сталого розвитку системи - це безперервний процес, що полягає в обґрунтуванні та реалізації найбільш раціональних методів, засобів і шляхів вдосконалення захисту, безупинному контролі, виявленні її вузьких і слабких місць, потенційних каналів витікання інформації та нових засобів несанкціонованого доступу.

Поділ і мінімізація повноважень із доступу до оброблюваної інформації та процедурам обробки, т. е. надання як користувачам, і самим працівникам ІВ, мінімуму суворо визначених повноважень, достатніх до виконання ними своїх службовими обов'язками.

Повнота контролю та реєстрації спроб несанкціонованого доступу, т. е. необхідність точного встановлення ідентичності кожного користувача і протоколювання його дії щодо можливого розслідування, і навіть неможливість скоєння будь-який операції обробки інформацією ІТ без її попередньої реєстрації.

Забезпечення надійності системи захисту, т. е. неможливість зниження рівня надійності у разі виникнення у системі збоїв, відмов, навмисних дій зловмисника чи випадкових помилок користувачів та обслугованого персоналу.

Забезпечення контролю над функціюванням системи захисту, тобто створення засобів і методів контролю працездатності механізмів захисту.

Забезпечення різноманітних коштів боротьби з шкідливими програмами. Забезпечення економічної доцільності використання системи захисту, виражену в перевищенні можливої шкоди ІС та ІТ від загроз над вартістю розробки та експлуатації системи захисту інформації.

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об’єднати у такі групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зазначимо, що такий поділ є досить умовним. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту.

Як показує практика, збиток від вчинення аналізованих злочинів у багато разів перевищує вартість технічних та організаційних заходів щодо здійснення профілактики злочинів у сфері ІТ. У зв'язку з цим відмова від прийняття організаційних заходів із захисту інформації з мотивів високої собівартості, є недоцільним

Основні засоби захисту інформації:

Перешкода — засіб фізичного перекриття шляху «комп'ютерному пірату» до певної інформації.

Протидія атакам шкідливих програм - це комплекс різноманітних заходів організаційного характеру і антивірусних програм.

Примус — метод захисту, у якому користувачі і персонал ІВ змушені дотримуватися правил обробки, передачі й використання захистимої інформації під загрозою матеріальної, адміністративної чи кримінальної відповідальності.

Механізми шифрування — криптографічне закриття інформації. Ці засоби захисту широко застосовуються як і в обробці, так і при зберіганні інформації на магнітних носіях.

Пробудження — метод захисту, який спонукує користувачів і персонал ІВ не порушувати встановлені порядки з допомогою дотримання сформованих моральних і етичних норм.

Регламентація — створення умов автоматизованої обробки, збереження і передачі захистимої інформації, у яких норми і стандарти захисту виконуються найбільше.

Що до автоматизованих банківських систем, то вони використовують криптографічні методи захисту інформації і реалізуються у вигляді апаратних, програмних чи програмно-апаратних методів захисту. Використовуючи шифрування повідомлень в поєднанні з правильною установкою комунікаційних засобів, належними процедурами ідентифікації користувача, можна добитися високого рівня захисту інформаційного обміну.

Криптографія є одним з найкращих засобів забезпечення конфіденційності і контролю цілісності інформації. Вона займає центральне місце серед програмно-технічних регулювальників безпеки, є основою реалізації багатьох з них і, в той же час, останнім захисним рубіжем.

ВИСНОВОК

Таким чином, як показує статистика, у всіх країнах світу від зловмисних дій втрати безупинно зростають. Причому головні причини збитків пов'язані й не так з недостатністю коштів безпеки як, як із відсутністю взаємозв'язку з-поміж них, тобто, з нереалізованістю підходу. Тому необхідно випереджальними темпами удосконалювати комплексні засоби захисту безпеки інформації. Слід підкреслити, що деякі фахівці з банківської безпеки пов'язують надійність фінансових інформаційних систем з засобами їх зовнішнього захисту, тобто системою паролів для входу не тільки у саму комп'ютерну мережу, а й до різних рівнів інформації системи, залежно від допуску користувачів. Потрібно знайти принципово нові підходи для розробки та впровадження відносно надійних систем захисту банківської діяльності від комп 'ютерних злочинів. Така система повинна будуватися згідно із технологією банківського документообігу та особливостями форм розрахунково-кредитних операцій.

Список використовуваної літератури:

1. *http://mdu.in.ua/Nauch/Konf/2017/zbirnik_kiberbezpeka.pdf*
2. *http://ua-referat.com/Засоби_захисту_інформації*
3. *http://allref.com.ua/uk/skachaty/Zasobi_zahistu_informaciy*

Місевіч Катерина Сергіївна
Державний Університет Телекомунікацій
Навчально-науковий інститут захисту інформації
м.Київ

ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И IOT

Более пяти лет подряд мы говорим о проблемах безопасности мобильных сетей, в частности – об уязвимостях SS7. Сейчас большинство операторов использует сети LTE, где на смену стеку протоколов SS7 пришел иной протокол — Diameter. Помимо традиционных угроз в последнее время в обществе активно обсуждается тема развития «умных городов». Необходимо отметить, что жизненно важные системы для таких городов — светофоры, дороги, коммунальные услуги - будут управляться через мобильные сети LTE, это следующий этап развития мобильных сетей LTE — LTE-M, 5G. Однако атаки через уязвимости мобильных сетей

могут полностью парализовать работу «умного города». Самоуправляемые автомобили также находятся под угрозой. С помощью мобильных сетей автомобили обмениваются данными о скорости, расположении автомобилей на трассе и пр. DDoS-атаки могут оставить такой автомобиль буквально без «чувств и глаз». А также множество других проблем остаются актальными в сфере телекоммуникаций.

Телекоммуникационные сети и IoT

Более пяти лет подряд мы говорим о проблемах безопасности мобильных сетей, в частности – об уязвимостях SS7. Нас часто спрашивают, когда же телекоммуникационные компании научатся защищать этот протокол или, наконец, заменят его на более безопасный? Выбором средств защиты обеспокоены как зарубежные, так и российские операторы. Кроме того, сейчас большинство операторов использует сети LTE, где на смену стеку протоколов SS7 пришел иной протокол — Diameter. Согласно статистике аналитического агентства Ovum, по итогам второго квартала 2017 года в мире осуществляется больше подключений к сетям LTE, нежели к сетям 3G. Приведем цифры, актуальные для второго квартала 2017 года:

- 2,36 млрд — число пользователей LTE по всему миру.
- 878 млн — число LTE-подключений за последние 12 месяцев.
- 59% — рост количества LTE-абонентов за год.
- 30% — доля LTE-абонентов от общего числа подключений.

Blackbox атака ― одна из самых распространенных jackpotting-атак направленная на прямую выдачу наличных средств из SDC/USB и RS232 диспенсеров путем подключения внешнего контроллера к шине передачи данных. В настоящий момент, данный вид атаки повсеместно используется на все территории РФ и Европы и является прямой угрозой финансовой безопасности банков так как зачастую потери не покрываются страховкой. Каждая исследованная сеть 4G на базе Diameter обладала аналогичными с устаревшим протоколом SS7 уязвимостями. Используя их, злоумышленник может вести слежку за абонентом, перехватывать SMS-сообщения в целях взлома аккаунтов онлайн-банка, социальных сетей и т.п.

Помимо традиционных угроз в последнее время в обществе активно обсуждается тема развития «умных городов». Необходимо отметить, что жизненно важные системы для таких городов — светофоры, дороги, коммунальные услуги - будут управляться через мобильные сети LTE, это следующий этап развития мобильных сетей LTE ― LTE-M, 5G. Однако атаки через уязвимости мобильных сетей могут полностью парализовать работу «умного города». Уязвимые мобильные сети связывают миллионы «умных» устройств, которые рано или поздно могут «сойти с ума». По данным экспертов, к 2020 году число IoTустройств, подключенных к сотовым сетям, увеличится с 400 млн до 1,5 млрд. Бурное проникновение «умных» устройств в бизнес и повседневную жизнь — еще один повод задуматься о безопасности мобильных сетей. IoT-устройства проникают не только в наш дом, но и в производство, добывающую промышленность и энергетику. Человек принимает минимальное участие в их работе: машины общаются с друг другом, принимая решения без его участия. В таком случае компрометация даже одного «умного датчика» может привести к непредсказуемым последствиям. Наши исследования показывают, что мир Интернета вещей имеет разную степень защищенности: от надежно защищенных устройств до откровенно «дырявых», с помощью которых злоумышленник может наблюдать, что происходит у вас дома. Результат аудитов «умных домов» показывает, что самым уязвимым устройством является видеокамера: злоумышленник может получить к ней полный доступ и использовать для слежки, проникновения в сеть, подмены видеопотока.

Самоуправляемые автомобили также находятся под угрозой. С помощью мобильных сетей автомобили обмениваются данными о скорости, расположении автомобилей на трассе и пр. DDoS-атаки могут оставить такой автомобиль буквально без «чувств и глаз». Машины не смогут обновлять информацию о дорожной ситуации. Таким образом,

уязвимости мобильных сетей могут стоить не только больших денег, но и человеческих жизней. Если сейчас пользователи могут повлиять на безопасность устройства, правильно настроив роутер и доступ к устройству извне, то в случае использования мобильных операторов все будет полностью зависеть от защищенности мобильных сетей, которая как мы знаем, сейчас оставляет желать лучшего.

Если ситуация с безопасностью мобильных сетей и IoT-устройств не изменится, первыми под удар попадут те сервисы или службы, для которых отказ в обслуживании будет наиболее чувствительным: в качестве примера можно назвать умные светофоры, подключенные к мобильным сетям, уязвимости которых могут в конечном счете стать причиной транспортного коллапса или аварии.

Источниики:

1. *IT-ресурс «Computerworld UK». URL: http://computerworlduk.com/*
2. *IT-ресурс https://www.ptsecurity.com/*

Прокопенко Владислав Олександрович
Державний Університет Телекомунікацій
Навчально-науковий інститут захисту інформації
м.Київ

ОСНОВИ ПОБУДОВИ КОМП'ЮТЕРНИХ МЕРЕЖ

Персональні комп'ютери з моменту свого виникнення сприймалися і використовувалися виключно як індивідуальний обчислювальний комплекс, здатний вирішувати величезне коло завдань автономно, без взаємодії з іншими обчислювальними ресурсами. Такий стан справ цілком задовольняв величезну масу користувачів доти, поки зростання кількісних показників потужності і продуктивність персональних обчислювальних комплексів не переросло в якісну зміну рівня складності завдань, що вирішуються за допомогою персональних комп'ютерів.

Сукупність кабельних систем, електронного обладнання і спеціалізованого програмного забезпечення складають поняття мережних інформаційних технологій. Дані технології можна умовно поділити на такі основні групи:

середовище передачі інформації – спеціалізована апаратура, необхідна для підключення персонального комп'ютера до мережі;

протоколи передачі інформації – системне програмне забезпечення, що організовує на основі передавального середовища безпосередню передачу деяких даних між об'єднаними в мережу комп'ютерами;

мережні послуги – системне і прикладне програмне забезпечення, що надає користувачеві засоби організації зручної та ефективної роботи у складі комп'ютерної мережі;

Тільки при чіткій взаємодії цих компонентів, як єдиного програмно-технічного комплексу можна говорити про наявність і функціонування обчислювальної мережі, назалежно від її масштабу і функціонального призначення.

Топологія комп'ютерних мереж

Топологія мережі характеризує властивості мереж, які не залежать від їх розмірів, відображає структуру, утворену вузлами мережі і безліччю зв'язуючих їх каналів. При цьому не враховується продуктивність і принцип роботи цих вузлів, їх типи і довжина каналів.

З погляду фізичного розташування функціональних компонентів мережі (кабелів, робочих станцій і т.д.) і методу доступу до середовища передачі можна виділити чотири базові топології: "загальна шина", "зірка", "кільце" і "чарункова (стільникова)" .

Топологія реальної мережі може повторювати одну з наведених вище або включати їх комбінацію.

Список використаної літератури

1. http://westudents.com.ua/glavy16035--1-zagaln-printsipi-pobudovi-kompyuternih-merej.html
2. *http://stud.com.ua/50138/informatikaprintsipi_pobudovi_lokalnih_merezh_osnovni_komponenti_priznachennya_funktsiyi*

Хоменко Тетяна Анатоліївна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

МІЖНАРОДНІ ЗАХОДИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Генеральний Секретаріат Інтерполу у 1994 році рекомендував всім країнам - членам організації створити національні центральні консультативні пункти з проблем комп'ютерної злочинності (National central reference point) та закріпити конкретних працівників для роботи з інформацією про комп'ютерні злочини для оперативного обміну такою інформацією між країнами.

Ці пункти створено, як правило, в апаратах Національних Бюро Інтерполу, або у спеціалізованих підрозділах, які ведуть боротьбу з комп'ютерною злочинністю, або у підрозділах боротьби зі злочинами у сфері економіки.

В окремих країнах створені у системі правоохоронних органів спеціальні підрозділи по боротьбі з кіберзлочинністю.

На міждержавному рівні створено Міжнародну комісію по боротьбі з відмиванням грошей (ФАТФ) та групу розробки фінансових заходів боротьби з відмиванням грошей (ГФМ). Нині до цих структур входять представники 29 країн і двох міжнародних організацій (Європейської Комісії та Ради по співробітництву країн Персидської затоки). Значна увага в діяльності цих міжнародних структур приділяється організації боротьби з відмиванням грошей за допомогою транснаціональних комп'ютерних систем телекомунікації.

Значним здобутком роботи ФАТФ є розробка 40 рекомендацій по боротьбі з відмиванням грошей.

На міждержавному рівні проводиться робота для прийняття Міжнародної конвенції щодо попередження кіберзлочинів.

На базі НЦБ Інтерполу в Україні 17 вересня 1996 року був створений національний консультативний пункт щодо боротьби з кіберзлочинністю . Це дало можливість:

- накопичити матеріал про законодавче регулювання боротьби з комп'ютерною злочинністю у різних країнах;
- узагальнити досвід організації попередження, розкриття і розслідування комп'ютерних злочинів;
- підготувати низку аналітичних оглядів і публікацій з цих питань; ознайомити працівників МВС, прокуратури, суду з цим новим для України видом злочинів;
- внести конкретні пропозиції щодо удосконалення кримінального законодавства України.

Література:

1. http://polka-knig.com.ua

Стефурак Олег Романович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ОСНОВНІ ПРИНЦИПИ ЗАХИСТУ ІНФОРМАЦІЇ

Нині інформаційна безпека відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів країни. Це, в першу чергу, обумовлено швидким розвитком сучасних інформаційно-телекомунікаційних технологій, засобів зв'язку й інформатизації і, як наслідок, — істотним зростанням впливу інформаційної сфери на життя нашого суспільства. Інформаційна безпека відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів країни.

Захист інформації від НСД є складовою частиною загальної проблеми забезпечення захисту інформації в ІТКС. В загальному випадку комплекс програмно-технічних засобів та організаційних рішень по захисту інформації в ІТКС реалізується в рамках системи захисту інформації від НСД, яка умовно складається з таких чотирьох підсистем:

– управління доступом до ІТКС, до її послуг та ресурсів;

– реєстрація і облік користувачів, послуг, інформаційних ресурсів;

– криптографічного захисту;

– забезпечення цілісності інформаційних потоків, інформаційних ресурсів та програмного забезпечення.

Закриття каналів несанкціонованого отримання інформації повинно починатися з контролю доступу користувачів до ресурсів ІТКС. Ця задача вирішується на основі ряду принципів:

Принцип виправданості доступу – користувач повинен мати достатню «форму допуску» для отримання інформації того рівня конфіденційності, що він вимагає, і ця інформація дійсно необхідна йому для виконання його виробничих функцій.

Принцип достатньої глибини контролю доступу. Засоби захисту інформації повинні включати механізми контролю доступу до всіх видів інформаційних і програмних ресурсів ІТКС, які у відповідності з принципом виправданості доступу слід розмежовувати між користувачами.

Принцип розмежування інформаційних потоків. Для попередження порушення інформаційної безпеки, яке, наприклад, може мати місце при запису секретної інформації на несекретні носії і в несекретні файли, її передачі програмам і процесам, які не призначені для обробки секретної інформації, а також при передачі секретної інформації по незахищених каналах зв'язку, необхідно здійснювати відповідне розмежування інформаційних потоків.

Принцип персональної відповідальності. Кожний користувач повинен нести персональну відповідальність за свою діяльність в системі, включаючи будь-які операції з конфіденційною інформацією і можливі порушення її захисту.

Принцип цілісності засобів захисту. Даний принцип передбачає, що засоби захисту інформації в ІКСМ повинні чітко виконувати свої функції у відповідності з переліченими принципами і бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів контролю, сигналізації про спроби порушення захисту інформації і впливу на процеси в системі.

Реалізація перелічених принципів здійснюється з допомогою так званого «монітору звернень», який контролює будь-які запити до даних чи програм з боку користувачів (чи їх програм) за установленими для них видами доступу до цих даних і програм.

Практичне створення монітору звернень передбачає розробку конкретних правил розмежування доступу у вигляді так званої моделі захисту інформації.

Найбільш розповсюджена модель отримала назву – багаторівнева модель захисту Белла Ла Падула. Основою цієї моделі є поняття рівня конфіденційності (форми допуску) і категорії (прикладної області) суб'єкта і об'єкта доступу. На основі присвоєних кожному суб'єкту і об'єкту доступу конкретних рівнів і категорій в моделі визначаються їх рівні безпеки, а потім встановлюється їх взаємодія. При цьому в моделі приймається, що один рівень безпеки домінує над іншим тоді і тільки тоді, коли відповідний йому рівень

конфіденційності більше чи дорівнює конфіденційності іншого, а множина категорій включає множину категорій другого.

Розмежування і контроль доступу до інформації

Розмежування доступу в ІТКС полягає в розділенні інформації на частини і організації доступу до неї користувачів відповідно до їх функціональних обов'язків і повноважень.

Задача такого розмежування доступу до інформації: скорочення кількості користувачів, що не мають до неї відношення при виконанні своїх функцій, тобто захист інформації від порушника серед законних користувачів. Розмежування доступу користувачів ІТКС може здійснюватися за такими параметрами:

– виглядом, характером, призначенням, ступенем важливості і секретності інформації;

– способами її обробки: обчислення, запис, внесення змін, виконання команди;

– умовним номером терміналу; часом обробки й ін.

При проектуванні ІТКС на її базі проводяться:

– розробка і реалізація функціональних задач по розмежуванню і контролю доступу до апаратури і інформації як в рамках інформаційної системи в цілому, так і до відокремлених інформаційних ресурсів;

– розробка апаратних засобів ідентифікації та аутентифікації користувачів та ресурсів системи;

– розробка програмних засобів контролю і управління розмежуванням доступу;

– розробка окремої експлуатаційної документації на засоби ідентифікації, аутентифікації, розмежування і контролю доступу.

Комплексна система захисту інформації

Комплексна система захисту інформації – це сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку й несанкціонованого доступу.

Головною метою створення КСЗІ є досягнення максимальної ефективності захисту за рахунок одночасного використання всіх необхідних ресурсів, методів і засобів, що виключають несанкціонований доступ до інформації, та створення умов обробки інформації відповідно до чинних нормативно-правових актів України у галузі захисту інформації: Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації» та «Про захист персональних даних».

Відповідно до ст.4 постанови Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» захисту підлягає інформація, вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу.

Для кожної конкретної інформаційно-телекомунікаційної системи склад, структура та вимоги до КСЗІ визначаються властивостями та актуальними загрозами безпеки оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС відповідно до нормативних документів з захисту інформації.

Комплексна система захисту інформації складається з організаційних та інженерно-технічних заходів. Зміст організаційних заходів полягає у розробці посадових інструкцій для користувачів та обслуговуючого персоналу, створенні правил адміністрування інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів, розробці планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації, навчанні правилам інформаційної безпеки користувачів тощо.

Щодо інженерно-технічних заходів, то це сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захищеності інформації, який необхідно забезпечити.

Суб'єктами комплексної системи захисту інформації є організація, для якої здійснюється побудова КСЗІ (Замовник), організація, що здійснює заходи з побудови КСЗІ (Виконавець), Адміністрація Державної служби спеціального зв'язку та захисту інформації України (Адміністрація Держспецзв'язку) (Контролюючий орган), організація, що здійснює державну експертизу КСЗІ (Організатор експертизи), організація, що, у разі необхідності, залучається Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядник).

Об'єктом захисту КСЗІ є інформація в будь-якому її вигляді і формі подання.

Впровадження комплексної системи захисту інформації складається з кількох етапів: підготовки організаційно-розпорядчої документації, обстеження інформаційної інфраструктури Замовника, розробки "Технічного завдання на створення КСЗІ", розробки "Плану захисту інформації", розробки "Технічного проекту на створення КСЗІ", приведення інформаційної інфраструктури Замовника у відповідність до "Технічного проекту на створення КСЗІ", розробки "Експлуатаційної документації на КСЗІ", впровадження КСЗІ, випробування КСЗІ, проведення державної експертизи КСЗІ і отримання "Атестата відповідності", а також підтримки й обслуговування КСЗІ.

Використана література:

1. http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive-zavdannya-sogodennya/
2. http://lib.detut.edu.ua/files/Nauk_trud_vukladahiv/Fakultet%20Infrastruktur_ruxomuy_sklad%20"/Kafedra_tel_texn_avtomatuka

Загиней Антон Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

МОДЕЛЬ ЦИФРОВОГО ВУЗЛА КОМУТАЦІЇ З ПОЗИЦІЙ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Розглянута модель безпеки ЦАТС (цифрової автоматизованої телекомунікаційної системи), визначенні завдання які повинна виконувати комплексна система інформаційної безпеки. Окресленні основні способи взаємодії порушника з ЦАТС.

Для надання послуг якісного, надійного, безпечного телефонного зв'язку має бути сформована надійна захищена інфраструктура ЦАТС та ліній телекомунікацій з використанням доступних та ефективних засобів і способів інформаційного захисту. Розрізнені заходи щодо інформаційної безпеки, які приймаються при забезпеченні якості послуг, ефективності технічної експлуатації та управління ЦАТС необхідно привести у єдину керовану комплексну систему інформаційної безпеки, яка має забезпечити:

- стійке функціонування ЦАТС та мережі телекомунікацій;
- попередження загроз їхній безпеці;
- захист законних інтересів підприємства від протиправних посягань;
- недопущення крадіжки фінансових засобів, розголошення, утрати, спотворення й знищення службової, технологічної, управлінської інформації;
- ефективну виробничу діяльність усіх підрозділів;
- підвищення якості наданих послуг та гарантії безпеки майнових прав та інтересів абонентів.

Що стосується конфіденційності інформації, яка є державним інформаційним ресурсом, під час передавання мережею забезпечує власник автоматизованої системи або оператор мережі передачі даних за договором із власником автоматизованої системи. Заходи щодо технічного захисту конфіденційної інформації, що не належить державі, та відкритої інформації, важливої для особи та суспільства, якщо остання циркулює поза межами державних органів, підприємств, установ і організацій, встановлюються власником інформації або розпорядником.

Обладнання ЦАТС поділяють на станційну частину, блоки абонентських виносів (БАВ) і мережу абонентських, з'єднувальних та міжстанційних цифрових та аналогових ліній, які є для порушника об'єктами несанкціонованого доступу до них, до інформації, що ними передається, і впливу на їх працездатність. На лініях може бути обладнання, встановлене порушником (ОВП).

Станційна частина виконує функції опорної станції або опорно-транзитної станції і з'єднана з іншими станціями міжстанційними з'єднувальними, а з блоками абонентського виносу – з'єднувальними цифровими лініями Е1 з потрібним числом підсилювальних та регенеративних ділянок. БАВ приєднується до опорної станції, як правило, за інтерфейсом V3.1, V3.2.

На рисунку 1.1 зображена модель інфраструктури цифрового вузла комутації з позиції захисту інофрмації. Тут можна розглянути основні способи зловмисника

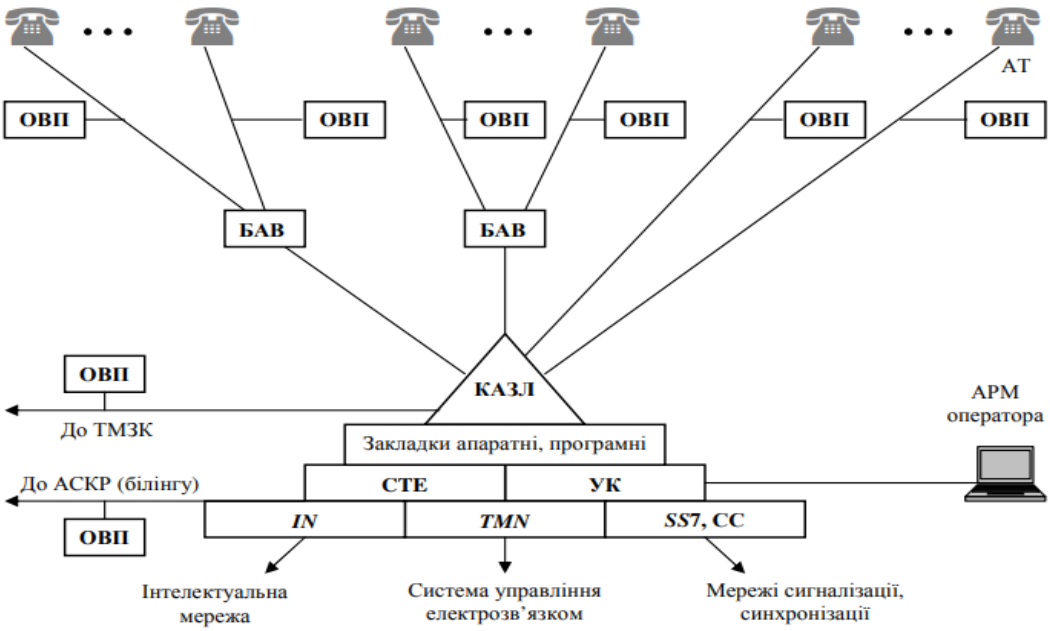


Рисунок 1.1 – Модель інфраструктури цифрового вузла комутації з позицій захисту інформації

Позначення: АРМ () – автоматизоване робоче місце; АСКР – автоматизована система комплексних розрахунків з абонентами; АТ – абонентські термінали; БАВ – блок абонентського виносу; КАЗЛ – підсистема комутації абонентських та з'єднувальних ліній; ОВП - обладнання, встановлене порушниками; СС – система синхронізації; СТЕ – система технічної експлуатації; ТМЗК – телекомунікаційна мережа загального користування; УК – управляючий комплекс; IN - інтелектуальна мережа; TMN - мережа управління телекомунікаціями; SS7 - система сигналізації № 7.

Структурна схема станційної частини програмно-керованої АТС з позицій ТЗІ наведена на рис. 1.2 [8].

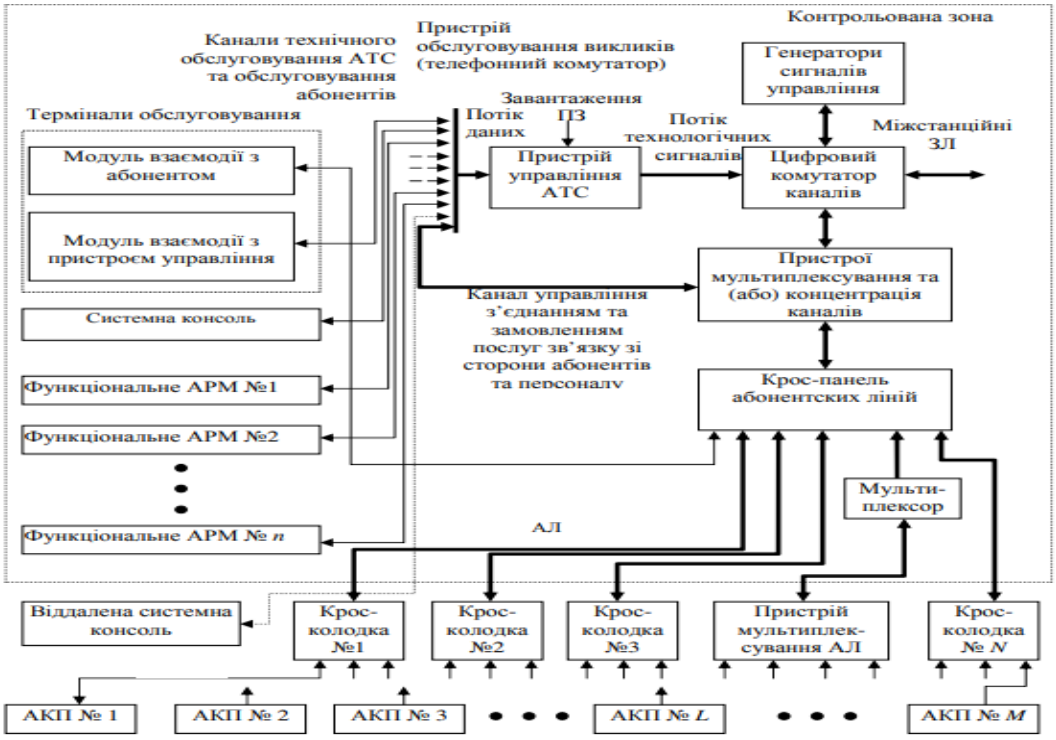


Рисунок 1.2 – Структурна схема станційної частини програмно-керованої АТС з позицій ТЗІ

Позначення: АКП – абонентські кінцеві прилади (апарати); АЛ – абонентські лінії; АРМ – автоматизоване робоче місце; АТС – автоматична телефонна станція; ЗЛ – з'єднувальні (міжстанційні) лінії; ПЗ – програмне забезпечення; L – поточне число АКП; M – загальна кількість АКП (ємність станції); N – кількість кросових колодок; n – кількість АРМ; контрольована зона – територія, де унеможливлюється присутність сторонніх осіб.

Станційне обладнання ЦАТС розміщується на охороняємому об'єкті, де проводиться повний цикл організаційно-технічних заходів з комплексної інформаційної безпеки певного атестованого рівня. Обладнання програмно - керованих АТС має захищеність базового рівня, яка забезпечується фірмою-виробником даного обладнання. При встановленні обладнання на мережу рівень захищеності знижується за рахунок можливого впливу на саму систему зі сторони мережі каналами абонентського доступу, сигналізації, синхронізації, тарифікації і системи управління з віддалених терміналів.

Також слід зазначити, що на виходах підсистеми управління утворюються в реальному часі потоки технологічних сигналів, за допомогою яких має місце процес управління підсистемою КАЗЛ. З іншого боку, абонентські прикінцеві пристрої мають можливість обмінюватися керуючою інформацією з підсистемою управління станцією через канали управління з'єднаннями й замовлення послуг.

Коректність такої декомпозиції структури програмно-керованих АТС обумовлена прийнятими щодо них проектними рішеннями, що не передбачають: - можливостей штатних впливів на підсистему управління станцією з боку абонентських прикінцевих пристроїв, за винятком можливості запуску абонентом задач із фіксованого набору, що реалізують заздалегідь передбачені функції замовлення абонентом додаткових видів послуг, які надаються станцією; - можливостей штатних впливів на інформацію в розмовних трактах із боку підсистеми управління станцією, за винятком можливості штатних приєднань 20 до вже встановлених з'єднань (наприклад, із боку телефонного комутатора або абонентських прикінцевих пристроїв у режимі конференц зв'язків), однак з обов'язковим оповіщенням учасників розмови про всі додаткові підключення до їхніх розмовних трактів (зокрема, фоновими тональними сигналами).

Список використаної літератури

1. *Забезпечення інформаційної безпеки цифрових програмно керованих АТС Інформаційна безпека телефонного зв'язку: навч. посібник / [Кононович В.Г., Стайкуца С.В., Тардаскіна Т.М., Шинкарчук Т.М.] За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2010. – С. 168.*
2. *НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id= 40371&cat_id=38835*

Батрак Іван Геннадійович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Нині інформаційна безпека відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів країни. Це, в першу чергу, обумовлено швидким розвитком сучасних інформаційно-телекомунікаційних технологій, засобів зв'язку й інформатизації і, як наслідок, — істотним зростанням впливу інформаційної сфери на життя нашого суспільства. Інформаційна безпека відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів країни.

Технічний захист інформації (*ТЗІ*) — діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.
Суб'єктами системи технічного захисту інформації є:

- Держспецзв'язку України;
- органи, щодо яких здійснюється ТЗІ;
- науково-дослідні та науково-виробничі установи Держспецзв'язку України, державні підприємства, що перебувають в управлінні Держспецзв'язку України та виконують завдання з питань технічного захисту інформації;
- військові частини, підприємства, установи та організації всіх
- форм власності й громадяни-підприємці, які провадять діяльність з
- технічного захисту інформації за відповідними дозволами або ліцензіями;
- навчальні заклади з підготовки, перепідготовки та підвищення
- кваліфікації фахівців з технічного захисту інформації

Технічні канали витоку інформації:

- візуально-оптичний;
- акустичний;
- електромагнітний;
- матеріальний.

Оптичний канал витоку інформації - візуальні методи, фотографування, відео зйомка, спостереження.

Акустичниі - Мембранне перенесення енергії мовних сигналів через перегородки за рахунок малої маси і слабкого згасання сигналів; витік через тріщини, отвори, щілини та інші акустичні отвори, тобто прямим розповсюдженням акустичних коливань.

Електромагнітні - побічні електромагнітні випромінювання (ПЕМІ), що виникають при роботі технічних засобі, а саме:

- побічні електромагнітні випромінювання, що виникають внаслідок протікання по елементах технічних засобів обробки інформації (ТЗОІ) і їх з'єднувальним лініях змінного електричного струму;

- побічні електромагнітні випромінювання на частотах роботи високочастотних генераторів, що входять до складу ТЗПІ;
- побічні електромагнітні випромінювання, що виникають внаслідок паразитної генерації в елементах ТЗОІ.

Електричні канали витоку інформації:

- наведення електромагнітних випромінювань ТЗПІ на з'єднувальні лінії ДТЗС і сторонні провідники, що виходять за межі контрольованої зони;
- просочування інформаційних сигналів у колі електроживлення ТЗПІ;
- просочування інформаційних сигналів у колі заземлення ТЗПІ.

Матріальні - вивчення відходів виробничої діяльності (зіпсовані документи або їх фрагменти, чернетки різного роду поміток, записів, листів і т. д.), викрадення, несанкціоноване ознайомлення, копіювання, фотографування, відеозапис документів, креслень, планів, зразків технічних або програмних засобів.

Захист інформації від її витоку технічними каналами зв'язку забезпечується наступними засобами й заходами:

- використанням екранованого кабелю й прокладкою проводів і кабелів в екранованих конструкціях;
- установкою на лініях зв'язку високочастотних фільтрів;
- побудовою екранованих приміщень ("капсул");
- використанням екранованого устаткування;
- установкою активних систем зашумлення.

Використана література:

1. https://tzi.com.ua/texnchnij-zaxist-nformacz.html
2. http://zakon3.rada.gov.ua/laws/show/1229/99
3. http://biblio.royalwebhosting.net/elektromagnitnyie-kanalyi-utechki-40520.html
4. http://studentam.net.ua/content/view/5490/132/

Семенова Інна Дмитрівна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ОБЩАЯ ХАРАКТЕРИСТИКА МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ И КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

В условиях форсированного формирования глобального информационного пространства и развития информационного общества, широкого использования инновационных технологий в телекоммуникационных системах и сетях, а так же при внедрении и реализации высокоуровневых информационных услуг особое значение приобретают проблемы информационной и кибернетической безопасности государства. Наиболее важными направлениями деятельности в этой отрасли являются: всесторонняя оценка угроз и опасностей, национальной уязвимости, идентификация критической инфраструктуры, как в рамках государства, так и в рамках отдельной инфо-систем

Деятельность по обеспечению информационной безопасности осуществляется с помощью различных способов, средств и приемов, которые в совокупности и составляют методы. Метод предполагает определенную последовательность действий на основании конкретного плана. Методы могут значительно меняться и варьироваться в зависимости от типа деятельности, в которой они используются, а также сферы применения.

1. Классификация методов анализа защищенности системы

Важными методами анализа состояния обеспечения информационной безопасности (ИБ) являются методы описания и классификации. Для осуществления эффективной

защиты той или иной системы следует описать, а только потом классифицировать различные виды угроз и опасностей, рисков и вызовов, и, соответственно, сформулировать систему мер по осуществлению управления ими.

В качестве распространенных методов анализа уровня защищенности используются методы исследования при действующих связях. С помощью данных методов обнаруживаются причинные связи между угрозами и опасностями; осуществляется поиск причин, которые стали источником и вызвали актуализацию тех или иных факторов опасности, а также разрабатываются меры по их нейтрализации. В числе методов причинных связей можно назвать следующие: метод сходства, метод различия, метод сообщения сходства и различия, метод сопутствующих изменений, метод остатков.

Выбор методов анализа состояния защищенности зависит от конкретного уровня и сферы организации защиты. В зависимости от угрозы становится возможным решение задачи по дифференциации, как различных уровней угроз, так и различных уровней защиты. Что касается сферы ИБ, то в ней обычно выделяют семь уровней. Физический (организация и физическая защита), программно-технический (управление доступом, аудит, криптография), управленческий (координация и контроль организационных, технологических и технических мероприятий), технологический (реализация политики информационной безопасности (ПИБ)), пользовательский (реализация ПИБ направлена на уменьшение рефлексивного воздействия на объекты ИБ, предотвращения информационного воздействия со стороны социальной среды), сетевой (политика реализуется в формате координации действий компонентов системы управления) и процедурный (принятие мер реализующихся людьми: управление персоналом, поддержание работоспособности и т.д.).

2. Классификация методов обеспечения информационной безопасности

- Одноуровневые методы строятся на основании одного принципа управления информационной безопасностью;
- Многоуровневые методы строятся на основании нескольких, каждый из которых служит решением собственной задачи, при этом частные технологии не связаны между собой и направлены только на конкретные факторы информационных угроз;
- Комплексные методы - многоуровневые технологии, объединены в единую систему координирующими функциями на организационном уровне с целью обеспечения ИБ, исходя из анализа совокупности факторов опасности, которые имеют семантическую связь или генерируются из единого информационного пространства;
- Интегрированные высокоинтеллектуальные методы - многоуровневые, многокомпонентные технологии, построены на основании мощных автоматизированных интеллектуальных средств с организационным управлением.

Общие методы обеспечение информационной безопасности активно используются на любой стадии управления угрозами. К таким стадиям относятся: принятие решения по определению области и контекста информационной угрозы и состава участников процесса противодействия; принятия общей стратегии и схемы действий; управление инцидентами и т.д.

3. Методы обеспечения информационной безопасности

Специфика использующихся методов в значительной мере зависит от субъекта деятельности, объекта воздействия, а также преследуемых целей.

Весьма важным является *применение аналитических методов познания и исследования состояния общественного сознания* в сфере ИБ. Необходимо донести, что сейчас важным условием обеспечение ИБ является не столько секретность, конфиденциальность информации, сколько ее доступность, целостность и защищенность от различных угроз - система должна адекватно реагировать и гарантировать эффективную деятельность.

Одним из методов обеспечения ИБ является *метод развития*. Поскольку, угроза и опасность есть атрибутивными компонентами системы ИБ, то их реализация и неизбежные негативные последствия служат импульсом и руководством к совершенствованию системы и повышению уровня ее защищенности.

Основным методом анализа информационных рисков является количественный и качественный анализ, факторный анализ и др.; цель качественной оценки рисков - ранжировать информационные угрозы и опасности по разным критериям, система которых позволит сформировать эффективную систему воздействия на них.

Важным методом обеспечения ИБ является также *метод критических сценариев*. В указанных сценариях анализируются ситуации, когда воображаемый противник парализует систему управления и соответственно снижает способность поддерживать систему в пределах оптимальных параметров.

Также можно указать на *метод моделирования*, с помощью которого целесообразно обучать будущих специалистов в сфере информационной безопасности развивая практические навыки защиты систем путем моделирования форм информационных атак присущих информационной войне.

Среди методов обеспечение ИБ важную роль играет *метод дихотомии*: для противодействия угрозам информационной безопасности принимаются необходимые меры как в направлении предоставления определенного воздействия на источник угрозы, так и в направлении укрепления объекта безопасности. Соответственно, выделяют две предметные области противодействия: одна - совокупность источников угроз, а другая - совокупность мероприятий по обеспечению информационной безопасности объекта.

Защита информации не ограничивается техническими методами, для эффективного обеспечения ИБ важно разнообразие моделей и методов оценки угроз. Для успешного проектирования, реализации и поддержки защищенной системы важно понимать характер, природу, сущность и содержание угроз и опасностей; уметь своевременно идентифицировать их источники и находить средства противодействия; знать способы минимизации негативных последствий реализации угрозы; обладать навыками управления последствиями инцидентов для восстановления корректного функционирования системы, а так же для последующего развития и совершенствования, функциональных возможностей защиты системы.

Список использованных источников:

1. *Липкан В.А. Национальная безопасность Украины: учебное пособие. Киев: КНТ, 2009 – 576 стр.*
2. *Доктрина информационной безопасности Украины от 1.05.2014*
3. *Кавун С.В. Информационная безопасность. Учебное пособие. Харьков: ХНЕУ, 2008. – 352 стр.*

Кущ Владислав Романович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

У поданій роботі розглядаються аспекти організації і розвитку національної системи кіберзахисту. Визначено сфери безпеки, які можуть стати головними жертвами хакерських атак, пріоритетні напрямки стратегії захисту інформаційного простору. Ключові слова: захист інформації. кіберзахист, кіберзлочинність, національна безпека, інформаційний простір.

Високі темпи розвитку інформаційно-комунікаційних технологій актуалізують питання захисту відповідної інфраструктури, оскільки її пошкодження або руйнування може мати значні наслідки для безпеки країни.

До найбільш істотних особливостей злочинів і інформаційному просторі зазвичай відносять: особливу складність розкриття і розслідування, надзвичайно високу латентність,

прозорість національних кордонів для злочинців, високопрофесійний склад осіб, які вчиняють такі злочини, особливо великі розміри збитку.

У наш час у всьому світі налічується понад тридцяти тисяч сайтів, які орієнтовані на злом і навчання цим прийомам. За невеликі гроші будь-який підліток може дозволити собі таку книгу, яка навчить його елементарним методам атаки на інформаційні системи; виведення вашого комп'ютера з ладу; відключення його від інтернету (у випадку, якщо комп'ютер є сервером, що надає якийсь корисний інтернет-сервіс клієнтам, це може спричинити за собою репутаційні й фінансові втрати, якщо він не зможе надавати ці послуги); запуск на вашому комп'ютері шкідливої програми; крадіжка ваших даних; блокування ваших даних з метою здирництва; додавання вашого комп'ютера під шкідливий бот-нет. І це далеко не повний перелік цілей зловмисників.

В інтернеті існує величезна кількість організованих груп , які вчиняють злочини. Такі групи часто займаються «атаками» на сервера і банки, щоб заволодіти інформацією для продажу або подальшого шантажу. Так, влітку 2011 р, сотні комп'ютерів в державних органах, головним чином, в дипломатичних представництвах за кордоном були заражені вірусом, який дозволяв хакерам отримати контроль над комп'ютером і конфіденційними даними.

Фінансова сфера - один з найбільш привабливих секторів злочинності: розкрадання грошей шляхом розтрати або присвоєння, виготовлення підроблених грошових коштів, підробки пластикових карт, порушення права і так далі.

Хоча такі атаки залишаються можливою загрозою, але актуальності набувають проблеми пов'язані з інформаційною безпекою в стратегічно важливих секторах економіки - енергетиці та транспорті, які можуть стати головними жертвами кібератак.

Українські державні і приватні компанії стали все частіше страждати від кібератак. Відтак, у грудні 2015 р. хакери атакували шість енергокомпаній в Західній Україні, в результаті чого 225 тис. українців у 103 населених пунктах залишилися без електроенергії внаслідок її навмисного відключення.

Зловмисники використовували програму, яка виявилася ще більш могутньою, ніж відомий вірус BlackEnergy, вже застосовувалися раніше для кібератак на енергооб'єкти. Ймовірною метою хакерів було вивести з ладу кілька ланок енергетичних систем і створити «ефект доміно», щоб обвалити всю систему або принаймні значну її частину.

Атаки хакерів з використанням вірусу BlackEnergy також вразили такі стратегічні об'єкти: аеропорт «Бориспіль», «Укрзалізницю», телеканал СТБ (медіа-група Starligh Media). Експертне співтовариство пояснює, що такі загрози - глобальний тренд. Це зайвий раз підтверджує актуальність досліджуваної проблеми і необхідність серйозного підходу до її вирішення.

27 січня 2016 р. Президент П. Порошенко затвердив «Стратегію кібербезпеки України», а 7 червня 2016 р. - «Положення про Національний координаційний центр кібербезпеки». Згідно з документом, основу національної системи кібербезпеки складуть Міністерство оборони, Державна служба спеціального зв'язку та захисту інформації, СБУ, Національна поліція, НБУ, розвідувальні органи. Метою стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особистості, суспільства і держави.

В документі підкреслюється, що поряд з перевагами сучасного цифрового світу і розвитком інформаційних технологій, вони можуть використовуватися для вчинення терористичних актів, у тому числі шляхом порушення штатних режимів роботи автоматизованих систем управління технологічними процесами на об'єктах інфраструктури.

Більшого поширення одержує політично мотивована діяльність у кіберпросторі у вигляді атак на урядові і приватні сайти в мережі інтернет. 27 червня 2017 р. став «чорним вівторком» для кібербезпеки нашої країни. Протягом одного дня комп'ютерний вірус

«Ransom:Win32/Petya» атакував приватний і державний сектори економіки України, зокрема банки, аеропорти, державну залізничну компанію, телекомпанії, телекомунікаційні компанії, великі мережеві супермаркети, енергетичні компанії, державні фіскальні служби, органи державної влади та місцевого самоврядування тощо.

Вірусом було вражено також приватні та державні суб'єкти інших держав, але спеціалісти в цій галузі сходяться в тому, що найбільше постраждала Україна. Наша держава виявилася неспроможною протистояти такій атаці, яка, своєю чергою, виявила незахищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору та відсутність можливості своєчасного виявлення, запобігання і нейтралізації реальних та потенційних загроз національній безпеці у кіберпросторі.

10 жовтня 2017 р. Верховна Рада України прийняла, а 7 листопада Президент ухвалив «Закон України про основні засади забезпечення кібербезпеки України». Закон встановлює правила гри на полі кіберзахисту і містить дуже багато планів та намірів. Експерти загалом схвально відгукуються про його ухвалення - як базового документу, хоч у ньому й є ціла низка недопрацювань.

Водночас на думку аналітиків, ще зарано говорити про ефективність цього закону для підвищення рівня кібербезпеки. «Поки не будуть сформовані суб'єкти, які безпосередньо займатимуться оперативним реагуванням на кіберінциденти, поки в цих суб'єктів не буде належної технічної бази та висококваліфікованих спеціалістів, що в свою чергу потребує належного фінансування, - всі заявлені в законопроекті положення так і залишаться на папері», - переконаний Анатолій Грабовий. Його підтримує і Віктор Жора. «Тепер справа за урядом, суб'єктами забезпечення кібербезпеки, які мають розробити вимоги до захисту критичних інфраструктур, нові стандарти і методики та забезпечити контроль за ефективністю кіберзахисту», - зазначає експерт.

Таким чином, швидка інформатизація, масштаби потенційних наслідків злочинів у кіберпросторі вимагають серйозної уваги до розвитку національної системи кібербезпеки і підвищення ефективності роботи відповідних інституційних структур з урахуванням зарубіжного досвіду в цій сфері.

Використані джерела

1. Закон України про основні засади забезпечення кібербезпеки України (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) [Інтернет ресурс]. Режим доступу: http://zakon5.rada.gov.ua/laws/show/2163-19

2. Закон про кібербезпеку та стратегія кібербезпеки України /Анатолій Грабовий, адвокат, старший юрист, GOLAW[Інтернет ресурс]. Режим доступу: http://uz.ligazakon.ua/ua/magazine_article/EA010553

3.Пташко П.М. Кібербезпека в Україні: 2016 та прогнози на майбутнє [Інтернет ресурс]. Режим доступу: https://core.ac.uk/download/pdf/84825455.pdf

4.Указ Президента України № 242/2016 Про Національний координаційний центр кібербезпеки [Інтернет ресурс]. Режим доступу: http://www.rnbo.gov.ua/documents/425.html

Хапун Анастасія Валеріївна
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

BEST PRACTICES FOR BUILDING A SECURITY OPERATIONS CENTER

If one cannot effectively manage the growing volume of security events flooding the enterprise, one cannot secure one's business. Yet IT security teams are now being overwhelmed by literally millions of security-related messages every day. This daily deluge of security data is

being generated by the numerous "point" security solutions deployed across the enterprise: firewalls, intrusion prevention and detection, access control, identity management, anti-virus, etc. These solutions all generate information in different formats, store it in different places, and forward to different locations. And it is more than anyone can handle.

A CHECKLIST OF SOC REQUIREMENTS

Delivers Situational Awareness: Many IT organizations struggle to compile the resources needed to review the data coming from all of these systems. IT managers may say they do not have the time to check the intrusion detection or firewall logs because they are constantly battling the ramifications of the latest threat. On a network, security situational awareness is a constant ongoing health check. A zero-day threat can move through a network in seconds, wreaking havoc and putting business-critical systems at risk. The SOC diagnoses attacks through constant monitoring of managed devices on the network and correlates the data in realtime so that operators can see what is happening as it is happening and quickly respond to the threat.

Meets Business Operations Requirements: While each organization has its own specific security needs, there are some common, top-level security information management business requirements that apply to most organizations. Reduce Risk and Downtime. For most networks and businesses, the most important requirement is to keep the network running at an acceptable risk level without downtime. Years ago it may have been possible for an organization to shut down the mail server when an e-mail virus was quickly spreading, but for most organizations this is no longer an option. E-mail is a critical business application. The SOC must support the organization by intelligently and proactively alerting the right people at the right time about critical security events. If this risk can be mitigated before the security event begins attacking critical business systems, then the IT staff will not be forced to shut down those systems. When building the SOC, implement tools that will assist the organization to actively report security incidents in realtime using various methods for alerting, such as pagers, e-mail, or a centralized security management console.

Threat Control and Prevention: Organizations also must ensure that threats are either prevented or contained. This involves early notification of suspicious activity and the ability to quickly implement a containment mechanism. For example, if a firewall and network management system report the infiltration of a root kit aimed for a targeted host, the operator could be alerted to this root kit and remove it from the target host before the install process is complete and the host has been compromised.

Ease Administrative Overhead: The SOC should be designed to involve the least amount of human overhead. The SOC provides organizations with the ability to centralize all critical security information into one single centralized console and reduce the need for multiple staff members to manage and monitor the distinct devices. The goal is to empower a few administrators with the best information to enable fast, automated responses. Security information management tools that are open and interoperable make this goal easier to accomplish because the disparate data can be correlated and integrated into a single management tool.

People and Responsibilities: Many organizations must share trust and administrative control across subsidiaries, business units, and between partner organizations. For example, a state government may need to have an SOC that collects and manages information from distinct agencies such as the educational system and the police department. Leveraging the organization's security policy standards, responsibilities must be defined, including who is responsible for specific tasks and assigning accountability for response and control for each business unit or agency.

Audit and Compliance Support: One of the most critical business needs that the SOC can help address is the requirement for auditing to comply with corporate, government, and industry regulations such as HIPAA, SB 1386, and Sarbanes–Oxley. Having quick, flexible access to threat information, identity and access control data, and patch levels is critical for proving compliance.

Incident Response and Recovery: When systems are affected by a security event, administrators must be ready to respond as efficiently as possible to limit the damage, determine the root cause, and get the system back up and running quickly. A welldesigned SOC empowers administrators to see attacks on the network and helps them leverage incident management tools to pinpoint and remediate problems.

24/7 Uptime: If a network is running 24/7, the SOC must run 24/7. Security information management tools help provide the high-availability support needed to meet the "always on" requirement.

Ability to Respond Quickly through Real-Time Data and Automation: "Zeroday threats," such as malware and viruses, can spread within minutes across the world and throughout an organization. The SOC must provide information in real-time, giving operators the data to immediately take action. At the same time, the SOC also must be able to provide automated actions and resolutions to threats such as restarting systems, initiating a trouble ticket to the help desk to initiate and implement shielding tactics, and working with a patch management system to push patches to vulnerable systems.

Support for Federated and Distributed Environments: Many enterprises are run on a federated model, whether they support multiple business units, subsidiaries, or complex partner and customer frameworks. Portions of the federated network often are managed by various groups, sometimes with different business charters. When it comes to managing these distributed organizational networks in a holistic manner, the SOC must support federated views and management roles. For example, a subsidiary might report all data to the central SOC, but control for remediation might not be shared with the parent organization. For the SOC to meet those parameters, security information management tools must provide flexible role-based views and accounts to accommodate these differing needs.

THE SOC IN ACTION: With the SOC gathering information, an organization can respond quickly and effectively to security events and threats — even internal threats — in real-time. Consider the following example. A security administrator at a company is in a room in Colorado that is lit by the glow of numerous monitors showing physical areas of the campus. Each monitor displays data that is reporting from the distributed geographic sites of the enterprise. The administrator receives an alert on her main screen, clicks a button, and then picks up a phone and puts in a call to a local operator in California. The administrator responds to a security alert that showed someone improperly sending proprietary information out of the company. In just a few seconds, the user's access is locked, the local operator is dispatched to remove the user from the building, and an investigation into the incident is initiated.

CONCLUSION. Organizations are inundated with security information overload coming from disparate and often decentralized security systems operating in individual silos. To address these problems, organizations must carefully plan and deploy an SOC that centrally manages and monitors the network and security systems across a diverse IT environment. To be effective, the SOC demands the use of a comprehensive security information management (SIM) solution. Security information management tools offer a comprehensive security management and incident response platform designed to improve the effectiveness, efficiency, and visibility of security operations and information risk management

Дорохін Орест Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ЕТАПИ РЕАЛІЗАЦІЇ КІБЕРНЕТИЧНОЇ АТАКИ

Темпи розвитку інформаційних технологій в останні 10—15 років викликають чимало питань про потенційні межі і наслідки інформаційної глобалізації. Питання ці

багатопланові і мають філософський, юридичний, економічний і, звичайно, технічний характер. Усе частіше предметом публічних дискусій виявляються комп'ютерні злочини і їхній вплив на глобальні процеси в суспільстві. Інструменти «інформаційної війни» пускаються в хід для одержання переваг у конкурентній боротьбі, стаючи невід'ємною частиною арсеналу будь-якої великої компанії, не говорячи вже про спецслужби. У структури органів керування безпекою великих компаній останнім часом включаються підрозділи комп'ютерної й інформаційної розвідки, а діяльність іноземних спецслужб спрямована на масштабні проекти створення і застосування інформаційної зброї, здатної приховано проникати в автоматизовані системи керування критичними об'єктами потенційного супротивника, порушувати їхню роботу і приводити до витоку конфіденційних зведень.

Для успішного захисту кіберпростору держави, компанії чи навіть персональних конфіденційних даних життєво необхідно знати етапи проведення кібератак, що незалежно від масштабу мають приблизно однакову структуру. Це необхідна умова того, що ви зможете захиститись та адекватно протидіяти зловмиснику на будь-якому з цих етапів.

1. Розбір уразливостей, можливість реалізації атак

В час розвитку й ускладнення засобів, методів і форм автоматизації процесів обробки інформації підвищується залежність суспільства від рівня безпеки інформаційних технологій.

Вразливість автоматизованої системи – властивість системи, що робить можливим виникнення і реалізацію загрози.

Розглянемо можливі уразловості та загрози:

По меті впливу вразливості розділяються на три основні порядки:

- вразливості першого порядку – загрози порушення конфіденційності інформації;
- вразливості другого порядку – загрози порушення цілісності інформації;
- вразливості третього порядку – загрози порушення доступності або DoS.

При розгляді наслідків атаки на вразливість системи, модель характеризує успішність атаки, але не вартісні наслідки, викликані розкриттям, порушенням цілісності інформації чи відмовленням в обслуговуванні.

Оцінкою наслідків використання вразливості є оцінка кількості користувачів, задіяних в результаті успіху атаки на вразливість ЗАС. Якщо вразливість присутня в ЗАС, що захищає інформацію від загрози розкриття, то можливі наступні варіанти несанкціонованого доступу:

- до визначеної інформації користувача;
- до всієї інформації користувача;
- до всієї інформації групи користувачів;
- до всієї інформації всіх користувачів у системі.

2. Розробка методів реалізації атак, підбір технічних і програмних заходів

Перш ніж виконувати атаку на комп'ютерну систему, створюється стратегічний план. Сюди входить розвідка сил противника, його оборони, формування відповідного складу сил, розробка (якщо потрібно) додаткових атакуючих резервів.

Для успішної реалізації атак на систему, хакеру необхідно дізнатися:

1) тип атакуючої системи;
2) рівень знань користувача системи (жертви)
3) заходи захисту;
4) слабкі місця даної системи;
5) усвідомлювати мету атаки,
6) оцінити ймовірність успіху,
7) дізнатися, чи не зламувалася подібна система раніше і чи має вона типові проблеми безпеки.

8) що робити після успішного проникнення / виконання мети атаки

3. Проникнення в систему будь-якими способами

Існує декілька основних методів проникнення в систему:

1. Соціальна інженерія
2. Технічні методи

a. Мережеві хробаки

Хробаки можуть розповсюджуватись наступними способами:

1) Електронні листи
2) FTP
3) ICQ або його сучасні аналоги
4) P2P
5) Напряму через порти
6) USB та інші носії
7) Трояни

b. Сніффери
c. DoS атаки
d. Bruteforce

3. Комбіновані методи

a. Фішинг
b. Антивірусні програми, що мають у собі шкідливій код

4. Фізичний підхід

4. Автоматичний збір інформації, обман системи

Електронне шпигунство, інтернет шпигунство - види збору інформації, в основі яких лежать інформаційно-комп'ютерні технології. За масштабами цей вид шпигунства вже далеко перевершив всі інші способи отримання інформації.

Можна виділити три рівні кібершпіонажу: державний, корпоративний, особистісний. Шпигунство завжди супроводжувало державну діяльність.

Автоматичний збір інформації передбачає автоматичне виділення інформації та її перетворення в необхідну форму.

Автоматичний збір інформації здійснюється за допомогою таких методів:

- Переповнення буфера
- Троянські коні, черв'яки, сніффери, руткіти та інші спеціальні програми
- Сніффінг пакетів
- Man-in-the-Middle

5. Реалізація цілей атак

Кібератака — спроба реалізації кіберзагрози, тобто будь-яких обставин або подій, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі.

Характерна особливість кібератак — миттевість їх здійснення (протягом секунд, хвилин). Класифікують кібератаки за наведеними далі ознаками.

За принципом впливу на об’єкт атаки поділяються на:

- використання прихованих каналів;
- застосування прав суб’єкта системи до об’єкта;

За характером впливу на об’єкт атаки поділяються на:

- активний вплив;
- пасивний вплив;

За способом впливу на об’єкт атаки поділяються на:

- систему дозволів (захоплення привілеїв),
- безпосередній доступ до даних, програм, служб, каналів зв’язку з використанням привілеїв.

За засобами впливу на об’єкт атаки поділяються на ті, що передбачають:

- використання стандартного ПЗ;
- спеціально розроблених програм.

За об’єктом атаки: напад може здійснюватися на:

- систему в цілому;
- дані і програми, що містяться на зовнішніх або внутрішніх пристроях системи, а також у каналах передавання даних;
- процеси і підпроцеси системи за участю користувачів. Метою таких атак є або прямий вплив на роботу процесу (його припинення, зміна привілеїв і характеристик), або зворотний вплив (використання зловмисником привілеїв, характеристик тощо іншого процесу у своїх цілях).

За станом об’єкта: безпосередньо під час атаки інформація в ньому може зберігатися, передаватися або оброблятися. Наприклад, у ході передавання інформації лініями зв’язку між вузлами мережі або всередині вузла можливий доступ до фрагментів переданої інформації через перехоплення пакетів на ретрансляторі мережі або прослуховування з використанням прихованих каналів.

Зауважимо, що абсолютна більшість зазначених видів кібератак на практиці не застосовується. Натомість набула поширення класифікація, запропонована компанією Internet Security Systems Inc. Скоротивши кількість можливих категорій кібератак до п’яти, фахівці компанії умовно виокремили з них такі, що мають на меті:

1) сприяти збору інформації;
2) сприяти спробам несанкціонованого доступу до інформації;
3) досягти стану відмови в обслуговуванні;
4) імітувати підозрілу активність;
5) чинити вплив на операційні системи.

Згідно з міркуваннями фахівців компанії, перші чотири категорії охоплюють вилучені (можливо, віддалені) кібератаки, а остання стосується локальних кібератак (вони реалізуються на вузлі, що зазнає атаки). При цьому всі кібератаки можуть бути як автоматизованими, так і неавтоматизованими.

Цілі хакерських атак:

- Готовий веб-хостин
- Розміщення ботів
- Збір поштових адрес.
- Крадіжка особистості
- Розкрадання віртуальних цінностей
- Розкрадання фінансової інформації

Данні користувачів які цікавлять хакерів:

- Акаунти у соціальних мережах..
- Електронна пошта.
- Номер мобільного.
- Паспортні дані / ідентифікаційний код / фото.
- Особисте листування / фотографії / відео.
- Дані платіжних карт.

Методи викрадання інформації

1.Методи отримання паролів:

1) Підбір пароля онлайн
2) Підбір пароля оффлайн
3) Повторне використання пароля
4) Викрадення або підглядання пароля
5) Відновлення пароля через email або SMS
6) Перехоплення пароля по мережі

2. Викрадення даних в компанії

3.Викрадання персональних даних
6. Формування скритого каналу передачі вкраденої інфомації

Прихований канал – це спосіб одержання інформації за рахунок використання шляхів передачі інформації, існуючих у КС, але не керованих КЗЗ, або спостереження за існуючими потоками інформації.

За допомогою прихованих каналів можуть бути реалізовані наступні порушення політики безпеки:

- Загроза застосування шкідливих програм і даних.
- Загроза подачі порушником команд агентом для виконання його функцій.
- Загроза витоку криптографічних ключів, паролів (несанкціонований доступ до них) або окремих інформаційних об'єктів.

7. Приховування слідів присутності в системі

Є два аспекти завдання приховування слідів у системі:

- По-перше, це локальна безпека. Слід мати на увазі, що всі дії в віртуальному комп'ютерному світі залишають сліди і у системі суб'єкта також, що може стати джерелом великих проблем, адже це може стати доказами протизаконних дій
- По-друге, це глобальна безпека. Будь-які дії, в Інтернеті відслідковуються веб-серверами і фіксуються в лог-файлами як на серверах провайдера Інтернету, так і на відвіданих серверах.

Кроки для зачистки перебування системи: локально:

- Очистка реєстру.
- Очистка log-файлів програм авто-запуску
- Відключення аудиту.

Кроки для зачистки перебування системи: в Інтернеті:

Основний метою приховання діяльності в мережі «Інтернет» - підміна IP адреси.

Література і посилання

1. *xakep.ru/2001/02/21/12020/*
2. *kaspersky.ru/internet-security-center/threats/viruses-worms*
3. *http://conference.uapa.ru/attachment.php?aid=83*
4. *https://blog.kaspersky.ru/*

Світіна Ольга Сергіївна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ ПРИ ВИРІШЕННІ ЗАДАЧ КІБЕРБЕЗПЕКИ

Зростання інформаційних зумовило не тільки швидкий розвиток і ефективне застосування інформаційних мереж в підприємницькій діяльності та в повсякденному житті, а й зростання нових загроз. Анонімність глобальних інформаційних мереж, швидкість передачі інформації і простота їх використання, - те, що є основними причинами технологічного буму і проникнення мережі Інтернет в усі сфери життя, - одночасно дозволяє використовувати всі ці переваги для вчинення протиправних діянь.

Кіберзлочинність – це злочинність у так званому кіберпросторі, який створений і (або) сформований таким чином: комп`ютери, комп`ютерні системи, мережі, їхні комп`ютерні програми, комп`ютерні дані, дані контенту, рух даних, і користувачі. В даний час офіційне визначення кіберпростору на міжнародному рівні відсутнє, втім, як і визначення кіберзлочинності. Кіберзлочини поділяють на види залежно від об`єкта, від предмета посягання, залежно від способів скоєння і т. п.

У першу группу виділено злочини протии конфіденційності, цілісності та доступності комп`ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.

У другу группу входять злочини, пов`язані з використанням комп`ютера, як засобу скоєння злочинів - а саме, як засіб маніпуляцій з інформацією. У цю группу входять комп`ютерне шахрайство та комп`ютерне підроблення.

Третю группу складають злочини, пов`язані з контентом (змістом даних). У цю группу входять злочини, пов`язані з контентом - тобто з вмістом даних, розміщених в комп`ютерних мережах. Найпоширеніший і караних практично у всіх державах вигляд цих кіберзлочинів - злочини, пов`язані з дитячою порнографією.

У четверту группу увійшли злочини, пов`язані з порушенням авторського права і суміжних прав, при цьому встановлення таких правопорушень віднесено документом до компетенції національних законодавств держав.

П`ята группа злочинів зафіксована в окремому протоколі – це акти расизму та ксенофобії, вчинені за допомогою комп`ютерних мереж.

У рамках інформаційного забезпечення національної безпеки, захисту особистої інформації є боротьба з кіберзлочинністю. Для найбільш повного захисту до цього процесу залучається все більше інтелектуальних технологій:

- інформаційні технології інтелектуального управління автономними мобільними кібернетичними системами;
- зорові інформаційні технології, призначені для сприйняття та розпізнавання зображень;
- мовленнєві інформаційні технології, призначені для сприйняття, розпізнавання та синтезу природної людської мови;
- знання, орієнтовані інформаційні технології, призначені для аналізу, розуміння, інтерпретації, генерації текстовоїі нформації, та цифрові технології змістовної обробки текстової інформації;
- інформаційні нейромережеві технології для ефективної обробки знань.

Література:

1. *Башмаков А. И., Башмаков И. А. Интеллектуальные информационные технологии: Учеб.пособие. — М.: Изд-во МГТУ им. Н. Э. Баумана, 2005. — 304 с*
2. *uk.wikipedia.org/wiki/Інформаційні_злочини*
3. *Роберт І. Сучаснііінформаційнітехнологіїосвіти [Текст] / І.Роберт. — М. : Школа-Пресс, 2004. —*

Перепелиця Ліна Сергіївна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ПЕРСОНАЛ КАК ОДНА ИЗ ГЛАВНЫХ УГРОЗ ИБ.

При смене способа хранения информации с бумажного вида на цифровой, появился главный вопрос - как эту информацию защитить, ведь очень большое количество факторов влияет на сохранность конфиденциальных данных. Для того чтобы организовать безопасное хранение данных, первым делом нужно провести анализ угроз, для правильного проектирование схем информационной безопасности. Угрозы – неотъемлемая часть существования любой системы. Полностью обезопасить себя от них невозможно. И какой бы «идеальной» система защиты не была, существует угроза, действия которой невозможно предсказать – это человек.

Угрозы информационной безопасности – это различные действия, которые могут привести кнарушениям информационной безопасности. Другими словами, это потенциально возможные события/процессы или действия, которые могут нанести ущерб информационным и компьютерным системам. Угрозы ИБ можно разделить на два типа: естественные и искусственные. К естественным относятся природные явления, которые не зависят от человека, например, ураганы, наводнения, пожары и т.д. Искусственные угрозы зависят непосредственно от человека и могут быть преднамеренные и непреднамеренные. Непреднамеренные угрозы возникают из-за неосторожности, невнимательности и незнания. Примером таких угроз может быть установка программ, которые не входят в число необходимых для работы, в дальнейшем нарушающих работу системы, что и приводит к потере информации. Преднамеренные угрозы, в отличие от предыдущих, создаются специально. К ним можно отнести атаки злоумышленников как извне, так и изнутри компании. Результат этого вида угроз – огромные потери компанией денежных средств и интеллектуальной собственности.

Существует множество угроз и все их можно разделить по определенным характеристикам:

- По природе возникновения (естественные, искусственные);
- По степени преднамеренности проявления (непреднамеренные, преднамеренные);
- По непосредственному источнику угроз (природная среда, человек, программно-аппаратные средства);
- По положению источника угроз и т.д. (внешние, внутренние).

Еще з давних времён, когда человечество начало задумываться про безопасность не только своей жизни, но и всего, что его окружало, самой главной угрозой оставался сам человек. Даже стремительно развитие технологий, методов и средств защиты, не может полностью обеспечить защиту от человеческого фактора.

Точно такую же тенденцию можно наблюдать и в ИБ. Используя самые новые технологии по защите информации, руководитель не может полностью уберечь ее от персонала, который имеет дело с ней.

Начиная от простой ошибки в запросе и заканчивая умышленным вмешательством в работу систем защиты – человеческий фактор непредсказуем. Существует множество факторов, способных влиять на действия человека. В основном, их делят на «позитивные» и «негативные» факторы, но, в априори, они равносильны друг другу. На каждый минус всегда найдется плюс. Каждый из них тем, или иным способом влияет не только на человека, но и на уровень угрозы, которую может представлять из себя личность.

Человек (персонал), исходя из вышеизложенного, относится к внутренним угрозам ИБ. И в этому случае, персонал может как непреднамеренно оказывать негативное влияние на ИБ (ошибки в процессе работы с информацией и/или с системами защиты), так и преднамеренные (инсайдеры). Если инсайдера можно вычислить и ликвидировать (т.е. как-то обезопасить организацию от него), то уберечь предприятие от непреднамеренных угроз невозможно. Они, так или иначе, имеют место быть.

К непреднамеренным угрозам можно отнести:

- Уничтожение запрещенного для удаления файла;
- Изменение запрещенного для изменения файла;
- Некорректная установка программного обеспечения;
- Несоблюдение режима безопасности.

Так же, в этот список мы можем отнести некоторые социальные состояния, такие как: паника, страх, всеобщая апатия и т.д. При каждом из этих состояний, персонал будет по-разному выполнять одну и ту же работу или задание. Любое действие в одном из названых состояний, либо любая названная угроза, могут привести

организацию/предприятие к колоссальным убыткам. Контроль персонала под действием, например, паники, становиться практически невозможным.

Именно поэтому, руководителю следует, в первую очередь, быть как можно более внимательным к персоналу, который имеется в его организации. Если руководитель сможет правильно управлять подчиненными, шанс появления внутренних угроз, со стороны персонала, будет сводиться к минимуму. Традиционными методами управления персоналом можно назвать:

-Административные;

-Социально-психологические;

-Экономические.

Пропорцию, какой метод и в каком соотношении с другими следует использовать, составляет сам руководитель. Именно от его действий и решений зависит уровень угроз со стороны человеческого фактора. Полностью, к сожалению, избавиться от такого типа угроз невозможно.

И в заключение, хотелось бы напомнить, что человек, сам по себе, непредсказуем. Именно поэтому, человеческий фактор стоит в самом верху потенциальных угроз ИБ.

Литература:

1. *Угрозы информационной безопасности. [Электронный ресурс]: - Режим доступа - https://www.anti-malware.ru/threats/information-security-threats*
2. *Анализ угроз информационной безопасности. [Электронный ресурс]: Режим доступа - http://ypn.ru/106/analysis-of-threats-to-information-security/*
3. *Виды и источники угроз информационной безопасности. [Электронный ресурс] –Режим доступа – https://sites.google.com/site/kontrolnaarabotapooek000123/teoriticeskij-vopros-no2*

Хворостяний Родіон Віталійович

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

ЗАХИСТ МОВНОЇ ІНФОРМАЦІЇ

У сучасних умовах успішне функціонування і розвиток підприємств все більше залежать від забезпечення інформаційної безпеки. Інформація відіграє вирішальну роль як у сфері виробництва, бізнесу та підприємництва, так і в ході конкурентної боротьби. Особливе місце займають органи державного управління, де інформація нерідко носить таємний характер, і її захист повинен здійснюватись у суворій відповідності з державними нормативними актами у цій сфері. Одним з напрямків забезпечення інформаційної безпеки є захист інформації з обмеженим доступом, яка озвучується (під час проведення нарад, показів зі звуковим супроводом відеофільмів тощо) або здійснюється обробка технічними засобами акустичної інформації (системи звукопідсилення, засекречений зв'язок, у т.ч. урядовий зв'язок тощо).

Захист мовної інформації – діяльність, спрямована на запобігання витоку інформації, яка циркулює у вигляді акустичних хвиль (голосу людини).

Мовний сигнал – складний фізичний процес, пов'язаний зі зміною акустичних параметрів, які містять інформацію про зміст повідомлення .Мовний сигнал створюється голосовим апаратом людини і являє собою обурення повітряного середовища у вигляді хвиль стиснення і розтягнення (акустичні коливання). Енергія мовного сигналу зосереджена в діапазоні 300 - 4000 Гц.

Усвоєму первісному вигляді мовний сигнал в приміщенні присутній у вигляді акустичних і вібраційних коливань.

Залежно від середовища поширення сигналів і способів їх перехоплення технічні канали витоку мовної інформації можна розділити на:

Акустичні- за рахунок поширення акустичних коливань у вільному повітряному просторі (переговори на відкритому просторі, відкриті двері, вікна, вентиляційні канали);
Вібраційні (віброакутсичні) - за рахунок впливу звукових коливань на елементи і конструкції будівель, викликаючи вібрації (огороджувальні конструкції (стіни, стелі, підлоги, вікна, двері, короба вентиляційних систем тощо), інженерні комунікації (труби водопостачання, опалення, кондиціонування тощо));

Акустоелектричні - за рахунок впливу звукових коливань на ДТЗС (за рахунок зміни параметрів (ємність, індуктивність, опір) під дією акустичного поля,створюваного джерелом мовного сигналу та виникнення електрорушійної сили (ЕРС), або до модуляції струмів, що протікають по цим елементам, за рахунок «мікрофонного ефекту», за рахунок використання «високочастотного електромагнітного нав'язування»);

Оптико-електронні (лазерні канали) канали - за рахунок приймання та демодуляції відбитого відвібруючих під дією акустичного сигналу поверхонь приміщень (шибок, дзеркал тощо) випромінювання;

Параметричні - за рахунок впливу звукових коливань на ОТЗ і ДТЗС (за рахунок паразитної модуляції інформаційним сигналом випромінювань гетеродині в радіоприймальних і телевізійних пристроїв, які перебувають у приміщеннях, де ведуться конфіденційні переговори, за рахунок утворення вторинних радіохвиль, при «при високочастотному опроміненні» приміщення, де встановлені закладні пристрої, що мають елементи, параметри яких змінюються під дією мовного сигналу);

При проведенні робіт із технічного захисту інформації одночасно, з використанням одних і тих же приладів, методик та спеціалістів можуть здійснюватися заходи із захисту декількох каналів витоку інформації. Так, при проведенні робіт із захисту інформації від витоку акустичним каналом можуть проводитися роботи із захисту інформації від витоку віброакустичним і оптоелектронним каналами. Аналогічним чином здійснюються роботи із захисту інформації від витоку акустоелектричним та параметричним каналами побічних електромагнітних випромінювань та наводок (канали побічних електромагнітних випромінювань та наводок).

Виходячи з цього види роботи з технічного захисту інформації доцільно проводити за наступними напрямками:

- Захист інформації від витоку акустичним, віброакустичним та оптоелектронним каналами;
- Захист інформації від витоку акустоелектричними та параметричними каналами;
- Захист інформації від витоку через закладні пристрої.

Для захисту мовної інформації з обмеженим доступом від витоку технічними каналами на об’єктах інформаційної діяльності створюється комплекс ТЗІ.

Використана література

1. *Інтернет ресурс www.tzi.ua*
2. *Інтернет ресурс www.tzi.com*
3. *Інтернет ресурс www.nauka.com.ua*

Місевіч Катерина Сергіївна

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

ОПТИМАЛЬНЕ РІШЕННЯ ПРОБЛЕМ РОЗМЕЖУВАННЯ ДОСТУПУ НА ПІДПРИЄМСТВІ

У наш час контроль і розмежування доступу стали повсякденним явищем. Установка системи контролю доступу дуже швидко окупається за рахунок економії на

зарплаті та зменшенні розміру збитків, пов'язаних із крадіжками як речей, так і інформації, що становить комерційну таємницю. Втрата+ майбутньому, не слід забувати, що СКД лише спрощує процес ідентифікації, економить час і підвищує ефективність роботи служб безпеки підприємства, але, при цьому, все одно вимагає контролю з боку людини. Відсутність досвіду в сфері використання СКД серед покупців і відсутність фахівців вищого класу, здатних здійснювати ремонт і техобслуговування на високому рівні і в стислі терміни, призводить до помилок і недоліків, допущеним в процесі проектування систем, порушень правил експлуатації, що в цілому, значно знижує ефективність і доцільність застосування СКД.

Вибір варіанта СКД нерозривно пов'язаний з вимогами до забезпечення безпеки конкретного об'єкта. При виборі систем необхідно враховувати, що можливість проведення аналітичної роботи із застосуванням сучасних програмно-апаратних комплексів СКД є необхідною якісною характеристикою системи.Ефективність використання будь-яких технічних засобів СКД залежить від застосовуваної технології контролю доступу та кваліфікації оперативно-технічного персоналу.

Система, що пропонується, для контролю і управління доступом Fortnet призначена для вирішення завдань з регулювання та моніторингу доступу людей і інших об'єктів (наприклад, автотранспорту) через обладнані точки проходу. В рамках розмежування рівнів доступу персоналу і відвідувачів та забезпечення різних рівнів безпеки в СКД Fortnet передбачені гнучкі механізми контролю переміщень об'єктів як на рівні точок проходу (картки з PIN, прохід через тамбур-шлюз, додатковий датчик проходу), так і на рівні логічного контролю дій об'єкта (напр. заборона повторного проходу).

Централізовані мережеві системи контролю доступу FortNet будуються на основі керуючого контролера ABC-E.

В якості автономного сегмента системи контролю доступу або як елемент розподіленої мережевої СКД може виступати інтегрований контролер ANC-E, що поєднує в собі аналітичні можливості керуючого контролера і можливості управління зовнішнім виконавчим обладнанням (електромагнітний замок, турнікет, шлагбаум).

Програмно-апаратний комплекс FortNet являє собою приклад гідного рішення в контексті необхідності забезпечення обмеження та розмежування доступу на об’єктах як господарської, так і інформаційної діяльності. Апаратне забезпечення в сумісності з програмним додатком, розробленим спеціально для даного обладнання дозволяють здійснювати зручний моніторинг та контроль за розмежуванням доступу на підприємствах.

Література:

1.Гинце А. Новые технологии в СКУД // Системы безопасности, 2005.

2.Горлицин И. Контроль и управление доступом - просто и надежно КТЦ "Охранные системы", 2002.

3. Бондарчук А. П. Дослідження принципів системного підходу до проектування системи радіозв'язку //Наукові записки Українського науково-дослідного інституту зв'язку. – 2013. – №. 2. – С. 44-47.

4. http://www.intersyst.ru/solutions/165/460/

Хапун Анастасія Валеріївна

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

ПЕСИМІЗАЦІЯ. ЩО ЦЕ ТАКЕ І ЯК УНИКНУТИ?

На сьогоднішній день одним з найпопулярніших способів просування є оптимізація текстового контенту під пошукові системи. Це пояснюється досить високою ефективністю

і відносною простотою. Але часто трапляються ситуації, коли веб-майстри надмірно захоплюються оптимізацією текстів. Як результат, можна спостерігати переспам ключових слів або інші зловживання.

За такі провини пошукові системи передбачають покарання, саме воно має назву песимізація.

Головним змістом цих санкцій є зниження займаних позицій в пошуковій видачі. Крім того, в результаті пессимізації може наступити ще один вкрай небажаний наслідок – сайт можуть відключити від посилання ранжирування.

Песимізація – це не новий термін в області пошукового просування. Його почали застосовувати розробники однієї популярної пошукової системи ще в 2003 році. Виділяють два типи пессимізації: ручну і автоматичну. Розглянемо відмінності між цими явищами.

Автоматична песимізація відбувається в результаті перевірки сайту роботами пошукової системи. В ході перевірки, алгоритм визначає, що сторінка штучно переоптимізована. У підсумку місце сторінки в результатах пошуку істотно знижується.

Ручна песимізація передбачає накладання на ресурс певних санкцій, як відповідну реакцію на скарги користувачів про те, що Вам хтось продає рекламу. Зрозуміло, що недостатньо просто поскаржитися і сайт втратить позиції, – цією лазівкою б користувалися безліч недобросовісних конкурентів. Тому на скарги реагують компетентні кваліфіковані співробітники – модератори.

Песимізація не є незворотнім моментом. Всі негативні наслідки її застосування можна усунути. Але для цього веб-майстру доведеться виправити всі недоліки свого сайту. Після чого потрібно звернутися в службу підтримки для проведення повторного моніторингу.

Як уберегти сайт від песимізації?

Як ми визначилися, песимізація – це падіння рейтингу сайту у видачі. Це зниження є результатом накладання різних фільтрів. Пошукові системи використовують песимізацію для того, щоб зробити ТОП чистим від неякісних або недостатньо інформативних сайтів. Крім того, загроза песимізації тримає в рамках тих веб-майстрів, які тяжіють до сірих або чорних методів оптимізації.

Щоб не відчути на собі і своєму ресурсі, що таке песимізація, потрібно користуватися тільки легальними методами розкрутки. Крім того, сайт повинен відповідати вимогам цільової аудиторії і бути корисним.

Ресурси максимально схильні до ризиків песимізації:

- Сайти з неунікальним контентом, який копіюється з інших сайтів.
- Сайти, які використовують сторінки з перенаправленням відвідувачів на сторонні ресурси.
- Ресурси, які наповнені переспамленими ключами вмістом.
- Сайти, які не несуть ніякої користі користувачеві.
- Сайти, які займаються бездумним обміном неревалентних посилань.

Слід відрізняти бан і песимізація. Перше означає, що пошукова система повністю виключає ваш сайт з індексу. Друге ж передбачає штучне «притримування» пошуковими системами, тобто сайт продовжує індексуватися, але результати ранжирування будуть занижені.

Літеретура:

1. *Welant.com.* *SEO Glossary: Pessimization, Supplemental Results, Snippets*

Кисіль Владислав Андрійович
Державний університет телекомунікацій,
Навчально-науковий інститут захисту інформації
м.Київ

ВІРУС ШИФРУВАЛЬНИК ЯК ОДИН З ВИДІВ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розглянуто порівняння двох вірусів-шифрувальників, їх основні цілі, способи розповсюдження, способи шифрування Наведено основні методи запобігання інфікування вірусом комп'ютера користувачів. Оскільки за останній час було зафіксовано низку масштабних кібератак вірусів-шифрувальників, які були спрямованні на шифрування даних, що знаходяться на жорстких дисках користувач з подальшим вимаганням коштів.

Віруси-шифрувальники, також їх ще називають криптографічні віруси – це особливий вид програмного забезпечення, який здійснює шифрування всіх файлів на жорсткому диску. Після того як вірус зашифрував всі файли вірус активізується та блокує доступ до всіх даних, до того вірус не видає своє існування.

За останні пів року на території України сталося 4 масштабних кібератаки за участі вірусів-шифрувальників, а саме: PetyaA, Locky, Bad Rabbit та Scarab. За офіційними даними кіберполіЁції вірус PetyaA вразив по всій території України більше ніж 12500 комп'ютерів. На територію України припало 12,2% всієї атаки вірусів Locky та Bad Rabbit.

Вірусні атаки Locky та Bad Rabbit були здійсненні в один день, хоч кінцева мета кіберзлочинців і була ідентична – шифрування даних на жорсткому диску, але способи поширення шкідливого коду були різними.

Вірус Locky поширювався через фішингові розсилки електронних листів, зворотна адреса яких асоціювалася зі службою підтримки Microsoft, в яких містилися документи з розширенням .doc та .rtf. Після відкриття цих документів користувачем починалося інфікування комп'ютер, шкідлива програма завантажувала та виконувала файл вірусу, експлуатуючи вразливість у функції DDE офісного пакету. Далі вірус шифрував файли на диску і вимагав викуп для зловмисників..

Для поширення вірусу Bad Rabbit зловмисники скомпрометували популярні сайти, запровадивши в них шкідливий JavaScript код. Як тільки користувач заходив на заражений сайт з'являлося вспливаюче вікно з пропозицією завантажити оновлення для Flash Player. Але вспливаюче вікно з'являлося не завжди, а лише для користувачів, які були обрані за особливим алгоритмом. Далі поширення вірусу в локальній мережі відбувалося через сканування внутрішньої мережі на наявність SMB-файлів з відкритим доступом, також через протокол HTTP WebDAV, який заснований на HTTP і дозволяє використовувати Web як ресурс для читання і запису.

За даними антивірусних аналітиків ESET, Bad Rabbit — це модифікована версія вірусу Win32 / Diskcoder.C, більш відомого як Petya/NotPetya. У нової шкідливої програми виправлені помилки в шифруванні файлів. Тепер воно здійснюється за допомогою DiskCryptor — легітимного ПЗ з відкритим вихідним кодом, призначеного для шифрування логічних дисків, зовнішніх USB-накопичувачів і образів CD/DVD, а також завантажувальних системних розділів диска. Ключі генеруються з використанням CryptGenRandom і захищені жорстко закодованим відкритим ключем RSA 2048. Як і раніше, використовується алгоритм AES-128-CBC.

Кінцевою метою Bad Rabbit було шифрування жорсткого диску комп'ютера і друк на екрані повідомлення з вимогою викупу. Вірус вразив ряд популярних ЗМІ та деякі державні підприємства.

Успішність кібератак, що були спрямованні проти підприємств, свідчить про те що бізнес та держоргани приділяють недостатньо уваги інформаційному захисту. Важливо регулярно оновлювати антивірусне програмне забезпечення та прикладні програми, не

відкривати вкладення електронної пошти, що прийшла від неперевіреного відправника. Також одним з основних аспектів захисту від кібератак є своєчасне створення резервних копій критично важливої інформації.

Література:

1. Повідомлення департаменту кіберполіції Національної поліції [Електронний ресурс] – Режим доступу: https://www.facebook.com/cyberpoliceua/posts/601564659967701.

2. Повідомлення департаменту кіберполіції Національної поліції [Електронний ресурс] – Режим доступу: https://www.facebook.com/cyberpoliceua/posts/602125623244938

3. Звіт аналітиків ESET [Електронний ресурс] – Режим доступу: https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/

Кушнір Дмитро
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

HOW CYBERSECURITY SOLUTIONS CAN HELP WITH GDPR COMPLIANCE

Technical (protection) measures, means, technologies, rules and resources are mentioned multiple times throughout the GDPR text. The Regulation does not, however, specify any security technology implementation as obligatory (a few methods are suggested as optional solutions for the specific usage). Choice and evaluation of adequacy is the sole responsibility of the data controller and processor.

The range of possible technical mechanisms and safeguards for processing personal data depends primarily on the existing business processes and underlying ICT systems. Cybersecurity (or ICT security) solutions present a subset of possible technical approaches to ensuring compliance, characterized by its scope (digital domain) and purpose of application (preserving availability, authenticity, integrity, confidentiality, non-repudiation and privacy.

A saying, especially appropriate for GDPR, states that “there is no privacy without security” (not necessarily vice versa). So, what does InfoSec have in store for the GDPR buyer?

Before, during, and after

To put it bluntly, the purpose for cybersecurity protection lies in the very act of compromise. Since there is no way to eliminate threats altogether, only thing that’s left to do is strengthening the defences and then wait.

Security controls can be classified into one or more of the three groups: **preventive, detective and corrective controls**. Even if the division is not already familiar to the reader, their context can be inferred intuitively: certain measures can help minimize the risk of an incident and/or detect its occurrence and/or conduct an appropriate response; i.e. mitigate the consequences.

Most of the cybersecurity solutions today fall within more than one of the categories. For example, network and endpoint protection solutions prevent unauthorized access, but at the same time constantly monitor the systems’ usage and can detect anomalous behaviour, as well as block certain activities. An insider threat management portfolio provides a psychological barrier for the potential inside perpetrator, while storing a forensics audit trail and providing additional remediation functions.

On the other hand, some solutions are limited to a single domain. Most notable, but only on account of a specific mention in the GDPR, are encrypting and pseudonymising data. Inherently preventive, these solutions provide protection in two directions: rendering the data unreadable to the unauthorized user (not a member of the encryption chain of trust) or altering/masking the data in order to remove its ability to identify an individual (pseudonymising or data tokenization).

Cybersecurity maturity

A different perspective on ICT security posture offers several focuses, which could somewhat relate to the maturity of the security model of the organization.

The traditional basic approach to InfoSec was confined to **network perimeter and endpoint focus**, including primarily network firewall, antivirus and patch management solutions. Further need for protection and control lead to the **infrastructure and service focus**, offering implementations of Security Incident and Event Management (SIEM), Intrusion Detection/Prevention Systems (IDS/IPS), vulnerability management, Web Application Firewall (WAF), etc. Third is the **user focus**, which provides secure identity management mechanisms and monitoring of individual behaviour. This is achieved through tools and methods such as multi-factor authentication (MFA), Single Sign-on (SSO), Privilege Access Management (PAM), User Behaviour Analysis (UBA) and other solutions. Finally, data-centric focus concentrates on the data itself, by providing classification, encryption/pseudonymising, Data Leakage Protection (DLP) and others.

Although all four categories undergo constant progress and new types of solutions emerge, progression from the first to the fourth focus roughly resembles growth of cybersecurity maturity for most organizations. Adequate protection of (personal) data should therefore meet the corresponding qualities of all four security focuses.

Caveat emptor ("Let the buyer beware")

This short list of possible mapping of cybersecurity functionalities to GDPR requirements is by no means an exhaustive one. The security landscape is always widening—albeit one step behind the threat agents. An organization's InfoSec budget is the bottom line and risk management steers the wheel.

However, while prioritization of possible combinations of vulnerabilities, threats and mitigation measures will point to the specific technological direction, adequacy of the solution doesn't just depend on the requirements & specification matrix. Ongoing delivery and upgrade/maintenance of the solution bears as much importance to the continuous compliance as the functional and operational features.

To conclude: security is not perfect, and privacy has many difficulties. However, we simply can't afford to put up a Great Wall to keep our people's data in. Respecting their privacy via legally based business processes is not enough. In order to secure the data, organizations have to invest in the security technology (and continue to do so in a constant manner).

Bibliography

1. *https://www.helpnetsecurity.com/2017/12/05/cybersecurity-solutions-gdpr-compliance/*
2. *https://www.csoonline.com/article/3240245/security/cybersecurity-professionals-aren-t-keeping-up-with-training.amp.html*

М.В. Степаненко

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

МОДЕЛЬ ОЦІНКИ ЖИВУЧОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ КОРПОРАТИВНИХ МЕРЕЖ

Модель оцінки живучості систем захисту інформації корпоративних мереж зв'язку є сукупністю досить великої кількості окремих моделей різного призначення, що використовують для опису процесів як детерміновані, так і ймовірнісні методи .

Блок дестабілізуючих факторів (ДФ). За областю впливу розрізнятимемо точкові та просторові моделі ДФ. У точкових моделях вважатимемо, що ДФ точно виражає один або декілька функціональних елементів СЗІ КМЗ(Корпоративні мережі зв'язку). В останньому випадку область впливу ДФ – група точок, в яких розташовані структурні елементи системи захисту. Кількість елементів в СЗІ КМЗ завжди більша, ніж кількість точок в області впливу

ДФ. Тому для кожного елемента або групи елементів задамо ймовірність потрапляння в область впливу ДФ.

Розглянемо детальніше чотири характеристики моделі: розміри елементів, їхню надійність, стійкість і топологію системи. За розмірами елементи можуть бути точковими, лінійними, плоскими з межею у вигляді довільного контуру, об'ємні з межею у вигляді однозв'язної поверхні. За рівнем надійності елементів розрізнятимемо моделі з ідеально надійними елементами і моделі з обмеженою надійністю елементів. За рівнем стійкості розрізняємо елементи з нульовою і ненульовою стійкістю. Перший випадок є ідеалізованим та призначений для того, щоб в моделі оцінки живучості СЗІ КМЗ вважати непрацездатними всі елементи, що потрапили в зону впливу ДФ. У другому випадку ймовірність порушення працездатності залежить від інтенсивності ДФ і розміру тієї частини площі (або об'єму) елемента, яка потрапила в зону впливу ДФ.

За топологією системи розрізнятимемо моделі з довільною і заданою топологією. Модель першого типу використовуємо при точкових елементах і точкових ДФ. При просторових ДФ і плоских або об'ємних елементах використовуємо модель другого типу.

Таблиця 1

Моделі дестабілізуючих факторів за сукупністю характеристик

Фактори	Модель ДФ						
	1	2	3	4	5	6	7
Область дії	точка	точка	група точок	група точок	площа	площа	площа
Інтенсивність	∞	∞	∞	∞	∞	I0	I0
Тривалість дії	імпульс	імпульс.	імпульс.	імпульс.	імпульс.	τ	τ
Стратегія	1	2	1	2	1	1	2

Блок первинних наслідків (ПН) ДФ отримуємо у результаті взаємодії моделі працездатності з моделлю SFA, завдяки чому враховуємо аспект вразливостей моделі СЗІ КМЗ та ДФ, які через них впливають на систему захисту. В цій моделі не враховуємо управлінські впливи з боку засобів забезпечення живучості (ЗЗЖ).

Блок розвитку первинних наслідків (РПН) ДФ отримуємо в результаті поєднання моделі ПН і моделі ЗЗЖ, що дає змогу знайти траєкторію керованого перехідного процесу з урахуванням дій ЗЗЖ. Кінцевою метою аналізу моделі РПН є визначення нового стійкого стану системи. Оскільки деякі характеристики ЗЗЖ є ймовірнісними, результати аналізу моделі РПН також можна подати в ймовірнісній формі.

Блок надійності (Н) містить інформацію про безвідмовність і ремонтопридатність елементів, систему технічного обслуговування, про реакцію системи на окремі відмови елементів, про вплив різних факторів ДФ на безвідмовність елементів. Цю модель застосовуємо для оцінки живучості за наслідками виконання завдання.

Використана література

Костенко Б.Б., Кузнєцов С.Д. Історія и Актуальні проблеми темпоральних баз даних [електронний ресурс] -

http://citforum.ru/database/articles/temporal/. 13. Порай Д.С., Соловйов А.В., Корольков Г.В. Реалізація концепції темпоральной бази даних засобами реляційної СУБД //

Документообіг. Концепції та інструментарій / ред. В.Л. Арлазаров, Н.Є. Ємельянов: Едіторіал УРСС, 2004. - С. 92-109, Тр. Інституту системного аналізу Російської академії наук. 14. Темпоральні бази даних [електронний ресурс] - http://www.chair36.msiu.ru/articles/3/

html / node56.html.

Сухаревська Елеонора Сергіївна
Національний авіаційний університет
м. Київ

БЕЗПЕКА КІБЕРПРОСТОРУ У ЦИВІЛЬНІЙ АВІАЦІЇ

Досліджено актуальність впровадження єдиної системи кіберзахисту у сфері цивільної авіації як на рівні аеропортів так і на рівні повітряного судна. Розглянуто нормативно-правові документи, розроблені Міжнародною організацією цивільної авіації (ІКАО), які спрямовані проти незаконного захоплення і викрадення повітряних суден. Проведено аналіз кіберінцидентів, які виникли за останні роки дослідження кіберзагроз у цивільній авіації.

Сучасний рівень розвитку суспільства вимагає від розробників інформаційних систем та технологій більш високого рівня гарантій з приводу безпеки використання таких систем у різних сферах повсякденного життя та при виконанні професійних задач.

Слід зауважити, що цілісність та конфіденційність даних які обробляються, генеруються та використовуються для здійснення ефективної роботи авіаційної галузі у певній мірі залежить від наявності систем інформаційних технологій та систем забезпечення зв'язку. Також кіберінциденти у формі специфічного виду загроз для цивільної авіації (ЦА) швидко і постійно змінюється, та можуть забезпечувати злочинні наміри, спрямовані на порушення безпеки особистості або спотворення ділової репутації, чи заволодіння інформацією з політичних, фінансових або інших мотивів.

Кіберзагрози можуть легко завдати шкоди критично важливим системам ЦА в усьому світі. З підвищенням активності в економічній сфері завжди стрімко зростає обсяг транспортних потоків між країнами на великі відстані. Тому проблема підтримки безпеки при використанні повітряного транспорту пов’язана з необхідністю забезпечити високий рівень відмовостійкості повітряної техніки та наземних систем управління, не тільки як технічної системи, а й як інформаційної. Для вирішення такої складної задачі необхідно створити доволі розгалужену та уніфіковану систему управління безпекою польотів.

В останні роки кіберзагрози в ЦА набули реального прояву та реалізувалися. У якості прикладу можна навести дані про те, що у 2015 р. польська авіакомпанія LOT зіткнулася з хакерською атакою, яка привела до припинення діяльності компанії на деякий час. Були скасовані багато рейсів, співробітники варшавського аеропорту імені Фредеріка Шопена протягом декількох годин не могли скласти польотні плани. На щастя, проблема не торкнулася авіалайнерів, що знаходилися в той момент в повітрі. Представники авіакомпанії назвали інцидент «першою атакою такого роду» [1]. Також з’явилися офіційні відомості про те, що у грудні 2016 року групі комп'ютерних фахівців, за допомогою бездротового Wi-Fi підключення в салоні пасажирського повітряного судна, вдалося встановити контроль над літаком. Фактично, вони змогли обійти вбудований захист повітряного судна і отримати повний доступ до його систем керування [2].

У 2017 році тисячі пасажирів British Airways зіткнулися з хаосом, так як авіакомпанія була змушена скасувати понад сто рейсів з аеропорту Хітроу в Лондоні після відмови IT-системи. В даному випадку представники компанії виключили ймовірність кібератаки, проте ситуація добре продемонструвала, до яких проблем може призвести збій в інформаційній системі. Тому, ЦА - це одна з галузей економіки, для яких забезпечення безпеки є найвищим пріоритетом [1].

Сама проблема полягає в тому, що, фактично, будь-хто з присутніх в салоні пасажирського лайнера людей, за допомогою мобільного пристрою, може отримати доступ до систем літака, залишаючись до останнього моменту не викритим. Більш того, беручи до уваги можливості всесвітньої комп'ютерної павутини, доступ до управління системами повітряного судна може отримати і фахівець, який перебуває за межами повітряного судна,

наприклад, в тисячах кілометрах від нього, просто підключившись до пристрою одного з пасажирів і передаючи дані на системи літака.

Знати про існуючу загрозу, це лише половина справи, і куди більш важливим є створення відповідних методів захисту. У ЦА найбільш раціональним є використання спеціальних дублюючих систем, які працюють незалежно одна від одної, проте, це лише мінімізує ймовірність будь-якого інциденту, але не гарантує повної безпеки. Крім того, важливо захистити системи цивільного повітряного судна від втручання ззовні, зокрема, якщо мова йде про надання послуг доступу в мережу Інтернет, то устаткування, що забезпечує передачу даних, має бути повністю ізольовано від бортових систем, якщо мова йде про передачу даних екіпажу з землі, то інформація повинна проходити процедуру звірки і т.п. [2].

Сьогодні кіберзагрози розглядаються як незаконне втручання в процес управління повітряним рухом, як видача неправдивих вказівок, які можуть привести до авіакатастрофи. Але якогось спеціального документа Міжнародної організації цивільної авіації (ІКАО), який би чітко вказував, як діяти в разі кібернападів, поки немає. Держави, які є членами ІКАО - їх сьогодні вже 191, повинні виробити єдиний підхід до проблеми. Але в даний час немає навіть технологічної єдності в боротьбі з кіберзагрозами. Головне рішення за технічними фахівцями, які можуть захистити від таких загроз. Але тут, звичайно, є проблема секретності технологій.

ІКАО розробила декілька правових документів, спрямованих проти незаконного захоплення і викрадення повітряних суден [3]: 1) Токійська конвенції 1963 року, в якій вперше надано юридичну кваліфікацію незаконного захоплення і втручання в експлуатацію повітряного судна; 2) Конвенція про боротьбу з незаконним захопленням повітряних суден (Гаага, 1970 рік); 3) Монреальська конвенція 1971 року, в якій значно розширено перелік ознак, що визначають ті чи інші дії в якості актів незаконного втручання в діяльність ЦА; 4) Протокол про боротьбу з незаконними актами насильства в аеропортах, що обслуговують міжнародну ЦА, підписаний в Монреалі 24 лютого 1988 року, який доповнив Монреальську конвенцію; 5) Пекінська конвенція про боротьбу з незаконними актами щодо міжнародної ЦА і Пекінський протокол, що її доповнює, прийняті у 2010 року; 6) Протокол, що змінює Конвенцію про злочини та деякі інші акти, що здійснюються на борту повітряних суден (Монреаль, 2014 рік).

При формуванні рішень в сфері проблем кібербезпеки в ЦА необхідно визнати багатогранність і комплексний характер цих проблем. Тому ІКАО закликає держави і зацікавлені сторони галузі об’єднати зусилля та розробити заходи з протидії кіберзагрозам в сфері ЦА [4], серед яких: необхідність визначити загрози та фактори ризику, що подаються можливими кіберінцидентами щодо забезпечення польотів і критично важливих систем ЦА та коло обов'язків національних органів і зацікавлених сторін галузі по відношенню до кібербезпеки в ЦА; заохочення вироблення загального розуміння державами-членами ІКАО кіберзагроз та факторів ризику і загальних критеріїв для визначення важливості об'єктів і систем, що вимагають захисту; необхідність використовування гнучкого, заснованого на оцінці ризиків підходу до захисту критично важливих авіаційних систем шляхом впровадження систем управління кібербезпекою, а також визначення юридичних наслідків дій, що ставлять під загрозу безпеку польотів повітряних суден шляхом використання кіберврразливих місць.

Нові загрози змушують шукати нові рішення Загрози з боку кіберпростору можна здолати лише спільними зусиллями. Тому для критично важливих авіаційних систем, задля забезпечення їх ефективної роботи та протидії кіберзагрозам, мають бути наступними: безпека архітектури систем створюється на рівні конструкції; системи повинні мати запас міцності; способи передачі даних повинні забезпечувати цілісність і конфіденційність даних; повинні бути впроваджені методи моніторингу систем і виявлення інцидентів та подання повідомлень про них; необхідно здійснювати ретроспективний аналіз кіберінцидентів.

Література:

1. Испытывается новая система кибербезопасности в авиации [Електронний ресурс]. – Режим доступу: http://safe.cnews.ru/news/top/2017-12-02_novuyu_sistemu_kiberbezopasnosti_aviaperevozok. – Назва з екрану. – Перевірено: 14.03.18.

2. Кибербезопасность: как защитить авиацию? [Електронний ресурс]. – Режим доступу: http://avia.pro/blog/kiberbezopasnost-kak-zashchitit-aviaciyu. – Назва з екрану. – Перевірено: 14.03.18.

3. Пираты в воздухе [Електронний ресурс]. – Режим доступу: https://rg.ru/2017/07/17/kak-povysit-aviacionnuiu-kiberbezopasnost.html. – Назва з екрану. – Перевірено: 14.03.18.

4. Решение проблем кибербезопасности в гражданской авиации [Електронний ресурс]. – Режим доступу: https://www.icao.int/Meetings/a39/Documents/WP/wp_017_ru.pdf. – Назва з екрану. – Перевірено: 14.03.18.

СЕКЦІЯ №4. СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Лазоренко Анастасії Вячеславівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

СОЦІАЛЬНО-ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ ТЕЛЕКОМУНІКАЦІЙНОЇ СФЕРИ В УКРАЇНІ

Докорінні економічні перетворення, що здійснюються в Україні, спрямовані на посилення економічних методів управління та формування умов для повноцінного функціонування ринкових відносин, одне з найактуальніших завдань економічної науки і практики полягає у вивчені суті, структури й методологічних принципів наявного господарського механізму управління, а також у його моделюванні й на цих засадах – подальшому вдосконаленні. Пріоритетність цих напрямків зумовлюється тим, що на перших етапах соціально – економічних реформ у країні демонтаж попереднього господарського механізму відбувся випереджувальними темпами відносно формування нового; це призвело до відомих кризових явищ в економіці. І саме від успішної побудови механізму господарювання, адекватного сучасному стану продуктивних сил і виробничих відносин, значною мірою залежить перспективи розвитку як української економіки в цілому, так і окремих галузях.

Нині особливого значення набуває галузь зв'язку, справляючи величезний вплив на соціально – економічний розвиток суспільства, що переходить від індустріальної до інформаційної фази свого розвитку. Інформація дедалі більше стає повноправним учасником виробничих процесів і вирішальним чинником науково – технічного й соціального прогресу.

Розвиток соціально – економічних систем привів до того, що людина дістала можливості формування в новому соціумі. Вона стає соціально – активним, суспільним суб'єктом – особою зі своїм психологічним складом, дієздатністю і роллю в суспільстві. В цих умовах важливе місце в житті людини, в її соціальній діяльності займає зв'язок. Він (зв'язок) не лише перестає бути галуззю економіки країни в системі суспільного розподілу

праці, організаційних і економічних відносин, але й є безпосередньо включеним в органіку людини. “Людина як особа сама створює і будує свої відносини, бере участь у соціальному спілкуванні, управляє процесами. Зв’язок створює і матеріальні умови цього управління. За допомогою засобів зв’язку людина здійснює комунікацію як у сфері виробництва так і в соціальних відносинах. При цьому природа зв’язку проявляється передусім у характері його послуг, тобто його предмета. Саме через предмет долається простір. Зв’язок поєднує людей для спілкування...”, яке є однією з найбільш важливих потреб людини.

Сфера телекомунікацій особливу відіграє роль в забезпеченні управління економіки України. Створена така інформаційна система, яка дозволяє забезпечити функціональне, організаційне, економічне і соціальне узгодження та досягнення цілей управління телекомунікацій.

Телекомунікації відіграють важливу інфраструктурну роль у суспільстві, забезпечуючи оперативний обмін і розповсюдження інформації в процесах соціальної і економічної діяльності суспільства. Телекомунікації виконуватимуть роль комунікаційної основи при побудові інформаційного суспільства в Україні. Розвиток телекомунікацій повинен відбуватися випереджаючими темпами, порівняно з розвитком економіки, з тим, щоб не обмежувати економічний та соціальний розвиток суспільства.

Ці загальні закономірності повинні стати визначальними для розвитку телекомунікацій України на найближчу і більш віддалену перспективу. Телекомунікації повинні зіграти роль каталізатора у прискореному розвитку економіки та соціальної сфери України, оскільки основний ефект діяльності телекомунікацій проявляється не у вигляді доходів, прибутків і відрахувань у держбюджет, а у вигляді злагодженого і оптимізованого функціонування економіки та соціальної сфери країни, а також у вигляді покращення умов життя громадян.

Доходи від надання послуг зв’язку за 2007 – 2009 рр. зросли на 6414,7 млн. грн. або на 16,1 %.

Економічна діяльність сфери телекомунікацій характеризується рівнем доходів. Значне зростання доходів відбулось від надання таких послуг як надання комп’ютерних послуг (на 1730,2 млн. грн. або на 106 %), послуг кабельного телебачення (на 543,3 млн. грн. або на 73,3 %), проводового мовлення (на 83,6 млн. грн. або на 76,3 %). Відбулось зростання доходів від надання послуг мобільного зв’язку на 3419,8 млн. грн. або на 13,6 %

Таким чином, можна визначити, що розвиток телекомунікацій має величезну роль у загальному економічному розвитку країни, то як урядовим, так і неурядовим організаціям необхідно вжити ще більших заходів щодо сприяння розвитку саме цієї галузі. Недостатній розвиток телекомунікацій загрожує конкурентоздатності економіки України та перспективам її розвитку.

Література:

1. *Покровский В. Человеческое измерение рыночной экономики*
2. *Пугачев В. П., Соловьев А. И. Введение в политологию. - М.: Аспект-Пресс, 2000. - 275 с.*
3. *Человеческий потенциал: опыт комплексного подхода / За ред. И. Т. Фролова. - М.: Озон. 1999. - 176 с.*
4. *Управління суспільним розвитком: Словник-довідник / За заг. ред. А. М. Михненка, В. Д.*
5. *Бакуменка; Уклад.: В. Д. Бакуменко, С. О. Борисевич, О. А. Бутрін та ін. - К.: Вид-во НАДУ, 2006. - 248 с.*

Шахмайкін Тимофій Олексійович
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м.Київ

СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ ВПРОВАДЖЕННЯ ІНТЕРНЕТ-ПОСЛУГ В СІЛЬСЬКІЙ МІСЦЕВОСТІ

У статті досліджено соціально-економічні проблеми щодо впровадження інтернет-послуг у сільській місцевості України. Визначено проблеми та суперечності у телекомунікаційній сфері країни. Зазначено необхідність вирівнювання розбіжностей у рівнях соціально-економічного розвитку між сільськими та міськими населеними пунктами України.

Науково-технічна революція, що сталася у XX столітті, помітно змінила умови та характер економічного розвитку. Швидке розповсюдження в усьому світі наукових відкриттів, технічних винаходів, інформаційних технологій, нових засобів комунікацій - усе це чинить вагомий вплив на економіку, політику та культуру усіх країн світу.

Метою статті є визначення соціально-економічних проблему сфері телекомунікацй і шляхів впровадження інтернет-послуг у сільських регіонах та надання пропозицій щодо їх вирішення.Розвиток телекомунікаційної сфери стримується за рахунок низки проблем, які виникають унаслідок кризового становища економіки, зниження обсягу інвестування та доходів верств населення. У роботі не представляється можливості розкрити весь перелік питань, пов’язаних із вирішенням усіх наявних проблем у сфері телекомунікацій. Для аналізу розглянемо лише деякий перелік протиріч, наявних в області задоволення послуг зв’язку , які носять різний характер.

До них можна віднести:

- недоліки тарифної політики, у зв'язку з чим виникають проблеми зі взаєморозрахунками між телекомунікаційними підприємствами та споживачами послуг зв'язку, що спричиняє конфлікти, а, як наслідок, підвищуються тарифи на телекомунікаційні послуги. Крім того, існує проблема із забезпеченістю населення універсальними послугами зв'язку;
- фізичний та моральний знос обладнання, що спричиняє погіршення якості послуг зв'язку;
- недосконаліть стратегії розвитку телекомунікаційної сфери, тобто відсутність єдиної збалансованої стратегії розвитку та планування у телекомунікаційній сфері;
- недостатність кількості висококваліфікованих фахівців та зменшення їхньої кількості у зв'язку з постійною еміграцією, що сприяє зменшенню кількості інноваційних, науково-дослідних та дослідно- конструкторських робіт;
- відсутність механізму підтримки вітчизняного виробника, що спричиняє неможливість забезпечити себе продукцією власного виробництва;
- нестабільну економічну і політичну ситуацію в країні, що сприяє збільшенню рівня інфляції та безробіття, зменшенню споживання послуг зв'язку.

Найважливішою передумовою є розв'язання соціально-економічних проблем щодо вирівнювання рівнів розвитку телекомунікацій у міській та сільській місцевості. Нині лише у країнах Західної Європи, Північної Америки та в Японії показники телефонної щільності в містах і сільській місцевості приблизно однакові.

У країнах Східної Європи, включаючи Росію, а також Центральну Азію, Латинську Америку і Центральну Африку, телефонна щільність у містах приблизно у 2,5 рази вища, ніж у сільській місцевості, а в Північній Африці, країнах Близького Сходу та Південно-Східної Азії такий розрив досягає 5-7 разів. У цих регіонах проблема надання доступу до базових послуг усім громадянам незалежно від місця проживання постає найбільш гостро та належить до пріоритетних завдань розвитку національних телекомунікаційних мереж.

Також ми маємо змогу спостерігати ситуацію в Україні. В нашій країні треба більше уваги приділяти соціально-економічному розвитку сільських районів, враховувати та впроваджувати світовий досвід у цій сфері .

Однією з обов'язкових умов розвитку соціальної інфраструктури села є оновлення і розширення мереж телекомунікацій. Якісний телефонний зв'язок у сфері матеріального виробництва сприяє економії часу, дозволяє поліпшити використання

сільськогосподарської техніки та оперативне маневрування нею з урахуванням погодних умов, зменшити її простої і прискорити ремонт, забезпечити своєчасні поставки та заготівлі сільськогосподарської продукції.

Поширена думка, що експлуатація сільських мереж збиткова через низьку платоспроможність жителів аграрних районів та у зв'язку з високими капітальними витратами на один телефонний номер, що зумовлено більшою протяжністю ліній зв'язку (порівняно з міською мережею), а також низькою щільністю і нерівномірністю розподілу населення на селі. Тому протягом останніх двох десятків років одним із актуальних завдань залишається побудова рентабельних мереж телекомунікацій у сільських регіонах країн як з розвиненою, так і з економікою, що розвивається. Увага, яку приділяють даному аспекту, обумовлена перш за все тим, що ефективність одного телефону, що вводиться в сільській місцевості, значно вище, ніж у міській, хоча питомі капітальні вкладення на лінію в сільській місцевості можуть бути втричі-вчетверо більше .

Звичайна політика фінансування передбачала мінімальні інвестиції у створення телекомунікаційної інфраструктури в сільських і віддалених районах країн, що розвиваються. На жаль, ці інвестиції недостатні для гарантії загального доступу до основних телекомунікаційних послуг. Тому треба шукати інші способи фінансування. Нині уже загальновизнано, що сфера телекомунікацій невід'ємна, по своїй сутності, від комерції. Надання якісних телекомунікаційних послуг - це підприємство, що по праву може і повинно бути рентабельним. Воно забезпечує коштовні і життєво важливі стимули для економічного розвитку, поряд із соціальним і культурним розвитком, особливо у сільських і віддалених районах.

На мій погляд, до основних проблем щодо розвитку телекомунікацій у сільській місцевості можна віднести:

- розрив між існуючим і раціональним рівнем розвитку мережі.
- розрив між існуючим рівнем якості послуг, що надаються, та необхідним для більшості користувачів з урахуванням витрат на його забезпечення .
- моральний та фізичний стан основної маси обладнання телекомунікаційних мереж (лінійні споруди, автоматична телефонна станція (АТС), системи передачі), близько 60% парку обладнання є морально та фізично застарілим.
- однозначного визначення загальнодоступних телекомунікаційних послуг, затвердження механізму їх фінансування та реалізації з врахуванням сучасного стану економіки України.
- розрив між соціальною значущістю наявності повної номенклатури телекомунікаційних послуг для кожного населеного пункту і обсягів збитків для операторів, які повинні їх надавати.
- розрив між приведеними витратами на організацію послуги та можливими доходами від них.

Судячи з вищезазначеного, можна констатувати, що оператору практично може бути не вигідно розвивати сільський зв'язок с сучасними телекомунікаційними послугами, а тим більш його модернізувати, але з точки зору суспільства - це вкрай необхідно.

Таким чином, незважаючи на визначений обсяг соціально-економічних проблем, сфера телекомунікацій, яка займає значне місце в економіці країни (регіону, району), чинить значний вплив на її соціально-економічний розвиток. Проблеми складні, однак без їх вирішення неможливий подальший розвиток телекомунікацій та економіки країни в цілому та її окремих регіонів.

Література:

1. Закон України «Про Телекомунікації». К.: Державне видавничо-інформаційне агентство «Зв'язок», 2003. 58 с.

2. Современный экономический словарь / Б.А. Райзберг, Л.Ш. Лозовский, Е.Б. Стародубцева. М.: Инфра-М,

1996. 493 с.
3. Кузьминов А.В. Проблемы и противоречия в управлении электросвязью региона и пути их разрешения / А.В. Кузьминов // Спеціалізований випуск матеріалів конференції «Проблеми управління та економічного розвитку підприємств зв'язку - Економіка'99»: збірник наукових праць. О.: УДАЗ ім. О.С. Попова, 1999. 98 с.
4. Економіка телекомунікацій [Текст]: навч. посіб. [для студентів вищих навчальних закладів] ; за заг. ред. В.М. Орлова. О.: ОНАЗ ім. О.С. Попова, 2014. 512 с.

Лазоренко Анастасія Вячеславівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м.Київ

СВЯЗЬ И ТЕЛЕКОММУНИКАЦИИ

Современное состояние мирового рынка услуг связи характеризуется глубокими структурными сдвигами. Интенсивные процессы компьютеризации телекоммуникационного оборудования идут параллельно с процессами приватизации национальных систем связи, появлением на рынке крупных частных фирм — операторов, что приводит к усилению конкурентной борьбы. В результате непрерывно снижаются расценки на телекоммуникационные услуги, расширяется их ассортимент, а потенциальные пользователи имеют возможность выбора наиболее конкурентоспособного оператора.

Большинство промышленно развитых стран мира интенсивно переходят на цифровой стандарт связи, который позволяет мгновенно передавать колоссальные объемы информации, при этом гарантируется высокая степень информационной зашиты. В отличие от связи аналоговой, основанной на медном кабеле, координатных и декадно-шаговых АТС, цифровая система связи предполагает наличие электронных АТС с мошным процессором, волоконно-оптических кабелей и радиорелейных труб.

На мировом рынке телекоммуникационных услуг отчетливо проявляется тенденция развития полносервисных сетей, построенных на базе технологии коммутации пакетов услуг. Появление подобных сетей выводит на рынок принципиально новую услугу — универсальный широкополосный доступ к услугам связи и информации.

В 70-е гг. прошлого столетия Россия практически пропустила первую информационную революцию, не освоив промышленного производства цифровых АТС и оптико-волоконного кабеля. По оценкам специалистов, Россия в начале третьего тысячелетия по уровню развития средств связи и телекоммуникационных систем отстала от западных стран примерно на 10-15 лет.Доля отраслей связи и телекоммуникаций в ВВП промышленно развитых стран мира постоянно увеличивается и составляла в начале третьего тысячелетия от 5 до 8%. В России данный показатель не превышал 2%.

Література:

1. *Гальчинський А.С., КШах А.К., Семиноженко В.П. Інноваційна стратегія українських реформ. — К.: Знання України, 2002. — 326 с.*
2. *Дименко Р.А. Інноваційна складова конкурентних стратегій національного господарства*
3. *//Актуальні проблеми економіки. - 2008. - No 7. - С. 24- 29.*

Картамишева Олена Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м.Київ

ОСНОВНЫЕ ВИДЫ СВЯЗИ

Основным показателем развития рынка услуг электросвязи общего пользования является телефонная плотность (ТП), т.е. число телефонов на 100 жителей, он прямо

коррелируется показателем ВВП на душу населения. По данным официальной статистики, в 2009 г. телефонный парк в России насчитывал около 47 млн апла- ратов, т.е. на 100 россиян приходилось 30 телефонов, в то время как на столько же жителей США и стран Западной Европы — от 60 до 70 телефонов.

В России в начале третьего тысячелетия не было телефонизировано 54 тыс. населенных пунктов, насчитывалось 4 млн очередников (2009 г.) и около 50 млн потенциальных владельцев телефонов. Тарифы на местную телефонную связь для населения были ниже фактической себестоимости. Министерство связи РФ планировало увеличить количество телефонов к 2010 г. до 48 млн. Соответственно, показатель телефонной плотности должен возрасти до 33%.

Однако, чтобы достичь таких показателей, недостаточно увеличения емкостей за счет ввода новых АТС и прокладки новых километров кабелей: необходимо заменить морально устаревшее аналоговое оборудование цифровыми системами связи.

В России удельный вес телефонных сетей, использующих цифровые системы связи, возрос с 11% в 1995 г. до 27% в 2000 г. По планам Министерства связи РФ «цифровизация» телефонной системы связи в России к 2010 г. должна была достичь 94%. Однако этот показатель пока не выполнен.

С начала 90-х гг. прошлого века в мировой системе связи фантастическими темпами развивается сотовая связь. Число абонентов сотовой связи в России в 1995 г. составляло примерно 88,5 тыс. человек. Услугами данной системы связи пользовались преимущественно в Москве и Санкт-Петербурге, где было зарегистрировано около 90% всех абонентов. В начале 2000 г. в России насчитывалось уже более 3 млн абонентов сотовой связи, в 2001 г. — 7.8 млн, в 2002 г. - 17,6 млн, в 2003 г. — 35,6 млн, в 2004 г. — 71,3 млн, а в 2005 г. — уже 123,6 млн абонентов, в 2009 г. — свыше 140 млн абонентов. Показатель плотности мобильной связи значительно возрос, однако это было ниже аналогичного показателя для промышленно развитых государств.

Основные требования к закону о телекоммуникациях. Реформирование отрасли связи должно основываться на сильной законодательной базе, которая, в свою очередь, создается на основе действующего национального законодательства. Чтобы закон прошел горнило парламента, он должен получить поддержку на самом высоком политическом уровне государства. В законе о телекоммуникациях должны быть отражены следующие моменты: цели телекоммуникационной политики, регуляторные функции, процесс принятия решений и роль в нем государственных органов.

Література:

1. *Чекаліна М.А. Принципи стратегічного планування на підприємстві/ М.А. Чекаліна // Вісник ОДУ. – 2009. – No 1. – С. 83-89.*
2. *Кузьмінов А.В. Узгодження мотиваційних впливів на ефективність механізму управління телекомунікаціями регіону: дис. ... канд. екон. наук: 08.07.04 / А.В. Кузьмінов, Одеська національна академія зв'язку ім. О.С. Попова. – Одеса, 2005. – 224 с.*
3. *Економіка телекомунікацій: навч. посіб. [для студентів вищих навчальних закладів]; за заг. ред. В.М. Орлова. – О.: ОНАЗ ім. О.С. Попова, 2014. – 512 с.*
4. *Кравченко А.І. Історія менеджменту: підручник / А.І. Кравченко. – 3-тє вид., перероб. і доп. – М.: КНОРУС, 2010. – 432 с*

Картамишева Олена Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

ЦЕЛИ ТЕЛЕКОММУНИКАЦИОННОЙ ПОЛИТИКИ

Телекоммуникационная политика должна преследовать те же основные цели, что и любые другие направления правительственной политики: экономический рост, развитие

конкуренции, социальная стабильность. Поэтому цели телекоммуникационной политики могут быть в каждой отдельной стране разными, в зависимости от уровня развития в ней отрасли связи, а также социальной и законодательной среды. Но существует ряд универсальных требований, не зависящих от особенностей конкретных стран.

Государственное вмешательство в сферу телекоммуникаций должно соответствовать следующим категориям целей:

а) Развитие телекоммуникационной инфраструктуры

Такие государства, как Украина, сталкиваются со многими проблемами, связанными с развитием инфраструктуры связи, от решения которых зависит процветание нации. Создание условий для инвестирования в телекоммуникационную отрасль позволит приблизить национальную экономику к требованиям, выдвигаемым современным информационным обществом.

б) Повышение эффективности телекоммуникационного сектора

Повышение эффективности отрасли связи позволит снизить среднюю стоимость телекоммуникационных услуг для потребителей и повысить производительность предприятий, использующих телекоммуникации в процессе производства. Использование рыночных механизмов вместо бюрократического контроля также повышает эффективность отрасли. Европейский опыт показал, что открытый рынок и свободная конкуренция идут на пользу как отдельным пользователям, так и обществу в целом. Таким образом, одной из основных целей современной телекоммуникационной политики являются внедрение и поддержка функциональной конкуренции, которая сама по себе является наилучшим регуляторным инструментом для достижения эффективности, низких цен, внедрения новшеств и наивысшего уровня услуг для потребителей.

в) Обеспечение высокого качества услуг

Повышение качества услуг расширяет их роль в экономической деятельности в целом. Первоочередным шагом для обеспечения высокого качества услуг является разрешение существующих проблем в работе телекоммуникационных сетей, в частности, связанных с их перегрузками. Другим компонентом повышения качества телекоммуникационных услуг является технологический прогресс, расширение общей емкости сетей, внедрение новых технологий связи.

г) Защита общественных интересов

Естественно, что каждое правительство считает долгом защиту интересов своих граждан путем установления определенных стандартов на общедоступные услуги связи и защиту общих социальных ценностей (универсальные услуги, обеспечение конфиденциальности информации и защита прав потребителей). Государство может либо поддержать, либо тормозить этот процесс теми или иными регуляторными действиями.

д) Защита верховенства права и принципа эффективного управления

Характерной особенностью современных изменений в международном телекоммуникационном секторе является то, что операторами телекоммуникационных сетей и услуг становятся частные компании и акционерные общества. Государственное вмешательство в телекоммуникационный сектор должно базироваться на принципах верховенства права и эффективного управления. Все регуляторные решения государственных органов, касающиеся участников рынка, следует принимать прозрачно. Более того, все регуляторные функции государства должны выполняться в пределах закона и носить прикладной характер. Именно поэтому необходимо создать прозрачную и системную законодательную среду.

Для достижения общих целей телекоммуникационной политики законодательный орган совместно с правительством должны создать такую модель, которая определила бы функции регулирования, процедуры и процесс принятия решений, а также очертила полномочия регуляторного органа.

Регуляторная деятельность должна осуществляться в следующих сферах:

- регулирование условий вхождения операторов на рынок телекоммуникационных услуг;
- техническое регулирование таких направлений, как выделение, распределение и мониторинг частот и номерного ресурса, сертификация конечного оборудования и политика стандартизации;
- регулирование деятельности операторов на рынке для обеспечения добросовестной конкуренции и соблюдения требований антимонопольного законодательства (например, по поводу взаимоподключений и доступа к сетям), защиты пользователей, контроля над ценами и качеством услуг;
- контроль над выполнением лицензионных условий и требований нормативно-правовых документов государственных органов, регулирующих сферу связи.

Вышеупомянутые регуляторные функции означают, что государственное вмешательство в сектор возможно только в определенной форме. Регуляторные действия государства должны:
- основываться на прозрачных и последовательных целях телекоммуникационной политики и быть надежными и предсказуемыми для операторов и пользователей;
- быть достаточно гибкими, чтобы реагировать на развитие сектора;
- предусматривать и учитывать экономические и социальные последствия подобного регулирования.
- законодательная власть

Регулятор, его функции и процедуры принятия решений института необходимо определить в законе. Закон о телекоммуникациях устанавливает общие рамки для государственного вмешательства в телекоммуникационный сектор. Устанавливать в пределах этих рамок правила решения тех или иных вопросов и нести ответственность за принятие ежедневных регуляторных решений должны правительство и подведомственные ему структуры. Эти правила формулируются в виде подзаконных актов, что обеспечит гибкость регуляторной политики и возможность легко приспосабливаться к любым изменениям на рынке телекоммуникаций.
- исполнительная власть

Органы исполнительной власти призваны определять цели и политику для телекоммуникационного сектора, а именно:
- определять приоритеты развития сектора связи;
- инициировать предложения для новых направлений телекоммуникационной политики и соответствующего законодательства;
- защищать принцип верховенства права в отношении подведомственных правительству органов;
- управлять международной деятельностью отрасли.
- регуляторный орган

Существование независимого регуляторного органа имеет ряд преимуществ, а именно:
- базируется на положительном опыте многих стран и соответствует требованиям современных телекоммуникационных рынков;
- обеспечивает оптимальную защиту интересов пользователей;
- сводит до минимума политическое вмешательство и протекционизм;
- создает стабильную и предсказуемую регуляторную среду для инвесторов;
- делает возможным гибкое и быстрое приспособление к технологическим изменениям в отрасли.

Таким образом, регуляторный орган должен осуществлять ежедневный контроль над соблюдением определенных принципов телекоммуникационной политики. Это, в частности, касается выдачи лицензий и разрешений, регулирования тарифов и услуг, а также определения технических стандартов надзора за их соблюдением. Государственное вмешательство в телекоммуникационный сектор должно основываться на четком

размежевании операционных задач, функций, связанных с собственностью, и регуляторных задач. Следует создать механизмы, которые сделают невозможным влияние интересов отдельного оператора на регуляторную политику в отрасли. В то же время полномочия регуляторного органа должны быть ограниченными, чтобы не допустить дискриминации операторов или пользователей.

Регуляторный орган должен действовать исключительно в пределах предусмотренных процедур. Кроме этого, следует обеспечить разрешение споров в суде, предусмотрев, однако, и внесудебные пути урегулирования конфликтов.

С другой стороны, любое лицо, являющееся объектом регулирования, должно выполнять предусмотренные правила и процедуры. Необходимо создать возможность для применения адекватных санкций за совершенные нарушения действующего законодательства.

Предлагаемая вниманию читателей модель *(см. рис.1)*подытоживает требования к роли различных государственных органов и отношений между ними.

Література:

1. *Ligonenko L.O. Antikrizove upravlinnya pidprijemstvom: teoretiko-metodologichni zasadi ta praktichnij instrumentarij / L.O. Ligonenko. – K. : KNTEU, 2001. – 580 s.*
2. *Chuxno A. Suchasna finansovo-ekonomichna kriza: priroda, shlyaxi i metodi ïï podolannya / A. Chuxno Ekonomika Ukrajini. – 2010. – No 1. – S. 4-18.*
3. *Dosyagnennya sferi zv'yazku za sichen-veresen 2014 roku (vsya informaciya navedena bez uraxuvannya danix ARK ta m. Sevastopolya) [Elektronnij resurs] / Nacionalna komisiya z pitan regulyuvannya zv'yazku*
4. *Ukraïni. – Rezhim dostupu: ttp://www.nkrzi.gov.ua/index.php?r=site/ index&pg=138&language=uk*

Гукасян Анна Суревнівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м.Київ

ЭКОНОМИКА СОВРЕМЕННЫХ ТЕЛЕКОММУНИКАЦИЙ

Экономика современных телекоммуникаций представлена разнообразными видами сотовой, пейджинговой и тому подобной связи. Сегодня достаточно уплатить определенную сумму и операторы фиксированной связи рынка розничных телекоммуникационных услуг подключат любого гражданина России к качественной телефонии — международные, смешанные и национальные компании, МГТС, «Би Лайн» (торговая марка компании «ВымпелКом»), МТС (торговая марка компании «Мобильные ТелеСистемы»), операторы которых работают в сети GSM-900, GSM-1800. С 2001 г. на московском рынке сотовой связи появилась компания — «Соник Дуо», обслуживающая своей телекоммуникационной сетью Москву и города Подмосковья.

Тарифные планы современных телекоммуникаций сравнительно высоки. Среди дополнительных услуг, которыми можно воспользоваться, - переадресация вызова (если абонент отсутствует у данного телефонного аппарата, то все вызовы абоненту будут переключаться на любой другой запрограммированный им номер), развиты услуги конференц-связи, т.е. возможность вести телефонные разговоры одновременно с несколькими абонентами, услуги по оповещению во время телефонного разговора о том, что звонят и др.

Многие компании фиксированной связи предлагают телефонные карты, воспользоваться которыми можно с любого телефона. Такая предоплачиваемая телефонная карта, например «Диалог-Весь Мир» компании «Совинтел», предоставляет абоненту возможность телефонной связи с большинством стран мира из Москвы и Санкт-Петербурга.

Корпоративные клиенты получили возможность использовать пакет разнообразных телекоммуникационных и корпоративных Интернет-услуг.

Например, услуга Global Web Hosting заключается в том, что все ресурсы клиента будут круглосуточно защищены от несанкционированного доступа, при этом обеспечивается не только их охрана, но и бесперебойное питание. Другие новые услуги телекоммуникаций обеспечивают заказчикам полную надежность обмена информацией, находящейся внутри корпоративных Интернет-серверов, которые теперь недоступны компьютерным взломщикам-хакерам.

С 2000 г. тарифы телекоммуникаций с помощью мобильных радиотелефонов, компаний «Би Лайн» и МТС практически уравнялись, что вынуждает этих конкурентов предлагать все более экономные тарифные сетки. Такими экономными тарифами стали тарифы МТС «Экономный» и «Молодежный». Тарифы «Би Лайн» — «Профессионал» и «Ты и Я» — привлекают клиентов своей либеральной ценой услуг телекоммуникаций. Для отдельных, «многоговорящих» категорий абонентов, «Би Лайн» вводит тариф «Супер-GSM».

Література:

1. *Петюх В.М. Управління персоналом: [навч.-метод. посіб. для самост. вивч. дисц.] / В.М. Петюх. К.: КНЕУ, 2000. –124 с.*
2. *Інноваційний розвиток підприємства: [навч. посіб.] / Заред. П.П. Микитюка. – Тернопіль: Принтер Інформ, 2015. –224 с.*
3. *Юрасов И.А. Инновационные технологии управления /И.А. Юрасов // Управление персоналом. – 2006. – No 20. –С. 59–63.*
4. *Кошарная Б. Кадровые нововведения: понятие и харак-теристика / Б. Кошарная // Инновационный и кадровый менеджмент [Электронный ресурс].*
5. *Режим доступа: http://www.smartcat.ru/Personnel/innovacionnyykadrovyymenedzhmentQ.shtml.*

Гукасян Анна Суренівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м.Київ

ЦИФРОВА ЕКОНОМІКА. НАВІЩО ЦЕ УКРАЇНІ?

Сучасні технології швидко змінюють світ, і Україні потрібно йти в ногу з часом, щоб регулювати економіку. Які переваги може дати нашій країні цифрова економіка, у своїй колонці на НВ розповів перший віце-прем'єр-міністр України Степан Кубів. «Мінфін» скоротив.

Окремі цифрові рішення в Україні функціонують давно. Однак зосереджені вони переважно у великих містах. І лише там, де існує якісне інтернет-покриття. Тож цифровий розрив в Україні полягає, передусім, у нерівних можливостях доступу до інтернету на усій території.

Цей недолік треба якнайшвидше усунути!

Вирішити цю проблему можна кількома способами: через забезпечення широкосмугового доступу до інтернету по усій країні, а також через запровадження технологій 4G. До речі саме зараз триває збір заявок на участь у тендері на 4G, який запланований на 23 січня 2018 року.

Чим більшим буде охоплення інтернетом, тим краще можна буде скористатися цифровими можливостями у різних сферах. Наприклад в Естонії, про яку я вже казав, після цифровізації бази даних вакансій на 15% більше безробітних знайшли роботу. Уся економіка суттєво зміниться на краще.

Широке розповсюдження інтернету по Україні дозволить поширити використання цифрових сервісів на багато сфер. Так, збільшення кількості користувачів з 5 млн у 2016 році до 15 млн уже у 2021 дозволить 95% усіх магазинів, салонів, сервісів проводити розрахунки безготівково. Це зменшить витрати на друк паперових грошей і сприятиме виходу економіки з тіні. Зросте продуктивність праці і доходи громадян. Рівень корупції значно зменшиться, бо переважна більшість транзакцій буде проходити в електронній формі і автоматично у кількох реєстрах.

Цифрова сфера може формувати понад 300-400 тис. нових робочих місць по усій країні, міста стануть зручнішими, перейдуть на цифрові платформи управління інфраструктурою і сервісом.

Велика кількість змін потребує визначення пріоритетів, які дадуть найбільших «цифровий ефект».

На жаль, сьогодні в Україні відсутня єдина візія переходу на цифрову економіку. І це є основною причиною різноспрямованих зусиль та низької результативності України у цифровій сфері.

Є окремі проекти, рішення і технології, над якими працює Уряд, держагенства, представники окремих організацій та компаній, навіть окремі люди. 4G, ProZorro, «розумні-міста», електронна митниця, електронна медкарта (e-Health), електронне урядування тощо.

Вкрай потрібна єдина стратегія цифрової економіки, щоб загострити фокус та спрямувати зусилля на ключові пріоритети. Виходячи з потреб, з урахуванням наявних можливостей, аналізу сильних і слабких сторін. Бо нещодавно навіть виявилося, що розвиток інновацій та цифрова економіка як поняття взагалі відсутні у переліку повноважень профільного економічного міністерства! Тому ініційовано спільну роботу між Міносвіти та Мінекономрозвитку, аби визначити чіткі межі між суто академічними науковими дослідженнями та пошуком інновацій для реального сектору економіки. Уряд навіть вперше заклав у проекті бюджету 2018 року 50 млн грн на фінансування підтримки інновацій. У результаті зможемо більш ефективно впливати на перетворення результатів наукових досліджень у практичні рішення для розвитку інновацій та цифрової економіки в Україні.

Література:

1. *Дзюндзюк В. Б. Ефективність діяльності публічних організацій [Текст]: монографія / В. Б.*
2. *Дзюндзюк. — Х.: Видво ХарРІ УАДУ "Магістр", 2003. — 236 с.*
3. *2. Бабінова О. Проблеми оцінки якості та ефективності діяльності органів місцевої влади*
4. *[Електронний ресурс] - Режим доступу: http://www.niss.gov.ua/Monitor/September/6.htm*
5. *3. Д. Олійник Сучасні методи оцінки ефективності діяльності органів державного управління / Д. В.*
6. *Олійник // Ефективність державного управління. - 2013. - Вип. 34. - С. 275-283.*
7. *4. Ресурсний центр CAF Європейського інституту державного управління, м. Маастріхт. –*
8. *http://www.eipa.eu/en/pages/show/&tid=69*
9. *5. Д. Олійник Економічна, соціальна і політичні основи ефективної діяльності органів влади / Д. В.*
10. *Олійник // Теорія та практика державного управління. - 2012. - Вип. 4. - С. 242-250.*

Мирошниченко Наталія Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м.Київ

ДИНАМІКА РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ УКРАЇНИ

З впровадженням новітніх інфокомунікаційних технологій, як показує досвід України і більшості країн СНД, зв'язок може розвиватися випереджаючими економіку темпами, створюючи умови для прискореного економічного і соціального розвитку країни. Так, незважаючи на кількаразовий економічний спад у 1990-2009 роках, галузь зв'язку, в цілому, розвивалася безкризово. Загальний стан галузі зв'язку і рівень задоволення попиту на послуги зв'язку в Україні на кінець 2009 року можна охарактеризувати наступним чином.

Створена цифрова мережа міжнародного та міжміського зв'язку, яка задовольняє попит на ці послуги. Побудовані волоконно-оптичні лінії зв'язку (ВОЛЗ), що з'єднують Україну з усі ма сусідніми держава Протяжність цифрових каналів міжміської та зонових первинних мереж становить близько 85% від загальної протяжності каналів первинної мережі. Україна брала участь у будівництві міжнародних ВОЛЗ як для забезпечення власних потреб, так і з метою забезпечення транзитів через її територію. За останні роки в Україні побудовано близько 39 тис. км ВОЛЗ. Щорічне будівництво ВОЛЗ доведено до 4 тис. км. на рік. Найближчим часом буде закінчено побудову цифрової первинної магістральної мережі України. Розглянемо сучасний розвиток телекомунікацій України на прикладі аналізу діяльності філії Дирекція первинної мережі ВАТ Укртелеком за 2009рік[9,10]. Загальна сума доходів складає 36,7млн.грн.В порівнянні з минулим роком зросли на 16,7%. Сліід зазначити,що функції ДПМ значно ширші ніж у колишнього УКРТЕК. До обслуговування ДПМ раніше була включена зонова первинна мережа, а зараз філії передані для обслуговування сільські з'єднувальні лінії(СЗЛ). Протяжність ліній зв'язку транспортної телекомунікаційної мережі(ТТМ) ВАТ «УКРТЕЛЕКОМ» станом на 01.01.2010 становить 172967км.Утому 280 числі:ВОЛЗ 38143,3км, КЛЗ з металевими провідниками -134823,7км з них СЗЛ 84366,6км.Протяжність РРЛ складає 4617,3км. Протяжність каналів ТТМ по монтованій ємності становить 296371 тис. пот*км, по задіяній ємності 258698,3 тис. пот*км. Відсоток задіяння ємності складає 87,3%.На 01.01.2009 було-70,7.Зміни відбулися в зв'язку з тим, що були організовані тракти 10GbE на міжнародних напрямках,дообладнання мережі DWDM,CWDM,а також розвитку широкосмугового доступу(ШСД) і оптимізації мереж.На ТТМ експлуатуються 1398 НРПВ,з них 758 майданчиків на місцевих мережах, задіяно 1366 елементів транспортної магістральної та зонових мереж,а також 1653 елементи мережі цифрових ВОСП місцевих мереж. Монтована ємність мережі широкосмугового доступу та IP/MPLS Філії становить 1,196 млн. портів які організовані на 2234 майданчиках, із задіяних 5813 елементів мережі. Впродовж 2009 року проведена значна робота для підвищення надійності та потужності транспортної телекомунікаційної мережі. На мережі DWDM проведені роботи з модернізації Західного, Східного,Південного кілець на дільницях Немирів-Дніпропетровськ, Харків- Донецьк.Організовано канали Київ-Львів та Дніпропетровськ -Донецьк. На мережі DWDM також організовано тракти рівня 10 Гбіт/с у напрямках Київ- Братислава, Київ–Відень з підключенням до Інтернет провайдера, Київ–Варшава на дільниці Ковель–Окопи та Київ–Варшава на дільниці Яворів– Корзова. Модернізовано мережу DWDM на обладнанні ECI- 3 кільця та дільниця Немирів-Дніпропетровськ, на дільниці Харків-Донецьк, до мережі DWDM підключено НРПВ Свердловськ. З метою організації додаткових трактів 10GbE та розширення мережі IP/MPLS Донецької,Луганської областей встановлена додаткова платформа XDM-500 в ОРПВ Донецьк. -На мережі CWDM дообладнано діючу мережу в Дніпропетровській та Запоріжській областях.Організовано тракт рівня STM-16.Для забезпечення захисту трафіка GbE для ШСД по обємному кільцю модернізовано 4 НРПВ- Широке,Орджонікідзе ,Марганець,Покровське. Організовано тракт STM-16 на дільницях НРП Солоне-ОРПВ Дніпропетровськ, НРПВ Василівка-ОРПВ Запоріжжя, а також ЦЛТ для потреб Утел. -На мережі SDH в Харківській області модернізована магістраль В11-3 з заміною обладнання Nortel на ECI прикордонного переходу на Росію. У Львівській області перенесено AXD620-2 з ОПП Яворів в ЦЕЗ Яворів.Вивільнені оптичні волокна будуть задіяні для розвитку ШСД. Завершено модернізацію мережі Волинської області У Чернігівській області організовано об'ємне кільце рівня STM-16 з встановленням мультиплексорного обладнання TN-16X,TN-1X ,NN-1C. В Одеській, Кіровоградській та Черкаській областях модернізовано діючу магістраль В4-1Б з подальшим вивільненням мультиплексорів в 5-ти ОРПВ,та TN-1X/4 в 7-ми НРПВ. Модернізовані місцеві мережі міст: Вінниця,Житомир, Луганськ, Миколаїв, Полтава, Суми, Севастополь, Тернопіль, Ужгород, Хмельницький та Ялта. 281 В АР Крим організовано два оптичних тракти між RNC Утел у мм.

Херсон,Запоріжжя,Севастополь та міськими кільцями. Відповідно плану розвитку мобільного зв'язку UMTS, підключено 3 базові станції Утел доТТМ у м.Сімферополь. У Київській області організовано обємне кільце рівня STM-16, на 2-хНРПВ замінено мультиплексорне обладнання на більш потужне.Підключені базові станції Утел до ТТМ у 6-ти населених пунктах Київської області. Для забезпечення потреб мобільного зв'язку UMTS потоками Е1 розроблені та затверджені схеми організації зв'язку в Херсонській, Кіровоградській, Рівенській, Запоріжській, Хмельницькій областях. Розроблені пропозиції до технічного завдання щодо переключення базових станцій філії Утел по м.Києву з SDH-трафіку на IP. Модернізовано схеми синхронізації обємного кільця ВОЛЗ " Вуглик" та "Таврія",що забезпечує більш надійну та стабільну роботу джерел синхронізації 2-го рівня, виконано перепаспортизацію 18 SSU.які розміщуються в зонах технічного обслуговування РЦТЕТТМ-1,2,3,4,5,7. В ЦЛАЦ м. Київ виконано монтаж та тестування джерела синхронізації 2-го рівня OSA 5542B для заміни обладнання синхронізації DCD–521C. На виконання планів ВАТ «Укртелеком» з модернізації мережі IP/MPLS проводився технічний нагляд за монтажем обладнання Juniper в регіональних вузлах МПД та організовано з'єднання між РВ та ЦВ/РТВ. Продовжено роботи з модернізації мережної інфраструктури управління Філії та корпоративної комп'ютерної мережі.Організовано нове зєднання (1Гбіт/с)між мережами Філії та ВАТ «Укртелеком».Перенесено систему управління(СУ) обладнання Lukent Technologies з м.Кривий Ріг до м.Дніпропетровськ. СУобладнання Siemens з м.Херсон до м.Сімферополь. Модернізовано менеджер управління та оновлено програмне забезпечення на СУ мультиплексного обладнання ECI(CWDM,DWDM),а також переконфігуровано СУ обладнанняBG-20. Станом на 01.01.2010 ВОЛЗ побудовано в 550 районних центрах та виділених містах(РЦ,ВМ) з 552.Трафік РЦ і ВМ апаратно захищений використанням обладнання CWDM,SDH,Csco. Розроблено проект плану розвитку ТТМ на 2009-2012 роки. Станом на 01.01.2010 вивільнено з експлуатації 4254,6 км аналогових ліній.Залишились в експлуатації близько 2266,6 км. Метрологічними службами відремонтовано 360 одиниць ЗВТ,виконано перевірку 2625 одиниць ЗВТ та відкалібровано 3461 одиницю. Якісні показники роботи ТТМ за2009 рік відповідали встановленним нормативам. Розвиток ТТМУ не підпорядкований загальному державному плану,а вирішував певні комерційні поточні завдання.

Однак,слід зробити висновок про успішну роботуДПМ з розвитку ТТМ,яка розвивається на сучасних телекомунікаційних технологіях,з врахуванням перспективи розвитку мобільного зв'язку та Інтернету в Україні. Однак треба зауважити ,що все обладнання на ТТМ закордонне,мало узгоджене між собою.Зараз практично Україна не проводить ні наукових,ні промислових робіт з розвитку і виготовлення вітчизняного сучасного телекомутаційного обладнання 282 В Україні успішно працюють ряд фірм.

Так,наприклад,фірма «АТРАКОМ»побудувала біля 20000 км ліній ВОЛЗ і поставляє користувачам оптичні тракти.Але ряд фірм допускають,як конкуренти,неетичні дії.Вони не мають суттєвого контролю з боку держави за системним розвитком і доходить до пошкоджень ліній ВОЛЗ конкурентів.

Література:

1. *В.Цхведиани. Телекоммуникации Украины – перспективы развития и основные проблемы //Фондовый рынок. - No16. – 2000.*
2. *Н. Васильєва. Основні тенденції розвитку ринку інформаційних технологій та комунікацій // Економіст. - No10. – 2000.*
3. *С.О.Довгий. Стан та проблеми розвитку телекомунікаційної мережі України // Наука та наукознавство. - No3. – 2000.*

Лазоренко Анастасія Вячеславівна
Державний уверситет телекомунікацій

Навчально-науковий інститут менеджменту та підприємництва
м.Київ

РОЗВИТОК СУЧАСНИХ ПОСЛУГ

Найбільша частина в обсязі послуг припадає на телефонний зв'язок, яким охоплено близько 13,1 млн. абонентів. Телефонна щільність зараз становить близько 26,4 телефони на 100 мешканців,що перевищує середні показники країн з аналогічним економічним рівнем, однак в 3 рази менша, ніж в розвинутих країнах Загальні результати розвитку галузі телекомунікацій незалежної України можна охарактеризувати таким чином[7]: -з'явися і досяг насичення на рівні 55,3 млн. активованих SIM-карт новий вид телекомунікацій – рухомий (мобільний) радіозв'язок; -з'явився і в останні роки почав швидко розвиватися новий вид телекомунікаційних послуг – доступ до інформаційно-комунікаційних послуг Інтернету; кількість швидкісних підключень до Інтернету досягла 2,1 млн, а кількість користувачів Інтернету біля –10,5 млн. -кількість абонентів мережі фіксованого телефонного зв'язку зросла у 1,8 разу – до 13,1 млн; -міжміський і міжнародний трафік зріс майже у 17 разів (до 11,1 млрд телефонних переговорів на рік [7]). Для об'єктивної оцінки стану розвитку інфокомунікацій(ІКТ) в Україні використуємо методи,що застосовують міжнародні організації(ITU,WEF) і методики їх оцінок. Це індекси NRI [12] та IDI [11] Визнаним в світі є метод рейтингу окремих країн за значеннями узагальненого показника (індексу). Зміна цього індексу у часі та зміна місця країни у переліку країн за значенням індексу, і є оцінкою успіхів окремої країни. Питома вага показників галузі телекомунікацій в шндексі IDI(ICT Development Indeks) становить біля 70%.Він введений ITU,охоплює 11 показників і доволяє оцінити прогрес ІКТ. Оцінка розвитку різних країн світу за індексом NRI(Networked Readiness Indeks) ведеться з 2002 року. У першому звіті WEF(Всесвітній економічний форум), в якому була застосована методика NRI, за 2002-2003 роки було зібрано і проаналізовано показники розвитку ІКТ-сфери 82-х країн світу. Для України тоді індекс NRI склав 2,98 і вона тоді зайняла 70-те місце у рейтингу за значенням NRI. Перше місце у цьому рейтингу посіла Фінляндія з NRI=5,92. У звіті WEF за 2006-2007 роки ІКТ-сферу України оцінено вже значенням NRI=3,46 і вона зайняла 75 місце з 122-х країн світу. Перше місце діталося Данії з NRI=5,71. У останньому звіті WEF за 2008-2009 роки 283 Україна отримала оцінку NRI=3,88 і зайняла 62-ге місце у рейтингу серед 134 країни світу. Перше місце зайняла Данія з NRI=5,85 [7]. Ціновий кошик ІКТ.Фахівцями ITU показники цінової доступності ІКТ- послуг спеціально не були включені як складові до індексу IDI, оскільки цінова доступність ІКТ є дуже важливою оцінкою ІКТ-сфери і, крім того, більш складною у оцінюванні характеристикою. Тому для неї в звіті [26] введено спеціальний вимірюваний показник цінової доступності ІКТ-послуг – "ціновий кошик ІКТ" (ЦК_ІКТ). В цьому показнику комбіновано враховано тарифи на послуги фіксованої та мобільної телефонії і послуги фіксованого швидкісного підключення до Інтернету (ШПІ). Значний розвиток отримали радіотехнології, особливо в частині цифрового мобільного зв'язку. Системою мобільного зв'язку охоплено територію, де проживає близько 95% населення України. Початок будівництва мереж мобільного зв'язку третього та четвертого поколінь і початок перебудови центральних частин ТТМ за принципами NGN, які спостерігаються в Україні означає початок ери NGN в телекомунікаційній галузі. Варто зауважити, що високі техніко-економічні характеристики сучасних засобів телекомунікацій та нездорова конкуренція призвели до масового неефективного будівництва паралельних телекомунікаційних мереж. Потужним зовнішнім фактором впливу на розвиток телекомунікацій України є використання зарубіжного досвіду масового впровадження новітніх засобів телекомунікацій та пов'язане з цим зменшення витрат на будівництво і розвиток телекомунікаційних мереж України. Оператори телекомунікацій України, відстаючи на 4-5 років відносно операторів розвинутих країн, впроваджують на мережах засоби, що вже пройшли масову комерційну апробацію в розвинутих країнах.Відставання України з впровадження нових засобів телекомунікацій добре видно при порівнянні ходу

розвитку сучасних видів зв’язку (мобільного та швидкісного доступу до Інтернету) для розвинутих європейських країн і України (рис.3).[7]. Порівняння ходу розвитку мобільного зв’язку та швидкісних підключень до Інтернету в Германії, Італії, Франції та Україні Щільність швидкісних підключень до Інтернету Італія Германія Франція Роки Щільність мобільного зв’язку Україна Італія Україна Германія Франція Через постачальників телекомунікаційних засобів, а також через власні зв’язки з операторами телекомунікацій розвинутих країн, вітчизняні оператори отримують накопичений там досвід впровадження нових засобів, що зменшує витрати на впровадження нових видів зв’язку і дозволяє підтримувати високу прибутковість нових видів телекомунікаційних послуг за рахунок вищих тарифів, порівнняно з розвинутими країнами. Визначною подією в розвитку телекомунікаційної галузі України став прискорений розвиток у 2003-2005 роках і насичення мереж мобільного (в основному, телефонного) зв’язку. Щільність активованих SIM-карт цих мереж становить 121 на 100 жителів країни, що, наприклад, більше, ніж у Франції, але менше, ніж в Германії та Італії(див.Рис.3). Однак цей успіх дався дорогою ціною – Україна відстала у впровадженні цього виду сучасних послуг майже на 5 років від багатьох країн світу. Крім того, мобільний зв’язок в Україні потребує для свого функціонування і розвитку 2/3 платоспроможності українських споживачів телекомунікаційних послуг. Вього лиш 1/3 цієї платоспроможності приходиться на функціонування і розвиток усіх інших видів телекомунікацій. Ринковий, практично не керований розвиток телекомунікацій в Україні призвів до погіршення цінової доступності телекомунікаційних послуг. За показником “цінового кошика ІКТ“, до якого входять послуги фіксованої і мобільної телефонії, передавання коротких повідомлень (SMS) та швидкісного доступу до Інтернету, Україна сьогодні займає 76-е місце серед 150 країн світу. Цей результат, безумовно, не сприяє зменшенню “цифрового розриву“ України з розвинутими країнами світу, а також ліквідації “цифрового розриву“ всередині країни між окремими верствами населення і бізнесу. Внаслідок цього, конкурентоспроможність України у світовій економіці може погіршуватись. 285 Відсутність цілеспрямованої державної політики в розвитку телекомуінкаційної галузі України, мовчазне віднесення її до категорії окремої галузі економіки, що “автоматично“ дає щорік більші надходження до держбюджету, призвели до згортання планомірних науково-технічних робіт в цій галузі, спрямованих на оптимізацію розвитку телекомуінкацій і інш.Рівень держбюджетного і приватного фінансування цих робіт впав приблизно з 0,5% у 1991 році до 0,01% у 2009 році від обсягів доходів галузі. І це при тому, що доходи галузі протягом 1993-2004 випереджали розвиток економіки за рахунок підвищення середнього рівня тарифів на телекомунікаційні послуги [6]. При розробці шляхів інтеграції у світове і Європейське співтовариство повинні враховуватися: - менший рівень телефонізації і розвитку телекомунікацій і інформаційних мереж; - значна кількість застарілої техніки на мережах зв’язку; - слабка комп’ютеризація; - розвиток зв’язку і Інтернету в регіонах України; - розходження в стані економіки і у рівні добробуту населення. Розвиток ТТМУ повинен враховувати особливості цього стану та розвиток послуг електрозв’язку і попит на них, особливо в частині рухомого зв’язку супутникового і кабельного теле- і радіомовлення, передачі даних, доступу в Інтернет та.підвищення вимог до номенклатури послуг електрозв'язку і до їхньої якості; - покращення індексів розвитку інфокомунікаційих технологій країн IDI, NRI, що потребує подальшого удосконалювання телекомунікаційних і інформаційних технологій і їхньої конвергенції; - посилення ролі державного регулювання діяльності в галузі зв'язку особливо в частині взаємодії мереж, використання і розподілу радіочастотного спектру частот, розподілу ресурсу нумерації, здійснення нагляду за діяльністю в галузі зв'язку, регулювання тарифів.

Література:

1. *«Инновационное развитие» - [Электронный ресурс]http://www.eurasiancommission.org/ru2. «Обзор инновационного развития» - [Электронный ресурс] -*
2. *http://www.kt.kharkov.ua/_upload/file/-/innovation_performance_review_of_ukraine russian_copy.pdf*
3. *«Инновационное развитие» - [Электронный ресурс] - https://creativeconomy.ru/lib/7529*
4. *«Инновационные направления развития» - [Электронный ресурс https://creativeconomy.ru/lib/10064*

Картамишева Олена Водолодимирівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м.Київ

МОДЕЛЬ ПРИСКОРЕНОГО РОЗВИТКУ УКРАЇНСЬКИХ ТЕЛЕКОМУНІКАЦІЙ

Загальний хід розвитку телекомунікацій у державі або регіоні, як відомо, можна промоделювати низкою законів і закономірностей теорії інфокомунікаційного розвитку. Однак їх безпосереднє застосування для оцінки розвитку інфокомунікаційних систем під дією конкретних факторів практично неможливо.

Між тим, при грунтовній розробці стратегій (концепцій) розвитку галузі (видів зв'язку, інфокомунікаційних систем) або при плануванні інноваційних проектів, конче необхідна кількісна оцінка головних очікуваних результатів стратегій, концепцій або проектів (коротко, інновацій). Для таких оцінок необхідний простий і ефективний у застосуванні інструмент у вигляді узагальненої моделі розвитку 293 інфокомунікаційної системи, за допомогою якого можна було б кількісно визначати не тільки кінцеву результативність різних інновацій, але й чисельних їх варіантів, які, як правило, розглядаються на стадіях досліджень і проектування. Часто з цією метою застосовується метод періодизації (дискретизації) прогнозного часу розвитку системи та аналітичного простежування впливу інновації на кожному з часових дискретів.

Таким методом, наприклад, оцінювались прогнозні показники розвитку ЄНСЗ при розробці "Комплексної програми створення ЄНСЗ України до 2010 року". В пропонованій моделі метод часової дикретизації удосконалено урахуванням історичного відтинку часу розвитку основного ресурсу системи, поокремим урахуванням процесів введення нових і виведення зношених ресурсів (потужностей) системи на прогнозному відтинку часу. Крім того, запропоновано наочне графічно-гістограмне подання процесу розвитку системи за основним ресурсним показником. Отримана в результаті такого удосконалення дикретна модель розвитку телекомунікаційної системи уточнює і унаочнює процес її розвитку, а також дає можливість виконати досить точні кількісні розрахунки головних (стратегічних) результатів її розвитку. Пропонована модель використовує спрощене однолінійне подання процесу розвитку телекомунікаційної системи за її провідним ресурсним показником R. В якості такого показника можуть бути узяті, наприклад, ємність мережі зв'язку, протяжність її каналів, кількість терміналів, тощо.

Припускається, що розвиток системи відбувається під дією двох основних процесів: 1) введення нових ресурсів (потужностей) системи; 2) виведення з експлуатації зношених (фізично чи морально) ресурсів. Для наочного кількісного подання процесу розвитку системи, на осі часу (див. рис.10.4) призначається точка відліку історичного та прогнозного відтинків часу системи (t0), починаючи з якої, на систему починає діяти конкретний фактор або інновація. Вліво від точки t0 з певною дискретністю (рік, квартал, місяць) відкладається

історичний час розвитку системи, а вправо – прогнозний час розвитку з тією ж дискретністю. Тривалість історичного відтинку (Ті) приймають рівною віку (часу експлуатації) найстарішого основного ресурсу системи, а тривалість прогнозного відтинку – часу дії оцінюваного фактора або інновації. Над віссю часу на кожному з часових дискретів відкладається гістограмний стовпчик (w, w'), площа якого пропорційна обсягу введених ресурсів системи у відповідному часовому дискреті. Під віссю часу (униз) на прогнозному відтинку часу відкладаються гістограмні стовпчики (s'), площа яких пропорційна виведенню зношених (застарілих) ресурсів системи у відповідному часовому дискреті. Такий графік-гістограма стає точним і наочним поданням кількісно- часового розвитку системи. 294 Дійсно, сума площ ствпчиків у історичному відтинку часу (від t0 –Ті до t0) буде характеризувати розвиток системи за основним ресурсним показником R0 на момент t0. Якщо перемножити площу кожного стовпчика на його відстань у часі від t0, а потім поділити на величину ресурсного показника системи R0, то можна отримати величину середнього віку основного ресурсу системи Тс . По закінченні прогнозного відтинку часу Тр система під впливом досліджуваного фактора або інновації переходить у новий стан свого розвитку, який характеризуватиметься новими величинами основного ресурсного показника R', максимального Ті ' і середнього Тс віку основного ресурсу системи. На рис. 10.5, який ілюструє принцип побудови моделі, стовпчики на окремих відтинках часу мають однакову висоту, що характерно для рівномірного (лінійного) зростання системи за провідним ресурсним показником.

Приблизно такий характер розвитку на протязі вже близько трьох десятиліть має ТМЗК України. Такому характеру розвитку відповідає гранично спрощена (рівномірна) модель розвитку системи. За допомогою такої спрощеної моделі з'являється можливість отримати найпростіші аналітичні залежності стратегічних результатів розвитку телекомунікаційної системи від часу та від параметрів інновації.

Література:

1. Ефективність диверсифікації діяльності телекомунікаційного підприємства [Електронний ресурс] / Є.М. Стрельчук, Н.А. Калугіна // Економіка: реалії часу. Науковий журнал. - 2014. - No 2 (12). - С.28-33. - Режим доступу до журн.: http://economics.opu.ua/files/archive/2014/n2.html.

2. Удосконалення інноваційної діяльності підприємства галузі електрозв'язку [Електронний ресурс] / І.А. Дяченко // Технології та дизайн. - 2014. - No 1. - Режим доступу: nbuv.gov.ua/jpdf/td_2014_1_12.pdf.

Мирошниченко Наталія Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

ВПЛИВ РОЗШИРЕННЯ ЕВРОПЕЙСЬКОГО СОЮЗУ НА РОЗВИТОК УКРАЇНСЬКИХ ТЕЛЕКОМУНІКАЦІЙ

Розширення Європейського Союзу (ЄС) створює якісно нову ситуацію на шляху подальшого технічного, економічного та соціального розвитку України. Границі України стають границями з ЄС. Прямо і нагально постає завдання повноправного входження України до цього Союзу. Як наслідок, уже сьогодні починається підготовчий період до вступу України до ЄС. З точки зору українських телекомунікаційних систем також починається підготовчий період до їх функціонування в телекомунікаційному середовищі країн-членів ЄС, створення якого є одним з найважливіших національних завдань бо в XXI сторіччі сама інформація стає стратегічним ресурсом.

Прийнятий Верховною Радою України Закон "Про телекомунікації", 299 переважна більшість положень якого відповідає чинному європейському законодавству, відкриває

широкі перспективи розвитку вітчизняної телекомунікаційної сфери в її русі до інтеграції телекомунікацій держав Європейської спільноти.

Телекомунікації України, як і інших країнах, виконують три основні функції:

а) надання важливих послуг індивідуального споживання (міжперсональне телеспілкування, інформаційне самозабезпечення, самоосвіта, відпочинок, розваги, тощо);

б) складання частини виробничої інфраструктури (бізнес-зв'язки, реклама, брокераж, просторово-рознесені виробничі процеси, тощо);

в) участь у вдосконаленні соціальної організації суспільства (електронне врядування, осередки громадянського суспільства, екстренна та медична допомога, тощо).

Підготовча ситуація невідпорно потребуватиме швидкого вдосконалення сфери українських телекомунікацій в частині усіх зазначених функцій. Однак причини вдосконалення кожної із них будуть свої. Функція індивідуального споживання послуг зв'язку повинна бути піднята до рівня аналогічного споживання в країнах-членах ЄС. Без цього громадяни України не зможуть себе відчувати рівними з громадянами інших країн ЄС як у спілкуванні, так і в організації персональної інформаційно- комунікаційної сфери. Недостатній рівень споживання послуг зв'язку, особливо їх сучасних видів – мобільного та Інтернет, можуть бути істотною складовою невдоволення населення від вступу до ЄС. Лишати основну масу українських громадян з недорозвиненою системою стаціонарного телефонного зв'язку і з початковим рівнем забезпечення мобільним зв'язком і Інтернет – це означає лишати їх права на сучасні загальнодоступні види зв'язку, права, вже реалізованого в країнах ЄС.

Функція українських телекомунікацій, як складової виробничої інфраструктури, повинна розвиватися випереджаючими економіку України темпами з тим, щоб створювати максимально сприятливі умови швидкого зростання економіки і добробуту українських громадян перед вступом до ЄС. Без наближення рівня життя українських громадян до рівня, хоча б, нових членів ЄС не уникнути масового невдоволення вступом до ЄС, посилення міграційних процесів і соціальної напруги в українському суспільстві. Відомо, що розвиток інформаційно-комунікаційної сфери країни слугує каталізатором її промислового і економічного розвитку. Цю обставину слід сповна використати у даній підготовчій ситуації.

Функція вдосконалення суспільної організації також повинна розвиватися у підготовчому періоді якнайшвидше, оскільки ЄС вимагає від країн-членів більш прозорої, демократичної і соціально спрямованої організації суспільства. Це є однією з основних вимог до країн-кандидатів у члени ЄС. 300 Таким чином, високі вимоги до основних державотворчих функцій українських телекомунікацій перед вступом до ЄС та низький їх сьогоднішній рівень розвитку ставить на порядок денний необхідність розробки і прийняття стратегії швидкого кількісного розвитку (у 3-10 разів на протязі 10-15 років) базових видів зв'язку українських телекомунікацій.

Література:

1. *Покровский В. Человеческое измерение рыночной экономики Пугачев В. П., Соловьев А. И. Введение в политологию. - М.: Аспект-Пресс, 2000. - 275 с.*
2. *Человеческий потенциал: опыт комплексного подхода / За ред. И. Т. Фролова. - М.: Озон. 1999. 176 с. Управління суспільним розвитком: Словник-довідник / За заг. ред. А. М. Михненка, В. Д. Бакуменка; Уклад.: В. Д. Бакуменко, С. О. Борисевич, О. А. Бутрін та ін. - К.: Вид-во НАДУ, 2006. - 248 с.*

Пилипей Анастасія Святославівна

Державний університет телекомунікацій

Навчально-науковий інститут менеджменту та підприємництва

м. Київ

ПРОБЛЕМИ РОЗВИТКУ ГАЛУЗІ ТЕЛЕКОМУНІКАЦІЙ У СУЧАСНИХ УМОВАХ

Сьогодні стає загальновизнаним той факт, що засоби телекомунікацій знаходяться на етапі перетворення, який охопив системи і мережі електрозв'язку та інформаційні послуги, які вони надають. Розвиток галузі телекомунікацій визначається лібералізацією та глобалізацією ринку телекомунікації. Лібералізація зумовлена переходом від монопольної структури надання послуг до конкурентного середовища і, як наслідок, зростанням кількості операторів недержавної або змішаної форм власності та кількістю мереж, заснованих на сучасних технологіях.

Основними пріоритетами розвитку галузі зв'язку в Україні є:

• забезпечення розвитку телефонних мереж шляхом завершення створення цифрових мереж, прискорення переобладнання існуючих мереж на базі новітніх технологій і цифрового обладнання;

• впровадження нових видів послуг та нових технологій оброблення, перевезення і доставки усіх видів поштових відправлень на основі комплексної механізації та автоматизації виробничих процесів у поштовому зв'язку, використанні комп'ютерних методів оброблення повідомлень;

• дослідження, розробка та впровадження нових принципів організації зв'язку, організація розроблення та виробництва в Україні основних видів технічних засобів зв'язку на рівні європейських і світових стандартів якості.

Виконання таких завдань ставить нові вимоги по кадровому забезпеченню та науково- технічному розвитку галузі. Перед закладами освіти постає задача підготовки, перепідготовки та підвищення кваліфікації фахівців для галузі телекомунікацій, де освітянський рівень працівників галузі, сформований ще 10-20 років тому, не відповідає зростанню технологічної бази та новітніх засобів телекомунікацій. Особливо гостро проблема підготовки фахівців стоїть для підгалузі поштового зв'язку. Підготовкою спеціалістів для поштового зв'язку не займається жодна установа вищої освіти в Україні. Серед керівних та інженерно-технічних робітників підгалузі поштового зв'язку дуже низька доля фахівців з вищою освітою з поштового зв'язку (менше 3 %). Незважаючи на те, що галузь телекомунікацій та інформаційних технологій надзвичайно капітало- та науковомістка і в неї вже залучено значні суми, цих інвестицій замало, враховуючи потенціал країни. Можна говорити про два моменти, які об'єктивно пояснюють недостатній рівень інвестування в телекомунікації в Україні: незадовільне законодавче забезпечення діяльності інвесторів та слабка державна підтримка цьому процесу.

Отже, потреба України в інвестиціях та становленні сучасного зв'язку може бути забезпечена шляхом об'єднання зусиль усіх структур галузі телекомунікацій, включаючи уряд. Основою для інвестування вітчизняного та іноземного капіталу і кредитів мають стати продумане планування та тісна співпраця учасників галузі. Але відкриття ринку послуг іноземним компаніям у розвинених країнах допускається тільки за мірою достатнього його насичення послугами, що надаються національними операторами. Такий підхід дозволяє підвищити конкурентоспроможність національних операторів, підготувати їх до умов відкритого ринку та уникнути зайняття домінуючих позицій іноземними операторами. Нині ринок інформаційних і телекомунікаційних технологій - один з найбільш прибуткових секторів економіки України, що динамічно розвивається. Проте досягнутий рівень телефонізації досить низький у порівнянні з показниками розвинених країн.

Література:

1. Латік В. Основні показники рівня життя населення // Праця і зарплата, 2005. - №10. - С. 2.

2. Довгаль О.Г. Соціальні послуги , як елемент ринкової інфраструктури //Формування ринкових відносин в Україні, 2003. - № 7-8.

Пилипей Анастасія Святославівна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м.Київ

ПЕРСПЕКТИВЫ И ПРОБЛЕМЫ РАЗВИТИЯ ТЕЛЕКОММУНИКАЦИОННОЙ ОТРАСЛИ

Когда мы обсуждаем обеспечение интернетом удалённых населённых пунктов, где волоконнооптическая связь непозволительно дорога, безусловно, мы должны говорить об использовании относительно новой технологии LTE (4G). Главным фактором продвижения LTE является то, с какой скоростью будут появляться устройства, поддерживающие этот стандарт. Иными словами, скорость развития LTE будет соответствовать скорости проникновения умных устройств. Вместе с тем, взрывной рост умных устройств (смартфоны, планшетные компьютеры) уже заставляет операторов связи активно развивать сети LTE в городах и городских поселениях.

Стоит отметить «МегаФон», который проводит активную и агрессивную рекламную политику, скупает профилирующие компании и, очевидно, видит себя лидером на этом рынке. На данный момент наиболее реальны и интересны конвергентные сервисы. Транспортная инфраструктура позволяет без проблем пропускать потоки данных телевизионного объёма, не говоря уже о данных и голосе. Интеграция услуг данных интернета, голоса и телевидения позволяет создавать ресурсы, сочетающие одновременно интерактивность телевидения и социальную активность потребителя. В данном случае граница между чистыми телекоммуникациями и медийными продуктами размывается. Смотрим в интернете развлекательную программу; тут же, в режиме реального времени, голосуем за участников;«лайкаем» в социальной сети; активно участвуем в форуме, обсуждая программу; через Skype передаём своё мнение в прямом эфире; скидываемся по платежной системе по 100 рублей на новый костюм ведущему, предварительно сделав заказ на одежду у ведущего кутюрье на его социальной страничке – абсолютно реальная картинка. Если границы медийного и телекоммуникационного продукта исчезают, логичным становится размытие такого рода границ между медийным агентством и оператором связи. Не за горами релиз слияния оператора и структуры, создающей медийный контент (телевидение, социальная сеть, образовательные программы, СМИ). Сами строим транспортную сеть, сами гоняем данные, сами готовим продукт.

И здесь возникает первая проблема – операторы не всегда способны оперативно и эффективно создать бизнес-модель, адаптированную к новому формату услуги или сервиса.

Вторая проблема – неспособность оператора, действующего в условиях постоянной ценовой войны с конкурентами, достаточно быстро переориентироваться с голоса на трафик данных. Создать нового рода услуги по передаче данных, адаптировать имеющиеся услуги и извлечь дополнительную прибыль. Следующая проблема, о которой хочется упомянуть, присуща всей российской экономике, независимо от отрасли. Это жёсткая организационная структура операторов и неспособность к гибкости и ускорению принятий решений и реализации. Низкая эффективность на всех уровнях. Низкий уровень компетенции производственного персонала. Отсутствие наработанных аналитических программ, способных монетизировать неструктурированные огромные массивы информации, полученной в результате изучения клиентуры. В локальном масштабе программы, позволяющие анализировать данные, есть у каждого оператора, но о результатах мы почти ничего не знаем. Неуверенность в готовности инвестировать в новые технологии, которые меняются достаточно часто. На смену 3G пришёл стандарт 4G. К 2020 году появится технология 5G со скоростью около 10 000 Мбит/с. И насколько быстро можно будет возвратить инвестиции в строительство новой инфраструктуры и при этом получить прибыль, сказать сложно. Во многом неуверенность основывается на следующем

риске – в отрасли имеет место быть большое регулирующее государственное влияние. На уровне госрегулирования риски становятся глобальными для бизнеса.

***Список використаної літератури*:**

1. International Data Flows: Access to the International On-Line Data Base Market, UN New York, 1983; Transborder Data Flows and Brazil, UN New York, 1983; Transborder Data Flows and Poland, Polish Case Study, UN New York, 1984. K.P. Sauvant. International Transactions in Services: the Politics of Transborder Data Flows, 1986.

Селина Дарья Юрьевна
Государственный Университет Телекоммуникаций
Научно-учебный институт менеджмента и предпринимательства
г.Киев

РАЗВИТИЕ СЕТЕЙ МОБИЛЬНОЙ СВЯЗИ 5G

Появление технологии 5G должно служить преодолению тех вызовов, которые наблюдаются на мобильном рынке, а именно:

1. Рост абонентского и служебного мобильного трафика передачи данных.
2. Потребности в дополнительном спектре.
3. Доступный спектр.
4. Развёртывание беспроводных широкополосных сетей.
5. Анализ новых вызовов рынка.
6. Рост и появление новых потребностей пользователей.

История мобильной связи началась в 1980 г. с 1G — технологии первого поколения, которые предназначались исключительно для предоставления голосовых услуг. Этот этап продлился 10 лет. Затем появилась технологии второго поколения (2G), которые дали возможность внедрения таких сервисов, как СМС и низкоскоростная передача данных. Тогда никто о большем не думал.

Третий этап — развитие сетей третьего поколения (3G). Кроме голоса и текстовых сообщений, появился сервис высокоскоростной передачи данных. Четвертый шаг — сети четвертого поколения (4G). Это более прогрессивная сеть 3G, с повышенной скоростью передачи данных, новыми сервисами и более качественным доступом к голосовым услугам. Работы по изучению 5G начались еще 10 лет назад. Были организованы рабочие группы, которые занимались исследованием рынков, потребностей клиентов и различных отраслей бизнеса. В течение этого времени готовилась база для технологии 5G. Сейчас продолжаются подготовительные работы, и параллельно ведется стандартизация технологии. Завершение стандартизации ожидается в 2018 году, а на Зимних Олимпийских играх в Корее будет запущена первая пресс коммерческая сеть. В этом же году появится оборудование для коммерческой эксплуатации. Полноценный запуск коммерческих сетей планируется в 2020 году.

Удовлетворению каких потребностей будет отвечать 5G? Существует три основных направления. Первое — предоставление абонентам сверхскоростного мобильного широкополосного доступа в интернет. На текущий момент в стандарте уже заложены ожидания к пиковой скорости порядка около 20 Гбит в секунду. Второе направление — это обеспечение работы устройств, которые передают большие объемы информации, и для которых требуется быстрое время реагирования. Например, автономный автомобиль пилотируется удаленно через сеть, самостоятельно передавая информацию в центр управления, где она анализируется и возвращается обратно в автомобиль в виде сигнала для совершения определенного действия. Очень важно обеспечить минимальную задержку

взаимодействия данного устройства и сети. И третий фокус — это подключение большого количества небольших сенсоров с требованием минимального энергопотребления, чтобы время жизни этих устройств было порядка 10 лет.

Технологическое развитие сетей 5G будет направлено на создание ультра-плотных сетей доступа на основе новых видов сигнально-кодовых конструкций, повышающих на порядок спектральную эффективность по сравнению с сетями 4G, на оптимальное управление ресурсами и на полную виртуализацию сетевых функций. Будущее развитие сетей 5G будет связано с использованием облачных технологий, которые потребуют изменения правил регулирования в отрасли и бизнес-моделей, используемых операторами.

Литература:

1. *«Развитие 5G в Украине» - [Электронный ресурс] - https://delo.ua/special/razvitie-5g-v-ukrainebudet-zaviset-ot-biznes-modeli-operatorov-331005/*
2. *«Развитие сетей мобильной связи 5G» - [Электронный ресурс] - https://www.itu.int/en/ITUD/Regional-Presence/CIS/Documents/Events/2014/09_Astana/Sesson_1_Tikhvinskiy_2.pdf*

Марчук Вікторія Ярославівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м.Київ

ПРОБЛЕМИ ПОДАЛЬШОГО РОЗВИТКУ ПІДПРИЄМСТВ ТЕЛЕКОМУНІКАЦІЙ

Постійний розвиток та подальше становлення ринкових відносин ставить свої вимоги до стабільно функціонуючої системи управління на підприємстві. Досягнення бажаного рівня неможливе без розв'язання вже накопичених суперечностей і вирішення проблем в усіх сферах економіки України. Сфера телекомунікацій та її підприємства як складові являють собою стратегічне значення для сталого розвитку й подальшої інтеграції усіх сфер і галузей економіки у процеси світової глобалізації. Це підтверджується вже доведеним міжнародним суспільно-економічним явищем – становленням наступного інформаційно-технологічного способу виробництва.

Управління підприємствами телекомунікацій – складне системне утворення й пов'язане з багатьма змінними, що сприяє виникненню супереч- ностей і проблем усередині системи. Суперечності, в свою чергу, являють собою джерело економічного прогресу, відсутність яких зупинить саме життя людства та його еволюцію, але їх накопичення призводить спочатку до кризи, а потім – до банкрутства підприємства. Виявлення суперечностей і подальше визначення структури проблем можна представити за допомогою принципів, які повинні враховуватись керівниками й фахівцями підприємства при реалізації своєї діяльності.

В умовах динамічного розвитку ринкової економіки зростають вимоги до соціально-економічної адаптованості та відповідного рівня функціонування усіх галузей та сфер економіки України. Прогресивний розвиток науки, техніки і технологій, інноваційність та висока наукомісткість сучасного виробництва висувають особливі вимоги до шляхів розвитку інформаційно-телекомунікаційної сфери.

Сфера телекомунікацій як складова сфери зв'язку та інформатизації має стратегічне значення для сталого розвитку й стабільного функціонування виробничої і соціальної інфраструктури України, що призначена для задоволення потреб фізичних та юридичних осіб, органів державної влади в телекомунікаційних послугах. Це можливо зробити лише за умов стабільної роботи підприємств телекомунікаційної сфери, що спрямована на подальший успішний розвиток. Так підприємства телекомунікацій повинні бути динамічними, адаптивними, швидко реагувати на стрімкий, схильний до кардинальних змін телекомунікаційний ринок. Унаслідок цього інформаційно-телекомунікаційні послуги не

можуть ефективно поширюватись без налагодженого механізму управління даними послугами.

Одним із елементів успіху в цьому процесі є правильно обрана, адаптована до сьогодення система управління й контролю за діяльністю об'єктів економіки, яка врахує всі можливі проблеми, недоліки, суперечності та кризові явища у майбутньому. Це дуже непросте завдання потребує вивчення кола суперечностей і проблем, що виникли на даному етапі та гальмують подальший розвиток підприємств телекомунікацій в Україні. Формування моделі структури проблем управління телекомунікаційними підприємствами допоможе послідовно й детально проаналізувати суперечності та проблеми для їх подальшого розв'язання. Інтеграція цієї структури у систему управління телекомунікаційним підприємством надасть можливість менеджменту підприємства своєчасно реагувати й швидко вирішувати проблеми, що постають у процесі управління життєдіяльністю об'єктом телекомунікаційного ринку.

Питанням дослідження суперечностей і проблем в економіці й філософії присвячено багато робіт: з точки зору системного підходу – О.О. Богданов, зарубіжних та вітчизняних економістів – це А. Файоль, Ф.У. Тейлор, Л.О. Лігоненко, А.А. Чухно, А.В. Кузьмінов, В.М. Орлов, В.М. Гранатуров, П.П. Воробієнко та ін.

Незважаючи на велику кількість наукових досліджень, публікацій і накопичений практичний досвід у теорії і практиці структуризації й розв'язання суперечностей та проблем на необхідному етапі розвитку підприємства, все ще залишаються аспекти, розглянуті недосить повно. Вони стосуються розробки моделі структури проблем для сприяння швидкісному та спрощеному їх вирішенню у сучасних динамічних умовах техніко-технологічного та інформаційного розвитку економіки.

Мета статті є формування моделі структури проблем та суперечностей, необхідної для подальшого вдосконалення системи управління телекомунікаційних підприємств України в сучасних економічних умовах.

Виклад основного матеріалу дослідження. У сучасних умовах недостатній аналіз кола актуальних суперечностей та проблем не дає змогу підприємствам реалізувати ввесь потенціал виробничих, економічно-соціальних і науково-технологічних можливостей з точки зору ефективного виробництва й реалізації кінцевих продуктів телекомунікацій. Ця проблема безпосередньо пов'язана з відсутністю структурного підходу до формування ефективної моделі структури проблем та протиріч, що визначає необхідність вивчення останніх. [1]. Сфера послуги телекомунікаційного ринку в Україні як складова сфери послуг країни на даному етапі відноситься до однієї з найдинамічніших за розвитком сфер економіки. Доходи від надання телекомунікаційних послуг за 9 місяців (січень-вересень) 2014 року порівняно з аналогічним періодом минулого року збільшилися на 2,9 % і склали 36289,0 млн. грн., що становить 92,3 % від загальної кількості доходів від надання послуг зв'язку. [2].

Для розв'язання окресленої проблеми Законом України «Про телекомунікації» (далі – Закон) було введено поняття «загальнодоступні телекомунікаційні послуги» (набір обов'язкових послуг загального користування встановленого рівня якості), які надаються споживачам на всій території України за тарифами, що регулюються державою і встановлені не тільки нижче їх реальної вартості, але інколи й нижче собівартості [3]. Доконечність надання збиткових загальнодоступних телекомунікаційних послуг викликало низку нових техніко-економічних проблем телекомунікаційної сфери, які потребують вчасного вирішення. У першу чергу, йдеться про мотивацію розвитку таких послуг. Із цією метою Законом передбачено необхідність компенсації збитків операторам, що надають загальнодоступні послуги. Створення відповідного механізму компенсації збитків покладено на Кабінет Міністрів України [4].

Після введення в дію Закону пройшло 10 років, проте такий механізм, який відповідав і ринковим принципам, і соціальним інтересам, з різних причин, на жаль, не створено, тому, як вказано, досить гостро стоять проблеми:

- ✓ визначення та обґрунтування загального обсягу витрат, необхідних для компенсації збитків операторам, що надають загальнодоступні послуги;
- ✓ визначення джерел надходження цих коштів;
- ✓ визначення організаційних структур, які акумулюватимуть ці кошти, їх прав та обов'язків;
- ✓ визначення порядку надходження коштів у ці структури;
- ✓ визначення порядку розподілу коштів між операторами, які надають збиткові загальнодоступні телекомунікаційні послуги.

Питання розвитку широкосмугового доступу до мережі Інтернет становить ще одну з проблем, яка викликана швидким зростанням соціальної ролі телекомунікацій у житті українців. Ця проблема у світі вирішується вже відомим шляхом – ще на початок 2012 р. більш ніж 40 країн включили широкосмуговий зв'язок у склад загальнодоступних послуг. За даними звіту Бюро розвитку електрозв'язку (ITU) за 2014 рік, більше 75 % телекомунікацій-ного потоку припадає на вільний широкосмуговий зв'язок Інтернету, тому стрімкий розвиток у світі широкосмугового зв'язку є самою значущою тенденцією у секторі інформаційно-комунікаційних технологій (ІКТ) за останні кілька років. Він суттєво вплинув на способи спілкування, доступу до інформації, обміну досвідом і знаннями, ведення господарської діяльності тощо [5]. Але такий стрімкий розвиток викликав низку проблем соціально-економічної безпеки. Телекомунікаційна сфера та її підприємства потребують, з одного боку, державного регулювання, а з іншого – допомоги, щоб максимізувати вигоди від нових технологій і послуг, але мінімізувати ризики для споживачів та економіки. Система управління телекомунікаційним підприємством є складним утворенням, що зачіпає безліч організаційних і технологічних аспектів телекомунікацій. Рівноважний стан системи, за думкою одного з засновників системного підходу в економіці О.О. Богданова, розглядається не як стійке й назавжди задане, а як «динамічна» або «рухлива» рівновага [6]. Структура системи з'являється як результат боротьби і взаємодії протилежностей (різноспрямованих елементів), а «рухлива рівновага» в цілому – як постійне пристосування до зовнішнього середовища, що змінюється, шляхом неминучих структурних перебудов та зміни одного рівноважного й стійкого стану іншим. Розгляд суперечностей в управлінні, що виникли під впливом об'єктивних дій економічних законів та закономірностей, має дуже молодий досвід. Зміна в способі й швидкості передання інформації завдяки динамічному розвиткові функціонування телекомунікаційного ринку призвело до більш гострого прояву деяких суперечностей і необхідності їх розгляду та вивчення. Економічному протиріччю властиві всі характеристики суперечності взагалі

В той же час це специфічне протиріччя, сутність якого визначається особливостями економічного руху, він не лише зміна, розвиток, але й діяльність людей. В результаті вирішення суперечностей відбувається подальше вдосконалення не лише соціально-економічних, але й організаційно- економічних та техніко-економічних відносин. Ці процеси – рушії прогресу, що супроводжують розвиток виробництва і стимулюють об'єктів телекомунікацій розв'язувати протиріччя. Стосовно техніко-економічних відносин, в умовах застосування високих технологій технологічна й маркетингова діяльність потребує від компаній істотно різних компетенцій персоналу й організації бізнес-процесів, тому на часі використання аутсорсингу в технічному обслуговуванні та підтримці мереж постачальникам обладнання, фахівці останніх є більш компетентними у прийнятті рішень.

Невирішені протиріччя стають бар'єром на шляху зростання ефективності економіки, стримуючи науковий поступ і впровадження нових технологій. Суперечності, що загострилися, переростають у конфлікт інтересів та перешкоджають задоволенню потреб

суб'єктів ринкових відносин. На жаль, таким гострим протиріччям в Україні є недосконаліть державної політики щодо стимулювання розвитку телекомунікаційних підприємств. Зарубіжний досвід показує, що серед заходів сприяння розвитку дієвішим є непряме фінансування – податкові пільги, знижки, позики, присвоєння спектру, надання державних гарантій, стимулювання спільного використання інфраструктури тощо [9]. Пізнання економічного протиріччя передбачає не просто конструювання його дефініції, а визначення й обґрунтування його місця в системі суперечностей. Так, якщо звернутись до критерію міри віддаленості економічних відносин, явищ, законів, в яких протиріччя виявляються, від абстрактно загального початку, цебто міри їх конкретності, то найпростішою є суперечність елементарного відношення власності, яка в один і той же час є привласненням та відчуженням, найскладнішим – протиріччя закону руху економічної системи.

Висновки:

Підхід до вирішення суперечностей і проблем повинен бути цілеспрямований та структурований. У процесі глобалізації національної економіки і в період трансформації ринкових відносин в Україні сфера телекомунікацій як складова сфери зв'язку та інформатизації є головною «артерією», що постачає, обробляє, допомагає споживати інформацію і потребує швидкого реагування на соціально-економічні протиріччя, що виникають, та їх загострення у вигляді проблем. Це можливо зробити, якщо комплексно підійти до системи управління об'єктом телекомунікацій та питання структури проблем на прикладі запропонованої моделі структури проблем.

- ✓ модель формування структури проблем управління об'єктом телекомунікацій зазначена в основному матеріалі дослідження, допоможе менеджменту підприємства структуризувати, зробивши більш ефективним механізм антикризового управління підприємством для стабільного його функціонування за умов поетапного системного підходу:
- ✓ аналіз та діагностика протиріч, їх структуризація, групування щодо виявленої проблемної спрямованості з урахуванням можливості виникнення кризового стану підприємства і загрозою банкрутства;
- ✓ формування проблем відповідно до часових обмежень вирішення проблем за їх спрямованістю, пріоритетністю й ресурсним потенціалом;
- ✓ визначення базового варіанту структури проблем та їх кінцево-цільової спрямованості та зразок оцінки соціально-економічної ефективності базового варіанта структури;
- ✓ коригування за необхідності базового варіанту структури проблем відповідно до визначених принципів згідно з контуром, що веде від блоку 10б знов до 4 блоку оцінки, так як, можливо, потрібна повторна або більш детальна оцінка складових з блоків 2-4;
- ✓ розробка можливих профілактичних засобів запобігання повторенню проблем чи загостренню протиріч.

Це потребує певних дій з боку системи управління підприємствами телекомунікацій в Україні для мотиваційного впливу за допомогою вирішення проблем системи управління на усіх соціально-економічних рівнях об'єкта та приведення останнього на бажаний фінансово- економічний та соціальний рівень. Але це вимагатиме певних, конкретних обмежень на виробництві й використання трудових і матеріальних ресурсів. Слід також зазначити, що в умовах стрімкого розвитку українського телекомунікаційного ринку зростає конечність постійного моніторингу та аналізу отриманих даних на предмет реального стану справ і необхідність своєчасного реагування й усунення протиріч, що зароджуються.

Література:

1. Чекаліна М.А. Принципи стратегічного планування на підприємстві/ М.А. Чекаліна // Вісник ОДУ. – 2009. – № 1. – С. 83-89.
2. Кузьмінов А.В. Узгодження мотиваційних впливів на ефективність механізму управління телекомунікаціями регіону: дис. ... канд. екон. наук: 08.07.04 / А.В. Кузьмінов, Одеська національна академія зв'язку ім. О.С. Попова. – Одеса, 2005. – 224 с.
3. Економіка телекомунікацій: навч. посіб. [для студентів вищих навчальних закладів]; за заг. ред. В.М. Орлова. – О.: ОНАЗ ім. О.С. Попова, 2014. – 512 с.
4. Кравченко А.І. Історія менеджменту: підручник / А.І. Кравченко. – 3-тє вид., перероб. і доп. – М.: КНОРУС, 2010. – 432 с.
5. Лігоненко Л.О. Антикризове управління підприємством: теоретико-методологічні засади та практичний інструментарій / Л.О. Лігоненко. – К.: КНТЕУ, 2001. – 580 с.
6. Чухно А. Сучасна фінансово-економічна криза: природа, шляхи і методи її подолання / А. Чухно // Економіка України. – 2010. – № 1. – С. 4-18.
7. Досягнення сфери зв'язку за січень-вересень 2014 року (вся інформація наведена без урахування даних АРК та м. Севастополя) [Електронний ресурс] / Національна комісія з пи- тань регулювання зв'язку України. – Режим доступу: ttp://www.nkrzi.gov.ua/index.php?r=site/ index&pg=138&language=uk
8. Юшманов В.В. Теорія рівноваги Богданова і Бухаріна, системний підхід і теорія самоорганізації систем / В.В. Юшманов // Новий історичний матеріалізм. – 2005. – № 100. – С. 4-18, С. 92-95. [Електронний ресурс]. – Режим доступу: http://www.situation.ru/app/j_art_1053.htm
9. Смірнов І.К. Формально-логічний і діалектичного протиріччя / І.К. Смирнов // Євразійський міжнародний науково-аналітичний журнал. – 2012. – № 4 (44) – С. 29-33.

Марчук Вікторія Ярославівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м.Київ

ПОЛІТИКА У СФЕРІ СТАНДАРТИЗАЦІЇ ТА ПІДТВЕРЖЕННЯ ВІДПОВІДНОСТІ

Метою стандартизації у сфері телекомунікацій є створення єдиної системи державних стандартів і стандартів галузевого рівня, які визначають вимоги до телекомунікаційних мереж, їх технічних засобів та якості надання телекомунікаційних послуг, а також гармонізація таких вимог з вимогами міжнародних нормативних документів. Пріоритетним напрямом роботи є створення сучасних національних стандартів у сфері телекомунікацій з урахуванням перспективності нових технологій, насамперед гармонізованих з європейськими та міжнародними.

Стандартизація у сфері телекомунікацій повинна відповідати положенням Закону України "Про стандартизацію" (2408-14) і орієнтувати національних виробників на впровадження нових технологій та створення обладнання на базі гармонізованих національних стандартів, а в разі їх відсутності - безпосереднє застосування сучасних міжнародних та європейських стандартів, рекомендацій Міжнародного союзу електрозв'язку та документів інших телекомунікаційних організацій відповідно до вимог законодавства.

Підтвердження відповідності технічних засобів телекомунікацій повинне здійснюватися за технічними регламентами у сфері телекому-нікацій, які розробляються згідно із Законом України «Про підтвердження відповідності» (2406-14) з урахуванням вимог ЄС.

До введення в дію технічних регламентів у сфері телекомунікацій підтвердження відповідності технічних засобів телекомунікацій здійснюватиметься відповідно до вимог нормативних документів державної системи сертифікації продукції.

Висновки

Таким чином, з вышесказанного можна зробити висновок, що надання загальнодоступних послуг забезпечуватиметься шляхом розвитку телефонних мереж відповідно до цієї Концепції.

У разі недостатнього задоволення потреб споживачів на загальнодоступні телекомунікаційні послуги в окремих регіонах України Національна комісія з питань регулювання зв'язку відповідно до Закону може прийняти рішення про покладення на операторів телекомунікацій, які займають монопольне (домінуюче) становище на ринку телекомунікацій і діяльність яких поширюється на всю територію України, обов'язків щодо надання загальнодоступних телекомунікаційних послуг споживачам із застосуванням механізму компенсації збитків.

Література:

1. Воробієнко П.П. Проблеми використання закономірностей впливу ІКТ на економічний розвиток країни [Текст] / П. Воробієнко, В. Гранатуров // Економіка України. – 2011. – № 8. – С. 26-33.

2. Державна служба статистики України [Електронний ресурс]. – Офіційний веб-сайт. – Режим доступу: http://www.ukrstat.gov.ua.

3. Костіна О.В. Тенденції розвитку інформаційного суспільства: аналіз сучасних інформаційних і постіндустріальних концепцій / Електронний журнал "Знання. Розуміння. Уміння" 2009 № 4

Пилипей Анастасія Святославівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м.Київ

ТЕЛЕКОМУНІКАЦІЙНА ГАЛУЗЬ УКРАЇНИ, ПРОБЛЕМИ І ПЕРСПЕКТИВИ

Одна зі стратегічних для будь-якої країни галузей – галузь телекомунікацій – відіграє величезну роль у збалансованому розвитку глобальної та регіональної економіки. Вона є з'єднувальною ланкою як промислової сфери, сфери послуг і споживачів, так і різних географічно розрізнених частин країни та економічних центрів. Стимулюючи людське спілкування за допомогою зв'язку, сучасні засоби телекомунікацій стають необхідною умовою для соціальної згуртованості та культурного розвитку всіх країн.

Вже зараз неймовірно збільшені потоки інформації – телефонні розмови, факсимільна інформація, електонна пошта, масиви даних та телебачення – показують, якою мірою світ стає ще більш залежним від засобів телекомунікацій, які змінюють бізнес, стиль життя, суспільство вцілому. Так, діти в Сінгапурі застосовуть пейджинг або стільниковий телефон для підтримання зв'язків з батьками, а аборигени Австралії продають свій живопис, використовуючи можливості відеоконференції, бразильські банки пропонують свої послуги в мережі Інтернет, а французькі домогосподарки радяться з телефонними компаніями у справі вибору слюсаря. Як бачимо, комунікаційні послуги стирають кордони між культурами, мовами та часом.

У багатьох країнах світу сектор послуг у наш час вже дає близько половини їх валового національного продукту, і ця тенденція не обмежується лише економічно розвинутими державами. В таких різних країнах, як наприклад Сінгапур, Гонконг або Угорщина, сектор послуг забезпечує до 60% економічної активності країни. Навіть у найменш розвинутих країнах частка сектору послуг (43%) перевищує частку сільськогосподарського сектору (37%) або промислового (20%). При цьому вже на початку 90-х років світова частка сфери послуг в економіці становила в середньому близько 60%, а вже протягом наступних років від 70 до 80% економіки розвинутих країн знаходяться під значним впливом інформаційних технологій.

Отже, наприкінці XX ст. – початку XXI ст. світ перебуває в стані інформаційної революції, вплив якої можна порівняти з впливом індустріальної революції минулого століття. Є всі підстави вважати, що обробка інформації – одна з найвагоміших складових економічної активності. Тому можна стверджувати, що розвиток телекомунікацій як важлива складова інформатизації суспільства та забезпечення населення високоякісними

послугами зв'язку є одним з найважливіших напрямів національного та економічного розвтку будь-якої держави, і, зокрема, України.

Література:

1. В.Цхведиани. Телекоммуникации Украины – перспективы развития и основные проблемы // Фондовый рынок. - №16. – 2000.
2. Н. Васильєва. Основні тенденції розвитку ринку інформаційних технологій та комунікацій // Економіст. - №10. – 2000.
3. С.О.Довгий. Стан та проблеми розвитку телекомунікаційної мережі України // Наука та наукознавство. - №3. – 2000.

Пилипей Анастасія Святославівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

СТАН ТА ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ УКРАЇНИ

Одним з найдинамічніших за останні роки сегментів українського телекомунікаційного ринку є мобільний зв'язок. Причому як з точки зору зовнішніх впливів на галузь, так і з точки зору взаємовідношень між суб'єктами ринку. Але довготривала економічна криза та нестабільність вітчизняного законодавства суттєво пригальмувала розвиток українського ринку мобільного зв'язку. Однак, як і інших галузей економіки. Більш того, мобільний зв'язок, як один з найприбутковіших напрямів діяльності, потрапив під пильну увагу контролюючих, інспектуючих та інших подібних "експроприюючих" органів. За останні роки спостерігалися спроби накласти як на суб'єктів ринку, так і на його споживачів різного роду додаткові збори, податки, акцизи і т.д. Це аж ніяк не сприяє розвитку галузі. Але все ж таки на сьогоднішній день можна сказати, що український ринок мобільного зв'язку поступово набуває цивілізованих рис, незважаючи на активну боротьбу (а, можливо, і завдяки їй) п'яти мобільних операторів зв'язку (UMC, KyivStar GSM, DCC, Wellcom, Golden Telecom GSM) за невелику частину платоспроможної клієнтури.

Також порівняно динамічною сферою українських телекомунікацій можна назвати Інтернет. Загальна кількість користувачів Інтернетом в Україні на початок 1999 року становила приблизно 100-120 тис. У відношенні до загальної кількості користувачів у світі вона складає менше 0,1% або, точніше, 0,065%. Але в середньому за кожні шість місяців кількість користувачів збільшується в 1,67 раза, що вище середніх темпів зростання у світі в цілому. Зараз мають місце такі прогнозні коефіцієнти росту кількості українських користувачів Інтернетом: 2002 р. – 1,5; 2003 р. – 1,5; 2004 р. – 1,4; 2005 р. – 1,4. Необхідно зазначити, що скільки існує та розвивається вітчизняний сегмент Інтернету, впадає в око один не дуже приємний факт – складається враження, що "існує та розвивається" він тільки у Києві. В інші регіони протягнено лише невеличкі джерела виділених каналів від крупних київських провайдерів. Але не слід забувати, що перші виділені канали, наприклад, з'явились не в Києві, а в Харкові, що помітна частина найкращих інформаційних ресурсів України знаходиться не тільки у Києві, але й в Одесі, Донецьку, Дніпропетровську.

Щодо сегмента електрозв'язку, то рівень телефонізації в Україні на сьогодні у два рази нижчий, ніж у країнах Центральної та Західної Європи. Із загальної кількості діючих у телефонній мережі АТС 21,1% належать електронним та квазіелектронним, решта – морально застарілим аналоговим. Щільність телефонного зв'язку, як вже зазначалося, становить близько 20,1 телефонів на 100 осіб. Кількість основних телефонних номерів складає в Україні близько 9 млн., з яких 86,6% встановлено у міських телефонних мережах, 13,4% - у сільських. Подальша телефонізація населених пунктів з низьким показником кількості телефонних номерів через низьку платоспроможність у таких регіонах триває

повільно – в цілому по країні показники телефонізації зростають за рахунок, знову ж таки, Києва та інших великих міст.

Взагалі, характерною особливістю української телекомунікаційної галузі є значне відставання за часом по застосуванню нових технологій між Києвом та іншими регіонами країни. Наприклад, мобільний зв'язок у Харкові з'явився через 2-3 роки після його появи у Києві, а в деяких великих містах з населенням в 25 і більше тис. людей він відсутній і досі. Мобільним зв'язком покрито усього біля 25% території України.

Слід зазначити також, що ринок телекомунікацій в Україні характеризується високим рівнем монополізму. "Укртелеком", "Утел", UMC, "Укрпошта" – їх сумарна частка у структурі даних послуг становить 90 %. Як вважає Інтернет Асоціація України, зараз практично всі недержавні учасники телекомунікаційного ринку у тій чи іншій мірі потерпають від монопольного становища ВАТ "Укртелком".

Для світового телекомунікаційного ринку характерні процеси інтеграції та глобалізації, тому що в цілому світовий ринок стає все більш інтегрованим. А Україна, нажаль, часто не може налагодити роумінг у масштабах країни. Україна повинна мати стратегічних партнерів. Ці партнери повинні бути у Європі, Америці, Азії. Бажаним для України є входження до одного з глобальних об'єднань.

Проблемою розвитку телекомунікацій в Україні також є наявність близько 70% аналогових АТС від їхньої загальної кількості. На модернізацію вітчизняних комунікацій потрібно близько 19 млрд. дол. В Україні капітальні інвестиції в розвиток телекомунікацій складають лише 0,3% ВВП. Для порівняння, у Німеччині – 4,8%, у Франції – 3,1%.

Отже, як бачимо, стан галузі телекомунікацій України особливо не вражає, але оскільки, як було зазначено раніше, розвиток телекомунікацій має величезну роль у загальному економічному розвитку країни, то як урядовим, так і неурядовим організаціям необхідно вживати усіх можливих заходів щодо сприяння такому розвитку, зокрема, аби підвищити конкурентоспроможність України в цій галузі.

Література:

1. О состоянии телекоммуникационного рынка Украины //www.cdmaua.com/russian/telecom.shtml

2. О. Шевчук. О телекоммуникаций Украины //www.fas.com.ua/14_06_00/brams.html

3. Ю.Соловйов, консультант "Телесистеми України" о рынке телекоммуникаций Украины //www.niss.gov.ua/iso/Table/Litvin1/03.htm

Пилипей Анастасія Святославівна

Державний університет телекомунікацій

Навчально-науковий інститут менеджменту та підприємництва

м. Київ

ПРОБЛЕМИ РОЗВИТКУ ГАЛУЗІ ТЕЛЕКОМУНІКАЦІЙ У СУЧАСНИХ УМОВАХ

Сьогодні стає загальновизнаним той факт, що засоби телекомунікацій знаходяться на етапі перетворення, який охопив системи і мережі електрозв'язку та інформаційні послуги, які вони надають.

Розвиток галузі телекомунікацій визначається лібералізацією та глобалізацією ринку телекомунікації. Лібералізація зумовлена переходом від монопольної структури надання послуг до конкурентного середовища і, як наслідок, зростанням кількості операторів недержавної або змішаної форм власності та кількістю мереж, заснованих на сучасних технологіях.

Основними пріоритетами розвитку галузі зв'язку в Україні є:

• забезпечення розвитку телефонних мереж шляхом завершення створення цифрових мереж, прискорення переобладнання існуючих мереж на базі новітніх технологій і цифрового обладнання;

• впровадження нових видів послуг та нових технологій оброблення, перевезення і доставки усіх видів поштових відправлень на основі комплексної механізації та автоматизації виробничих процесів у поштовому зв'язку, використанні комп'ютерних методів оброблення повідомлень;
• дослідження, розробка та впровадження нових принципів організації зв'язку, організація розроблення та виробництва в Україні основних видів технічних засобів зв'язку на рівні європейських і світових стандартів якості.

Виконання таких завдань ставить нові вимоги по кадровому забезпеченню та науково-технічному розвитку галузі. Перед закладами освіти постає задача підготовки, перепідготовки та підвищення кваліфікації фахівців для галузі телекомунікацій, де освітянський рівень працівників галузі, сформований ще 10-20 років тому, не відповідає зростанню технологічної бази та новітніх засобів телекомунікацій.

Особливо гостро проблема підготовки фахівців стоїть для підгалузі поштового зв'язку. Підготовкою спеціалістів для поштового зв'язку не займається жодна установа вищої освіти в Україні. Серед керівних та інженерно-технічних робітників підгалузі поштового зв'язку дуже низька доля фахівців з вищою освітою з поштового зв'язку (менше 3 %).

Незважаючи на те, що галузь телекомунікацій та інформаційних технологій надзвичайно капітало- та науковомістка і в неї вже залучено значні суми, цих інвестицій замало, враховуючи потенціал країни. Можна говорити про два моменти, які об'єктивно пояснюють недостатній рівень інвестування в телекомунікації в Україні: незадовільне законодавче забезпечення діяльності інвесторів та слабка державна підтримка цьому процесу.

Отже, потреба України в інвестиціях та становленні сучасного зв'язку може бути забезпечена шляхом об'єднання зусиль усіх структур галузі телекомунікацій, включаючи уряд. Основою для інвестування вітчизняного та іноземного капіталу і кредитів мають стати продумане планування та тісна співпраця учасників галузі. Але відкриття ринку послуг іноземним компаніям у розвинених країнах допускається тільки за мірою достатнього його насичення послугами, що надаються національними операторами. Такий підхід дозволяє підвищити конкурентоспроможність національних операторів, підготувати їх до умов відкритого ринку та уникнути зайняття домінуючих позицій іноземними операторами.

Нині ринок інформаційних і телекомунікаційних технологій - один з найбільш прибуткових секторів економіки України, що динамічно розвивається. Проте досягнутий рівень телефонізації досить низький у порівнянні з показниками розвинених країн.

Література:

1. *Латік В. Основні показники рівня життя населення // Праця і зарплата, 2005. - №10. - С. 2*
2. *Довгаль О.Г. Соціальні послуги , як елемент ринкової інфраструктури //Формування ринкових відносин в Україні, 2003. - № 7-8.*

Пилипей Анастасія Святославівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

ПЕРСПЕКТИВЫ И ПРОБЛЕМЫ РАЗВИТИЯ ТЕЛЕКОММУНИКАЦИОННОЙ ОТРАСЛИ

Когда мы обсуждаем обеспечение интернетом удалённых населённых пунктов, где волоконнооптическая связь непозволительно дорога, безусловно, мы должны говорить об использовании относительно новой технологии LTE (4G). Главным фактором продвижения LTE является то, с какой скоростью будут появляться устройства, поддерживающие этот

стандарт. Иными словами, скорость развития LTE будет соответствовать скорости проникновения умных устройств. Вместе с тем, взрывной рост умных устройств (смартфоны, планшетные компьютеры) уже заставляет операторов связи активно развивать сети LTE в городах и городских поселениях.

Стоит отметить «МегаФон», который проводит активную и агрессивную рекламную политику, скупает профилирующие компании и, очевидно, видит себя лидером на этом рынке.

На данный момент наиболее реальны и интересны конвергентные сервисы. Транспортная инфраструктура позволяет без проблем пропускать потоки данных телевизионного объёма, не говоря уже о данных и голосе. Интеграция услуг данных интернета, голоса и телевидения позволяет создавать ресурсы, сочетающие одновременно интерактивность телевидения и социальную активность потребителя. В данном случае граница между чистыми телекоммуникациями и медийными продуктами размывается. Смотрим в интернете развлекательную программу; тут же, в режиме реального времени, голосуем за участников;«лайкаем» в социальной сети; активно участвуем в форуме, обсуждая программу; через Skype передаём своё мнение в прямом эфире; скидываемся по платежной системе по 100 рублей на новый костюм ведущему, предварительно сделав заказ на одежду у ведущего кутюрье на его социальной страничке – абсолютно реальная картинка.

Если границы медийного и телекоммуникационного продукта исчезают, логичным становится размытие такого рода границ между медийным агентством и оператором связи. Не за горами релиз слияния оператора и структуры, создающей медийный контент (телевидение, социальная сеть, образовательные программы, СМИ). Сами строим транспортную сеть, сами гоняем данные, сами готовим продукт.

И здесь возникает **первая проблема** – операторы не всегда способны оперативно и эффективно создать бизнес-модель, адаптированную к новому формату услуги или сервиса. **Вторая проблема** – неспособность оператора, действующего в условиях постоянной ценовой войны с конкурентами, достаточно быстро переориентироваться с голоса на трафик данных. Создать нового рода услуги по передаче данных, адаптировать имеющиеся услуги и извлечь дополнительную прибыль.

Следующая проблема, о которой хочется упомянуть, присуща всей российской экономике, независимо от отрасли. Это жёсткая организационная структура операторов и неспособность к гибкости и ускорению принятий решений и реализации. Низкая эффективность на всех уровнях. Низкий уровень компетенции производственного персонала.

Отсутствие наработанных аналитических программ, способных монетизировать неструктурированные огромные массивы информации, полученной в результате изучения клиентуры. В локальном масштабе программы, позволяющие анализировать данные, есть у каждого оператора, но о результатах мы почти ничего не знаем.

Неуверенность в готовности инвестировать в новые технологии, которые меняются достаточно часто. На смену 3G пришёл стандарт 4G. К 2020 году появится технология 5G со скоростью около 10 000 Мбит/с. И насколько быстро можно будет возвратить инвестиции в строительство новой инфраструктуры и при этом получить прибыль, сказать сложно. Во многом неуверенность основывается на следующем риске – в отрасли имеет место быть большое регулирующее государственное влияние. На уровне госрегулирования риски становятся глобальными для бизнеса.

Література:

1. International Data Flows: Access to the International On-Line Data Base Market, UN New York, 1983; Transborder Data Flows and Brazil, UN New York, 1983; Transborder Data Flows and Poland, Polish Case

Study, UN New York, 1984. K.P. Sauvant. International Transactions in Services: the Politics of Transborder Data Flows, 1986.

Селина Дарья Юрьевна
Государственный Университет Телекоммуникаций
Научно-учебный институт менеджмента и предпринимательства
г.Киев

РАЗВИТИЕ СЕТЕЙ МОБИЛЬНОЙ СВЯЗИ 5G

Появление технологии 5G должно служить преодолению тех вызовов, которые наблюдаются на мобильном рынке, а именно:

1.Рост абонентского и служебного мобильного трафика передачи данных.

2.Потребности в дополнительном спектре.

3.Доступный спектр.

4.Развёртывание беспроводных широкополосных сетей.

5.Анализ новых вызовов рынка.

6.Рост и появление новых потребностей пользователей.

7.Разработка новых технологий

На каком этапе сейчас находится развитие технологии 5G в мире?

Рассказ о 5G стоит начинать с того, как все страны мира двигаются к связи пятого поколения. История мобильной связи началась в 1980 г. с 1G — технологии первого поколения, которые предназначались исключительно для предоставления голосовых услуг. Этот этап продлился 10 лет.

Затем появилась технологии второго поколения (2G), которые дали возможность внедрения таких сервисов, как СМС и низкоскоростная передача данных. Тогда никто о большем не думал. Третий этап — развитие сетей третьего поколения (3G). Кроме голоса и текстовых сообщений, появился сервис высокоскоростной передачи данных. Четвертый шаг — сети четвертого поколения (4G). Это более прогрессивная сеть 3G, с повышенной скоростью передачи данных, новыми сервисами и более качественным доступом к голосовым услугам.

Работы по изучению 5G начались еще 10 лет назад. Были организованы рабочие группы, которые занимались исследованием рынков, потребностей клиентов и различных отраслей бизнеса. В течение этого времени готовилась база для технологии 5G.

Сейчас продолжаются подготовительные работы, и параллельно ведется стандартизация технологии. Завершение стандартизации ожидается в 2018 году, а на Зимних Олимпийских играх в Корее будет запущена первая пресс коммерческая сеть. В этом же году появится оборудование для коммерческой эксплуатации. Полноценный запуск коммерческих сетей планируется в 2020 году.

Удовлетворению каких потребностей будет отвечать 5G?

Существует три основных направления.

Первое — предоставление абонентам сверхскоростного мобильного широкополосного доступа в интернет. На текущий момент в стандарте уже заложены ожидания к пиковой скорости порядка около 20 Гбит в секунду.

Второе направление — это обеспечение работы устройств, которые передают большие объемы информации, и для которых требуется быстрое время реагирования. Например, автономный автомобиль пилотируется удаленно через сеть, самостоятельно передавая информацию в центр управления, где она анализируется и возвращается обратно в

автомобиль в виде сигнала для совершения определенного действия. Очень важно обеспечить минимальную задержку взаимодействия данного устройства и сети.

И третий фокус — это подключение большого количества небольших сенсоров с требованием минимального энергопотребления, чтобы время жизни этих устройств было порядка 10 лет.

Технологическое развитие сетей 5G будет направлено на создание ультра-плотных сетей доступа на основе новых видов сигнально-кодовых конструкций, повышающих на порядок спектральную эффективность по сравнению с сетями 4G, на оптимальное управление ресурсами и на полную виртуализацию сетевых функций.

Будущее развитие сетей 5G будет связано с использованием облачных технологий, которые потребуют изменения правил регулирования в отрасли и бизнес-моделей, используемых операторами.

Литература:

1. *«Развитие 5G в Украине» - [Электронный ресурс] - https://delo.ua/special/razvitie-5g-v-ukraine-budet-zaviset-ot-biznes-modeli-operatorov-331005/*
2. *«Развитие сетей мобильной связи 5G» - [Электронный ресурс] - https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2014/09_Astana/Sesson_1_Tikhvinskiy_2.pdf*

Селина Дарья Юрьевна

Государственный Университет Телекоммуникаций

Научно-учебный институт менеджмента и предпринимательства

г.Киев

РАЗВИТИЕ СЕТЕЙ И ИННОВАЦИОННЫХ УСЛУГ

Инновационные сети – это профессиональные объединения инфраструктурных организаций, деятельность и услуги которых связаны с коммерциализацией и передачей технологий, созданием и управлением инновационными старт-ап компаниями, инновационным развитием. Основная функция, которую обеспечивает сетевое взаимодействие таких организаций – это распространение информации разного рода и в различных формах.

К такой информации относятся: методы и технологии осуществления деятельности/предоставления услуг, технологические запросы/предложения по поиску партнеров, примеры лучшей практики и т.д.

В современной конкурентоспособной экономике основанные на знаниях инновации являются основой экономического развития.

Устойчивый экономический рост и повышение уровня жизни могут быть достигнуты только за счет повышения производительности труда и внедрения новых и более качественных продуктов и услуг, успешно конкурирующих на мировом рынке.

Важность инноваций признается во многих правовых и политических документах, в том числе на самом высоком уровне. Однако все еще отсутствует целостное видение национальной инновационной системы, ее различных компонентов и их взаимодействия.

Преобладает узкое толкование инноваций, в котором подчеркиваются лишь технологические аспекты. В политике большое внимание уделяется подсистемам науки и инновационных посредников, однако значительно меньший акцент делается на необходимости поощрения инновационной деятельности в подсистеме бизнес-предприятий, в особенности малых и средних предприятий, являющихся важной движущей силой экономического развития.

Недостаточно рассматриваются связи между подсистемами, в том числе между наукой и бизнес-сектором, которые являются ключевыми для определения стратегии в области науки, технологий и инноваций.

Эффективная координация является одной из основных задач управления инновационной деятельностью. Несмотря на прогресс, достигнутый в ходе административных реформ, мера ответственности ключевых участников все еще четко не определена.

Выделяемые ресурсы часто не соответствуют полученным полномочиям.

Связанная с инновациями деятельность распределена между различными государственными организациями, однако единый координирующий орган отсутствует. Существуют вертикальные механизмы координации (от агентств к министерствам и правительству), но горизонтальная координация недостаточно развита или отсутствует.

Инновационное развитие отрасли в существенной мере зависит от уровня инновационных изменений на мировом рынке, от предпринимательских действий субъектов управления торговых предприятий, уровня конкурентоспособности, объемов получаемой прибыли в процессе реализации инновационной стратегии.

В современном мире инновации являются незаменимым элементом функционирования и поступательного развития экономики, без инновационной составляющей невозможно добиться эффективного развития производственной и непроизводственной сфер хозяйства.

В XXI веке разработка и внедрение инновационных технологий в сферах производства и обращения, новых методов организации и управления предприятиями стали ключевыми факторами рыночной конкуренции, мощным средством повышения эффективности деятельности и улучшения качества товаров и оказания услуг.

Література:

1. *«Инновационное развитие» - [Электронный ресурс] - http://www.eurasiancommission.org/ru/act/prom_i_agroprom/dep_prom/SiteAssets/%D0%95%D0%B2%D1%80%D0%BE%D0%BF%D0%B5%D0%B9%D1%81%D0%BA%D0%B8%D0%B5%20%D1%81%D0%B5%D1%82%D0%B8.pdf*
2. *«Обзор инновационного развития» - [Электронный ресурс] - http://www.kt.kharkov.ua/_upload/file/-/innovation_performance_review_of_ukraine-russian_copy.pdf*
3. *«Инновационное развитие» - [Электронный ресурс] - https://creativeconomy.ru/lib/7529*
4. *«Инновационные направления развития» - [Электронный ресурс] - https://creativeconomy.ru/lib/10064*

Селина Дарья Юрьевна

Государственный Университет Телекоммуникаций

Научно-учебный институт менеджмента и предпринимательства

г. Киев

ВНЕДРЕНИЕ И РАЗВИТИЕ 4G

Как только украинские мобильные операторы начали разворачивать сети 3G, в стране заговорили о новом этапе развития — внедрении 4G, или, как ещё называют эту технологию, LTE. Так как за рубежом 4G начали массово развивать с 2010 года, Украине в очередной раз приходится быть в роли догоняющего.

Как и в случае с 3G, внедрение нового поколения мобильной связи в Украине не обходится без преодоления бюрократических препятствий. "Если бы украинское телеком-законодательство позволяло операторам перераспределить между собой частоты в рамках диапазона, то 4G был бы в Украине много лет назад вместо 3G, — объясняет Екатерина Карасёва, старший юрист юридической компании Juscutum. — Но тендер по 4G стал возможным только благодаря договорённости "большой тройки" мобильного рынка о "рефарминге" — отказе операторов от частот в диапазоне 1,8 ГГц и перераспределении диапазона на отдельные части-лоты, некоторые из которых выставляются на аукцион". То

есть, по её словам, "большой тройке" пришлось согласиться на аукционные траты на выкуп частично собственных же частот.

Кроме внедрения 4G перед операторами также стоит задача распространить покрытие сетями нового поколения на большую часть территории Украины, то есть вывести технологии "в поля", за пределы больших населённых пунктов. Но есть проблема — отсутствие принципа технологической нейтральности, который позволяет оператору самостоятельно решать, для какой технологии использовать свои частоты. Вместо этого в Украине в лицензии на частоты закрепляется конкретная технология — например, 3G за спектром 2,1 ГГц. Поэтому развернуть сети нового поколения на частоте 0,9 ГГц с покрытием почти всей территории страны пока не представляется возможным.

"Принцип технологической нейтральности — то, что необходимо телеком-рынку Украины, чтобы преодолеть технологический разрыв со странами ЕС и мира. Если в нашей стране будет законодательно закреплён этот принцип, все новые услуги и технологии начнут внедряться гораздо быстрее, и в технологическом плане Украина сможет наверстать отставание от других стран", — считает Чернышов. Чтобы сказанное стало реальностью, необходимо подкорректировать закон о радиочастотном ресурсе. И соответствующая работа уже ведётся.

С тем, что технологическая нейтральность полезна для рынка, сложно не согласиться. Однако у игроков со второй и третьей рыночной долей есть некоторые предостережения. "В Украине более 50% диапазона 0,9 и 1,8 ГГц находится в руках одной компании, в такой ситуации внедрение технейтральности работало бы на интересы одного оператора и привело бы к монополизации рынка. Поэтому государство приняло решение о рефарминге (обмене частотами), что позволит перераспределить частоты между операторами и затем внедрять технейтральность", — объясняет Андрей Отрощенко. Примечательно, что в сложившейся ситуации крупнейший игрок рынка "Киевстар" ради 4G даже согласился поделиться своими ресурсами в диапазоне 1,8 ГГц с конкурентами.

Связь 4G откроет новые возможности для малого и среднего бизнеса, современных отраслевых решений, таких как M2M/IoT, Smart-Home, Smart-City, e-Education, e-Government, m-Health и т.д. Что, в свою очередь, будет способствовать развитию экономики и созданию новых рабочих мест, считают в Киевстар. «В результате запуска новых технологий рынок получает новый импульс для развития, государство — больше отчислений в виде налогов от новых услуг, абоненты — больше возможностей для коммуникаций.

Для абонентов сотовых операторов появление 4G сетей будет означать увеличение скорости передачи данных и, в теории, благодаря 1800 МГц частотам, улучшение покрытия по сравнению с уже имеющимися 3G-сетями. Однако это улучшение не будет столь значимым, считают эксперты и, вполне возможно, скоро сойдет на нет.

К тому же, еще 3G заработал у нас не на полную мощность и пользоваться мобильным интернетом затруднительно порой не только «в поле», но и в столице. Сами операторы пеняют на чрезмерную зарегулированность рынка. В частности, в Украине все разрешения заточены под использование конкретной технологии — GSM-частоты нельзя использовать для 3G и, тем более, для 4G. То же самое с частотами, выданными под 3G.

Даже если подобные амбициозные планы удастся быстро воплотить в жизнь, мобильным операторам вряд ли придётся долго почивать на лаврах. Новые вызовы перед ними поставит следующее поколение связи 5G, массовое распространение которого по миру ожидается с 2020 года. Если сегодня мобильные операторы и государство сумеют действовать сообща в интересах рынка, стандарт 5G Украина уже сможет внедрить вместе со всем цивилизованным миром без отставания на десятилетия

Література:

1. *«Внедрение стандарта связи 4G» - [Электронный ресурс] - https://focus.ua/money/391179/*

2. *«4G в Украине» - [Электронный ресурс] - https://ubr.ua/ukraine-and-world/technology/razrjazhennye-smartfony-i-levye-diapazony-kakoj-4g-poluchat-ukraintsy-3856084*

Селина Дарья Юрьевна
Государственный Университет Телекоммуникаций
Научно-учебный институт менеджмента и предпринимательства
г. Киев

СОВРЕМЕННЫЕ ПОДХОДЫ К УПРАВЛЕНИЮ В ЧАСТНЫХ И ГОСУДАРСТВЕННЫХ СЕКТОРАХ

Важную роль в инвестиционном обеспечении научно-инновационных программ и проектов во всем мире играют государственные источники финансирования. Основным аргументом в поддержку тезиса о необходимости государственного финансирования научных исследований является существование «провалов рынка», не обеспечивающих для частного сектора достаточных стимулов для инвестирования в научные разработки в общественно оптимальных масштабах. Эти «провалы» обусловлены как возможностью использования результатов исследований другими экономическими агентами, что создает разрыв между показателями коммерческой и общественной эффективности инвестиций в НИОКР, а также высокими рисками инвестиций в НИОКР, которые большинство частных фирм не в состоянии эффективно диверсифицировать.

Государственный менеджмент представляет собой организацию процесса эффективного управления в рамках государственных учреждений. Его основополагающим принципом является переориентация работы госструктур на достижение конкретных результатов и качественное удовлетворение потребностей населения.

На сегодняшний день финансирование программ осуществляется исходя из объема необходимых на те или иные нужды денежных средств, фактический результат их освоения является второстепенным фактором и зачастую заставляет желать лучшего.

Это происходит в силу бюрократического стиля управления, при котором работа чиновников нацелена на четкое выполнение инструкций и собственное продвижение по иерархической лестнице. Отсутствие конкуренции в государственном секторе позволяет не беспокоиться о качестве предоставляемых услуг. Государственный менеджмент подразумевает отказ от бюрократического стиля поведения чиновников и внедрение предпринимательского подхода к обслуживанию населения, что требует расширения полномочий служащих нижнего звена , а вместе с тем и увеличения ответственности за результаты проделанной работы.

Еще одним важным принципом государственного менеджмента является децентрализация оказания услуг населению и внедрение конкурентной борьбы путем наделения одинаковыми полномочиями нескольких органов. Как вариант, может быть использована передача некоторых направлений государственной деятельности в частные руки предприятий как большого, так и малого бизнеса с обязательным применением антимонопольных мер. Рыночная оценка деятельности государственных учреждений позволит избавить бюджет от неоправданных расходов и поможет в его модернизации.

Государственный менеджмент направлен на повышение организационной эффективности, что подразумевает налаживание обратной связи с населением, позволяющей вовремя получать актуальную информацию и вносить инновационные изменения в процесс работы в соответствии с нуждами потребителей госуслуг. Также обратная связь является формой контроля работы работы чиновников. Кроме этого,

стимулируется аналитическая работа и обмен данными между различными ведомствами, что дает необходимую информацию для оценки эффективности применяемых методов, а также позволяет вышестоящим органам положить в основу планирования целей и задач решение самых острых проблем населения.

Процессы управления государственным сектором представляют собой реализацию складывающихся производственно-экономических общественных отношений в целях обеспечения социальной защиты населения, здесь приходится иметь дело с государственным, региональным и муниципальным управлением, которому присущи свои ценности, стиль, методы работы и т.д. В то же время стиль, методы работы и даже цели менеджмента выработаны в условиях рыночной экономики и эффективность здесь стимулируется получением прибыли и просто на просто выживанием в жестких условиях. Поэтому просто взять и перенести все плюсы менеджмента в государственный сектор не получится. Это две разные ветви управления со своими уникальными принципами.

В тоже время опыт зарубежных стран ясно дает понять, что некоторые принципы менеджмента вполне можно перенести в государственный сектор. Здесь выделяются такие страны как: США, Англия, Германия, Франция, Китай, Индии, Италия, Южная Корея, Япония и т.д. В этих странах в государственный сектор попадают только самым тщательнейшим образом подобранные кадры.

Государство должно поощрять людей, способных к инновациям и использующих свои созидательные способности, позволяющих снизить роль политических кланов и харизматических лидеров для достижения стабильности и упорядоченности общественных связей. На деле же без наличия такой же мощной мотивации, как в рыночном секторе, такие люди остаются без внимания. В заключение, можно сказать, что государственный сектор, особенно в нашей стране, остро нуждается в обновлении принципов, методов, системы мотивации и т.д. Все это можно привнести из менеджмента, предварительно переработав, учитывая особенности государственного сектора. Такой подход, по моему мнению, способен повысить эффективность государственного управления.

Література:

1. *«Современные подходы к управлению в государственных и частных секторах» - [Электронный ресурс]*
2. *«Государственный менеджмент» - [Электронный ресурс] - http://biznestoday.ru/ob/menikons/405-gosudarstvennyj-menedzhment.html*
3. *«Государственное управление и менеджмент» - [Электронный ресурс] - https://www.bibliofond.ru/view.aspx?id=707864*

Ковтун Ірина Василівна
Державний університет телекомунікацій
Науковий інститут менеджменту та підприємництва
м. Київ

СОЦІАЛЬНО-ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ ТЕЛЕКОМУНІКАЦІЙНОЇ СФЕРИ В УКРАЇНІ

Телекомунікації — це процес, фундаментальний засіб для досягнення різних цілей. В економічному світі телекомунікації слугують для розповсюдження інформації серед постачальників, споживачів, законодавців. Вони присутні у всіх процесах економічного виробництва і є невід'ємною складовою практично будь-якої сучасної бізнес-діяльності. У соціальному середовищі телекомунікації є засобом для інформування, розваг та обміну досвідом. Телекомунікаційні мережі та послуги дозволяють здійснювати всі ці дії на великих відстанях та серед широкого кола користувачів.

Рішення, які приймаються урядами у сфері телекомунікацій, матимуть надзвичайно великий вплив на соціальний та економічний добробут націй.

Основні вимоги до закону про телекомунікації

У законі про телекомунікації мають знайти відображення такі моменти: цілі телекомунікаційної політики, регуляторні функції, процес прийняття рішень та роль у ньому державних органів.

Цілі телекомунікаційної політики:

а) Розвиток телекомунікаційної інфраструктури

б) Підвищення ефективності телекомунікаційного сектора

в) Забезпечення високої якості послуг

г) Захист суспільних інтересів

д) Захист верховенства права та принципу ефективного управління

Рекомендації для України

Якщо Україна прагне досягти європейських стандартів у галузі зв'язку, вона насамперед має стимулювати розвиток власного телекомунікаційного сектора шляхом його реформування.

Наразі цілком очевидно, що в Україні існує гостра необхідність у створенні нового незалежного регуляторного органу для розроблення чітких правил та процедур регулювання національного телекомунікаційного ринку.

Телекомунікації відіграють важливу інфраструктурну роль у суспільстві, забезпечуючи оперативний обмін і розповсюдження інформації в процесах соціальної і економічної діяльності суспільства. Телекомунікації виконуватимуть роль комунікаційної основи при побудові інформаційного суспільства в Україні. Розвиток телекомунікацій повинен відбуватися випереджаючими темпами, порівняно з розвитком економіки, з тим, щоб не обмежувати економічний та соціальний розвиток суспільства.Повільні темпи розвитку телекомунікацій спричиняють зниження конкурентоспроможності економіки України.Телекомунікації відіграють значну роль у прискоренні розвитку економіки та соціальної сфери.

У сфері телекомунікацій існують такі проблеми:

- низький рівень забезпечення населення, підприємств, установ і організацій широкосмуговими телекомунікаційними послугами;
- нерівномірність забезпечення телекомунікаційними послугами та обмеженість доступу користувачів до загальнодоступних телекомунікаційних послуг особливо у сільській, гірській місцевості;
- використання на стаціонарних телекомунікаційних мережах морально застарілого та фізично зношеного аналогового обладнання,
- наявність великої кількості операторів телекомунікацій, що призвело до нескоординованості їх дій та відсутності єдиного підходу до вирішення проблемних питань розвитку телекомунікацій;
- неефективне використання можливостей прокладених волоконно-оптичних ліній зв'язку та побудованих стільникових мереж операторами телекомунікацій;
- недостатній регуляторний вплив держави на ринок телекомунікацій;
- обмеженість вибору альтернативних мереж операторів телекомунікацій

Основними напрямами розвитку телекомунікаційних мереж слід вважати:

- створення сучасних широкосмугових мультисервісних транспортних мереж на базі єдиних протоколів, сумісних з Інтернет-протоколами;
- розвиток широкосмугового абонентського доступу з використанням перспективних технологічних рішень,радіотехнологій доступу;
- прискорення розвитку телекомунікаційних мереж у сільській,гірській місцевості з використанням найбільш ефективних технологій;
- приведення системи нумерації телекомунікаційних мереж у відповідність з європейськими стандартами;

- забезпечення доступу до послуг, що надаються інформаційно-довідковими службами;
- участь у створенні національної супутникової системи зв'язку;
- модернізація та розвиток спеціальних телекомунікаційних мереж для задоволення потреб національної безпеки та оборони держави;
- забезпечення розвитку мереж загального користування;

Телекомунікації повинні зіграти роль каталізатора у прискореному розвитку економіки та соціальної сфери України, оскільки основний ефект діяльності телекомунікацій проявляється не у вигляді доходів, прибутків і відрахувань у держбюджет, а у вигляді злагодженого і оптимізованого функціонування економіки та соціальної сфери країни, а також у вигляді покращення умов життя громадян. Таким чином, можна визначити, що розвиток телекомунікацій має величезну роль у загальному економічному розвитку країни, то як урядовим, так і неурядовим організаціям необхідно вжити ще більших заходів щодо сприяння розвитку саме цієї галузі. Недостатній розвиток телекомунікацій загрожує конкурентоздатності економіки України та перспективам її розвитку.

Література:

1. *http://www.rusnauka.com/11_EISN_2010/Economics/64194.doc.htm*
2. *http://zakon5.rada.gov.ua/laws/show/316-2006-%D1%80*
3. *https://dt.ua/ECONOMICS/suchasni_telekomunikatsiyi_dosvid_evropi_ta_ukrayina.html*

Михайленко Микита Олександрович
Державний Університет Телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м.Київ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК СТИМУЛ ДЛЯ СОЦІАЛЬНО-ЕКОНОМІЧНОГО РОЗВИТКУ В УКРАЇНІ

Стрімкий розвиток інформаційних технологій зумовлює все більшу взаємозалежність соціально-економічного потенціалу держав і такого загальноприйнятого у світовому співтоваристві показника, як рейтинг розвитку інформаційно-телекомунікаційних технологій. Україна займає 71 місце з 143. Разом з тим, при аналізі численних агрегатних індексів у вищеназваному рейтингу розвитку ІКТ в нашій країні простежується чітка їх дивергенція. Видно, що при досить великому потенціалі розвитку інформаційно-телекомунікаційних технологій, в Україні практично відсутній попит, як з боку населення в цілому, так і з боку влади та бізнесу зокрема на такі технології. Представники влади та бізнесу досі користуються можливостями ІКТ лише на найнижчому, тривіальному рівні.

Причини:

- Ще не викоріненні корупційні інтереси державних чиновників
- Влада всіляко гальмує розширення сфери застосування ІКТ і штучно занижує на них попит.
- Бізнес також як і влада, став гальмувати розвиток інформаційних технологій в нашій країні.
- Можливі варіанти вирішення проблем
- Широке поширення і популяризація інформаційних технологій у сфері адміністративного, фінансового, роздрібного та соціально-побутового обслуговування малозабезпечених та соціально незахищених громадян.
- Впровадження та поширення ІТ розробок серед громадських організацій.
- Створення нових Web-ресурсів для бізнесу на основі застосування електронної комерції та сучасних інформаційних технологій.

Удосконалення системи початкової, середньої та вищої освіти з тим, щоб вона максимально стимулювала активність молоді не тільки в сфері ІТ розробок, але і в напрямку застосування інформаційних технологій та розробок у всіх сферах науки і техніки.

Висновок

Необхідно вжити системні та комплексні дії щодо впровадження інформаційних технологій у всі сектори громадянського суспільства.

Література:

1. *Рейтинг розвитку інформаційно-телекомунікаційних технологій (Networked Readiness Index +2015).*
2. *Інформаційні технології в Україні: Колос на глиняних ногах.*
3. *"В Україні відсутня стратегія розвитку ІКТ-сектора".*
4. *"Інформсуспільство – недієздатне".*

Дроботенко Надія Іванівна
Державний університет телекомунікацій
Навчально-науковий інститут
менеджменту та телекомунікацій
м. Київ

РОЗВИТОК П'ЯТОГО ПОКОЛІННЯ МОБІЛЬНОГО ЗВ'ЯЗКУ

В цілому, стандарт 5G, по суті, є тим, чим його практично всі вважають, - більш швидкою версією 4G і, тим більше, 3G. На жаль, немає поки чіткого і однозначного визначення ні програмного, ні апаратного забезпечення для побудови даного стандарту. Крім того, поки в світі немає жодного оператора мобільного зв'язку, який би реально обладнав свої станції для роботи в мережі 5G. З технічної точки зору, головна перевага технології доступу 5G - це дуже широкий канал і більш швидкі частоти доступу. Тільки уявіть собі зростання швидкості в більш ніж 10 раз.

Передбачуваний стандарт 5G буде працювати в високочастотної смузі бездротового спектра - від 30 до 300 ГГц. І так, ці міліметрові хвилі можуть передавати просто величезні обсяги даних на дуже високій швидкості. Крім того, смуга 5G не перекривається з смугою 4G. Тому ці смуги можуть працювати не заважаючи один одному. Але є один мінус від переходу на міліметрові хвилі. А саме, потрібно якось боротися з низькою проникаючою здатністю хвиль такої довжини. Низькочастотна область спектра не вимагає від операторів розміщувати свої антени дуже густо, адже низькочастотні хвилі не так сильно поглинаються предметами. Тому, для нормальної роботи мережі 5G операторам потрібно буде встановлювати набагато більше антен і відстань між ними стане набагато менше. Правда, не потрібно боятися, що телефонних вишок стане набагато більше. У багатьох випадках значно більше стане невеликих антен.

Через проблеми з поглинанням міліметрових такі компанії як Qualcomm і Intel, які стоять на передньому краї впровадження технології 5G, намагаються експериментувати з частотним діапазоном 6 ГГц. Компанії думають, що підмішування більш низьких частот дозволить зробити сигнал більш стабільним і не буде так поглинатися предметами навколишнього світу. Як бачите, з 5G є ще багато питань, які потребують вирішення.

Основні мобільні оператори США вже заявили, що планують перейти на рейки 5G тільки в 2020 році. Але вже сьогодні вони проводять деякі тести.

Нещодавно компанія Verizon оголосила, що на початку 2018 року запущена мережа 5G в 11 містах США, але розгортання призначене не для заміни фіксованого смуги доступу, а не все мобільної мережі. Інший оператор AT & T надасть відеосервіс DirectTV Now через мережу 5G. Але такий привілей доступна тільки обмеженому числу

клієнтів компанії в місті Остін, штат Техас. Першим оператором мобільного зв'язку в США, який продемонстрував своїм клієнтам всі переваги мережі 5G, став Sprint. Він надав можливість подивитися живу трансляцію відео в форматі 4К фіналу сезону з американського футболу. А T-Mobile вже зараз декларує наміри через канал 5G передавати відео для пристроїв віртуальної реальності.

Виробник апаратної частини також не сидять склавши руки. Так, компанії Intel і Qualcomm вже представили модеми, які можуть працювати в мережі 5G. Крім модемів на технічних виставках також були представлено та інше мережеве обладнання, яке необхідне для побудови мережі. Звичайно, всі ці тести свідчать про те, що компанії серйозно налаштовані на швидке впровадження 5G.

Дроботенко Надія Іванівна
Державний університет телекомунікацій
Навчально-науковий інститут
телекомунікацій
м. Київ

РІЗНИЦЯ МІЖ 4G ТА 5G

Кожен день ми стикаємося з черговим вибором, скрізь є альтернативи, нові рішення. І напевно ви не раз запитували себе: Який з товарів краще? Який більш технологічний? У чому принципова відмінність між ними? А яка різниця між 4G та 5G?

Різниця суттєва. І перш за все, у швидкості передачі даних, яка буде на порядок краща, ніж 4G. Але питання запровадження 5G у світі лише обговорюється. Тому що діапазон частот для цього стандарту ще не розподілений. Він буде визначений на Всесвітній конференції радіозв'язку, яка пройде в 2019 році. Коли вже будуть розподілені певні частоти, гармонізовані для того, щоби застосовувати їх у світі, то це можна буде вважати початком стандарту 5G у світі. Діапазон, який передбачається для запровадження 5G, це 700 Мегагерц. Європа звільняє цей діапазон від телевізійного мовлення. В Україні цей процес теж розпочато. Я думаю, він буде повільніший, ніж у Європі. Тому що в Європі від телевізійного мовлення цей діапазон майже звільнений. Нам потрібно рухатись у цьому напрямку і Український державний центр радіочастот робить для цього все можливе.

4G стає «застарілим» стандартом. Вважається, що п'яте покоління мобільного зв'язку з'явиться до 2020 року. Пояснити це досить просто: існує, так зване, правило десяти років. Якщо зазирнути трохи в минуле, можна помітити, що кожне нове покоління мобільного зв'язку з'являлося приблизно через 10 років після появи попереднього: перше покоління з'явилося на початку 80- років, друге на початку 90-х, третє на початку 00-х, четверте в 2009 році. Напрошується висновок, що перші мережі 5G з'являться приблизно в 2020 році. В даний час ведуться програми по розробці основних обрисів стандарту п'ятого покоління. Саме тому точного визначення 5G поки дати не можна, можна лише передбачити, якими стануть мережі після 2020 року.

Очевидно, що в майбутньому до мережі буде підключено набагато більше пристроїв, більшість з яких будуть працювати за принципом «завжди онлайн». При цьому дуже важливим параметром буде низьке енергоспоживання. Безумовно, в мережах п'ятого покоління середні швидкості повинні бути, як мінімум, на порядок вище, ніж в мережах четвертого покоління.

Таким чином, передбачається, що 5G забезпечуватимуть більш високу пропускну здатність у порівнянні з технологіями 4G, що дозволить забезпечити більшу доступність широкосмугового мобільного зв'язку, а також використання режимів device-to-device, наднадійні масштабні системи комунікації між пристроями, більш короткий час затримки, менша витрата енергії батарейок, ніж у 4G-обладнання, що сприятливо позначиться на розвитку Інтернету речей.

Література:

1. *https://hitech.buyon.ru/pages/3g-vs-4g-5g-1375/*
2. *https://comments.ua/ht/594269-chto-3g-4g-5g-zhdat-6g.html*

Харакоз Марія Олександрівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту и підприємництва
м. Київ

СУЧАСНІ ПІДХОДИ ДО УПРАВЛІННЯ В ДЕРЖАВНИХ ТА ПРИВАТНИХ СЕКТОРАХ

Одним із пріоритетів економічного розвитку визначено реалізацію інвестиційного потенціалу країни та формування сприят ливого інвестиційного середовища з метою зміцнення конкурентоспроможності України на світовому ринку. Таким чином, необхідно виокремити підходи до управління державними інвестиціями, окреслити їх особ ливості та способи вдосконалення в сучасних умовах з урахуванням спроможності національної економічної системи щодо фінансування таких проектів і програм. Проблематика визначення оптимальних підходів до управління інвестиційною діяльністю активно опрацьовується у вітчизняному науковому про- сторі такими вченими, як О. І. Амоша, С. О. Біла, І. А. Бланк, М. С. Герасимчук, М. Х. Корецький, І. М. Крупка, А. А. Пересада та ін. Розвиток державного інвестиційного потенціалу було визначено пріори-тетним у контексті реформування економіки.

У післякризовий період дер жавне фінансування інвестиційних програм набуло важливості у зв'язку з падінням підприємницької активності та підвищеною складністю доступу до кредитних ресурсів. Так, частка державних інвестицій в основний капітал у ВВП зросла з 0,73 % у 2009 р. до 1,18 % у 2011 р. та сягнула 1,22 % у 2012 р. Така тенденція потребує підвищеної уваги до процесів управління державними інвестиціями та вдосконалення відповідних підходів. В Україні у процесі реформування сфери державних фінансів проведено ряд змін стосовно управління інвестиціями та державними видатками загалом. Однак повного введення у бюджетний процес державної інвестиційної програми як об'єкта бюджетних відносин досі не відбулось. У Бюджетному кодексі України поняття державної інвестиційної програми та проекту об'єднане й тлумачиться як комплекс заходів, визначених на основі націо- нальної системи цінностей і завдань інноваційного розвитку та спрямованих на розвиток окремих галузей, секторів економіки, виробництв, регіонів, виконання яких здійснюється з використанням коштів державного та/або місцевих бюджетів чи шляхом надання державних та/або місцевих гарантій

В Україні наразі наявний портфель проектів, що мають статус інвестиційних, реалізація яких скеровується Державним агентством з інвестицій та управління національними проектами України. Поняття капітальних інвестицій у Податковому кодексі України сформульоване як господарські операції, що передбачають придбання будинків, споруд, інших об'єктів нерухомої власності, основних засобів і нематеріальних активів, що підлягають амортизації відповідно до нормативного Кодексу. Такі інвестиції не мають статусу проектів. В умовах сьогодення управління державною інвестиційною діяльністю здійснюється у трьох основних вимірах: стратегічному, що передбачає визначення напрямів інвестування та виокремлення галузевих пріоритетів; нормативному, який включає забезпечення законодавчого регулювання інвестиційної діяльності, гарантії прав інвесторів і формалізацію їх зобов'язань; та адміністративному, що передбачає розроблення нових і вдосконалення наявних методів та інструментів управління інвестиційною діяльністю, зокрема, інвестиційними проектами і програмами. Серед світових тенденцій розвитку інвестиційної діяльності спостерігається обмеження вихідних інвестиційних потоків, оскільки вони можуть призводити до виведення за кордон потенційних робочих місць в

умовах підвищеного рівня безробіття всередині країни. Інвестиційна політика держави значною мірою зумовлена якістю її розроблення.

За останніми дослідженнями UNCTAD, головні завдання у процесі формування інвестиційної політики з метою сприяння економічному зростанню та сталому розвитку можна поділити на три основні напрями впливу:

1. Інтеграція інвестиційної політики у стратегію розвитку Завдання: – визначення стратегічних інвестиційних пріоритетів та узгодження на- прямів інвестиційної політики у питаннях розподілу і розвитку продуктивних сил, що включає розвиток людських ресурсів, інфраструктуру, поширення технологій, розвиток підприємництва (зокрема сприяння налагодженню міжгалузевих зв'язків); – визначення заходів інвестиційної політики стосовно захисту вразливих галузей; – перевірка узгодженості заходів і напрямів інвестиційної політики щодо всіх галузей національної економіки.

2. Інтеграція цілей сталого розвитку до цілей інвестиційної політики Завдання щодо розроблення заходів: – інвестиційної політики та конкретних положень, що стосуються за- лучення й реалізації інвестицій, а також забезпечення дотримання прав і обов'язків інвестора, включаючи питання корпоративної відпо- відальності; – дотримання міжнародних стандартів щодо прав і обов'язків інвестора.

Література:

1. *Towards a New Generation of Investment Policies: World Investment Report 2012 [Електронний ресурс]. – Режим доступу: http://www.unctad-docs.org/fi les/UNCTADWIR2012-Preface-Key-messages-and-Overview-en.pdf; Investment Policy Framework for Sustainable Development : Chapter IV / Towards a New Generation of Investment Policies : World Investment Report 2012. – P. 28 [Електронний ресурс]. – Режим доступу: http://www. unctad-docs.org/fi les/UNCTAD-WIR2012-Chapter-IV-en.pdf.*

Чернявська Інна Сергіївна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

СОЦІАЛЬНІ МЕРЕЖІ В СУЧАСНОМУ СВІТІ

Інтернет, чати, віртуальні щоденники, соціальні мережі стали прикметою сучасності. Сьогодні там проводять більше свого час не лише дорослі але й діти. У віртуальних мережах вирує своє життя — людиьспілкуються, , закохуються, сваряться, висловлюють свої думки, завантажують фотографії, відео тощо...

Першою спробою створити таку мережу спілкування став ще 1995 року сайт classmates.com, який через обмаль реклами та фінансування невдовзі був закритий. Соціальні мережі, звісно, мають свій позитив. У них можна зустріти однокласників та знайомих, навіть якщо ви загубилися багато роківтому.. Коли людина реєструється у соціальній мережі, спершу відчуває легку ейфорію — стільки знайомих одразу! Ми шукаємо тих, хто знав нас ще юними та безтурботними, ніби створюємо навколо себе позитивнее психологічне поле — коло підтримки, черпаємо звідти нові ресурси... Але, на жаль, більшість із нас ідеалізує он-лайн друзів і приписує їмриси, яких насправді вони не мають. Проте необмежена свобода і відсутність цензури на соціальних мережах часто сприяють прояву не найкращих людських

Одна з найголовніших небезпек соціальних мереж — упевненість тамтешніх завсідників у тому, що більшість їхніх віртуальних дій минаються без наслідків. У житті ми звикли відповідати за свої вчинки, а тут — можна;підправити; підпис чи стерти коментар. У житті якщо вже

висловився — то;підправити ; свої слова важко, недарма ж кажуть:слово не горобець, — вилетить не впіймаєш. У соціальній мережі можна назватися чужим іменем і поставити на профілі не свою фотографію, абосвою, але десятирічної давності.

Сюзан Грінфілд, дослідниця впливу сучасних технологій на роботу головного мозку людини, вважає, що в сучасного покоління, яке виростає на соціальних мережах, зникає симпатія — здатність до співпереживання та розуміння інших.

А віртуал практично не дає нам такої інформації. Тому віддавати перевагу;інтернет-спілкуванню перед реальним — означає обмежувати себе в тому, чого справді потребує людина. Дружба в соціальних мережах досить поверхова, і деякі молоді люди, а особливо діти, намагаються;додати; до свого профілю якнайбільше друзів. Із великою кількістю;друзів; не лише нереально спілкуватися, а й неможливо привітати кожного хоча б із днем народженням. І зрозуміло, що переважно це незнайомі люди. Інколи підлітки створюють ще й по кілька різних профілів (із різними іменами) на одній і тій самій соціальній мережі. Згідно з опитуванням маркетингової компанії AWeber американських школярів та студентів, 90% підлітків постійно проводять час у Facebook (рідше — Email), часто використовуючи для цього і стільникові телефони. Молоді люди заходять у соціальні мережі, щойно прокинувшись зранку. Вони перебувають там дорогою на навчання (чи повертаючись додому), у школі, не можуть відірватися від он-лайн спілкування навіть на відпочинку. 18% опитуваних підлітків заявили, що взагалі перестануть спілкуватися, коли раптом зникнуть соціальні мережі.

На превеликий жаль, практично, неможливо простежити, чим займаються ваші діти в мережах. Фахівці радять не так забороняти спілкування в Інтернеті, як доступно, відповідно до віку вашого сина чи доньки, пояснювати можливі небезпеки і роз'яснювати правила
безпечного віртуального спілкування. А також вибірково контролювати соціальну он-лайн активність вашої дитини.

Висновок: Безумовно, соціальні мережі набули останнім часом неймовірної популярності. Це явище неоднозначне, але ж неоднозначно завжди ставляться до всього нового. Їхні прихильники стверджують, що вони несуть суцільний позитив, їхні опоненти вважають, що негатив, але правда десь посередині.

Савраненко Анастасія Романівна
Державний університет телекомунікацій
Навчально-наукового інституту менеджменту та підприємництва
м. Київ

РОЗВИТОК СУЧАСНИХ ПОСЛУГ

Сфера телекомунікацій в останні роки зросла надзвичайно високими темпами. Тому особливої уваги заслуговує питання її подальшого розвитку. Телекомунікації – це процес, фундаментальний засіб для досягнення різноманітних цілей. В економічному світі телекомунікації служать для поширення інформації серед постачальників, споживачів, дослідників, аналітиків, законодавців, регуляторів. Вони присутні у всіх процесах економічного виробництва і є невід'ємною складовою практично будь-якої сучасної бізнес-діяльності, метою якої є продукування товарів і послуг для споживачів. У соціальному середовищі телекомунікації є засобом для інформування, розваг та обміну досвідом. Телекомунікаційні мережі і послуги дозволяють здійснювати всі ці дії на великих відстанях і серед широкого кола користувачів.

Що стосується діяльності телекомунікаційних підприємств, то їх розвиток повинен базуватися на постійному моніторингу ринку телекомунікаційних послуг та удосконаленні їх технологічної складової, без якої подальше існування таких підприємств неможливо.

Сфера інформації та телекомунікацій охоплює такі види економічної діяльності: видавництво; виробництво кіно- та відеофільмів, телевізійних програм, видання звукозаписів; діяльність у сфері радіо- та телевізійного мовлення; комп'ютерне програмування, надання інформаційних послуг; надання послуг зв'язку. Близько двох третин послуг, що надаються суб'єктами господарювання сфери інформації та телекомунікацій, припадають на послуги зв'язку. За таких обставин важливо приділити увагу дослідженню стану та розвитку підприємств зв'язку України, які демонструють високу позитивну динаміку зростання та інноваційну спрямованість щодо підприємств інших галузей.

В даний час ринок телекомунікаційних послуг активно розвивається. Для реалізації послуг продовжують з'являтися нові технології, що викликають інтерес з боку підприємств і населення. Основними сегментами ринку телекомунікаційних послуг є послуги телефонного зв'язку, мобільного зв'язку, передачі даних через Інтернет, супутникове телебачення. Для ринку телекомунікацій характерні високі темпи зростання в порівнянні з іншими галузями, активне впровадження нових технологій, зміна структури послуг, що надаються. Сьогодні все частіше відзначається перенесення обсягів користування з традиційних телекомунікаційних послуг до нових видів, таким як надання послуг на основі мультисервісних транспортних мереж, широкосмуговий

Інтернет-доступ, технологію мобільного зв'язку третього покоління, що включає набір послуг, які об'єднують як високошвидкісний мобільний доступ з послугами мережі, так і технологію радіозв'язку, яка створює канал передачі даних. Звіти великих операторів зв'язку за останні роки підтверджують головну тенденцію розвитку ринку телекомунікацій. Кількість користувачів швидкісного Інтернету щорічно збільшується, відповідно і частка доходів в цьому сегменті також зростає. У той же час дещо сповільнилася міграція абонентів з мереж фіксованого зв'язку в мережі мобільного зв'язку, але посилюється міграція голосового трафіку в мережі Інтернет-телефонії, розвиток отримують технології віртуалізації і аутсорсинг - створення веб-ресурсів, розробка, установка, супровід програмного забезпечення, обслуговування техніки спеціальними компаніями. Незважаючи на складну макроекономічну ситуацію, очікується збільшення числа підключень, підвищення швидкості і якості передачі даних при збереженні і, можливо, зниження цінових показників.

Література:

1. *Лазоренко Л.В., Глушенкова А.А. «Сутність та основні тенденції розвитку телекомунікаційних підприємств України»*
2. *Толкачова Г.В., Ковалик О.В.,Одесская национальная академия связи им. А.С. Попова, «Стан та розвиток сучасних послуг зв'язку».*

Пилипей Анастасія Святославівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

ТЕЛЕКОМУНІКАЦІЙНА ГАЛУЗЬ УКРАЇНИ:ПРОБЛЕМИ І ПЕРСПЕКТИВИ КОНКУРЕНТОСПРОМОЖНОСТІ

Одна зі стратегічних для будь-якої країни галузей - галузь телекомунікацій - відіграє величезну роль у збалансованому розвитку глобальної та регіональної економіки. Вона є з'єднувальною ланкою як промислової сфери, сфери послуг і споживачів, так і різних географічно розрізнених частин країни та економічних центрів. Стимулюючи людське спілкування за допомогою зв'язку, сучасні засоби телекомунікацій стають необхідною умовою для соціальної згуртованості та культурного розвитку всіх країн. Вже зараз неймовірно збільшені потоки інформації - телефонні розмови, факсимільна інформація,

електонна пошта, масиви даних та телебачення - показують, якою мірою світ стає ще більш залежним від засобів телекомунікацій, які змінюють бізнес, стиль життя, суспільство вцілому. Так, діти в Сінгапурі застосовуть пейджинг або стільниковий телефон для підтримання зв'язків з батьками, а аборигени Австралії продають свій живопис, використовуючи можливості відеоконференції, бразильські банки пропонують свої послуги в мережі Інтернет, а французькі домогосподарки радяться з телефонними компаніями у справі вибору слюсаря. Як бачимо, комунікаційні послуги стирають кордони між культурами, мовами та часом. У багатьох країнах світу сектор послуг у наш час вже дає близько половини їх валового національного продукту, і ця тенденція не обмежується лише економічно розвинутими державами. В таких різних країнах, як наприклад Сінгапур, Гонконг або Угорщина, сектор послуг забезпечує до 60% економічної активності країни. Навіть у найменш розвинутих країнах частка сектору послуг (43%) перевищує частку сільськогосподарського сектору (37%) або промислового (20%). При цьому вже на початку 90-х років світова частка сфери послуг в економіці становила в середньому близько 60%, а вже протягом наступних років від 70 до 80% економіки розвинутих країн знаходяться під значним впливом інформаційних технологій. Отже, наприкінці XX ст. - початку XXI ст. світ перебуває в стані інформаційної революції, вплив якої можна порівняти з впливом індустріальної революції минулого століття. Є всі підстави вважати, що обробка інформації - одна з найвагоміших складових економічної активності. Тому можна стверджувати, що розвиток телекомунікацій як важлива складова інформатизації суспільства та забезпечення населення високоякісними послугами зв'язку є одним з найважливіших напрямів національного та економічного розвтку будь-якої держави, і, зокрема, України.

У даній роботі спробуємо дослідити реальний стан галузі телекомунікацій в Україні, позитивні та негативні фактори, що визначають розвиток українських телекомунікацій, проблеми такого розвитку, а також пропозиції та заходи, спрямовані на подолання проблем, для того, щоб оцінити конкурентоспроможність України у цій галузі.

Загальновідомим є той факт, що телекомунікації України значно відстають від телекомунікацій розвинутих країн як за обсягами, так і за рівнем технологій. Ринок телекомунікацій України - достатньо відкритий та лібералізований за останні 8 років. Наведемо деякі цифри. Телефонна щільність у розвинутих країнах складає біля 60 телефонних номерів на 100 чоловік, тоді як в Україні - 20, а, наприклад, у Польщі, яка так само, як і Україна, вважається країною, що розвивається, - 24,6. Інтернетом у розвинутих країнах користуються 15-20% населення, в Україні - 1%, а у Польщі - близько 5%. Щодо мобільного зв'язку, то у розвинутих країнах - близько 30 телефонів на 100 чоловік, в Україні - 0,3, а у Польщі близько 7. По міжнародних та міжміських розмовах спостерігається відставання України від Польщі десь у 5 разів. Послуги зв'язку в рік на одну особу у розвинутих країнах складають 254 дол., в Україні - 20,6, а у Польщі - 65,7. Загалом розвинуті країни вкладають у розвиток зв'язку до 20% від її доходу, країни, що розвиваються - близько 31%, слаборозвинені - 68,5%, тоді як в Україні - 18,1%, а у Польщі - 42,2%. Звідси й відповідні результати.

Взагалі, галузь телекомунікацій в Україні поділяється на два крупних сегменти: електрозв'язок та поштовий зв'язок. Електрозв'язок має два основні напрями: наземний (фіксований чи дротовий) та радіозв'язок. До першої групи, як правило, включають телефонний, телефонний міський, телефонний сільський, телефонний міжміський, телефонний міжнародний зв'язок. Сюди ж можна віднести Інтернет (хоча зараз Інтернет переміщується й у радіозв'язок). До другої групи належать супутниковий, стільниковий, пейджинговий, транкінговий зв'язок. Одним з найдинамічніших за останні роки сегментів українського телекомунікаційного ринку є мобільний зв'язок. Причому як з точки зору зовнішніх впливів на галузь, так і з точки зору взаємовідношень між суб'єктами ринку. Але довготривала економічна криза та нестабільність вітчизняного законодавства суттєво пригальмувала розвиток українського ринку мобільного зв'язку. Однак, як і інших галузей

економіки. Більш того, мобільний зв'язок, як один з найприбутковіших напрямів діяльності, потрапив під пильну увагу контролюючих, інспектуючих та інших подібних "експроприюючих" органів. За останні роки спостерігалися спроби накласти як на суб'єктів ринку, так і на його споживачів різного роду додаткові збори, податки, акцизи і т.д. Це аж ніяк не сприяє розвитку галузі. Але все ж таки на сьогоднішній день можна сказати, що український ринок мобільного зв'язку поступово набуває цивілізованих рис, незважаючи на активну боротьбу (а, можливо, і завдяки їй) п'яти мобільних операторів зв'язку (UMC, KyivStar GSM, DCC, Wellcom, Golden Telecom GSM) за невелику частину платоспроможної клієнтури. Також порівняно динамічною сферою українських телекомунікацій можна назвати Інтернет. Загальна кількість користувачів Інтернетом в Україні на початок 1999 року становила приблизно 100-120 тис. У відношенні до загальної кількості користувачів у світі вона складає менше 0,1% або, точніше, 0,065%. Але в середньому за кожні шість місяців кількість користувачів збільшується в 1,67 раза, що вище середніх темпів зростання у світі в цілому. Зараз мають місце такі прогнозні коефіцієнти росту кількості українських користувачів Інтернетом: 2002 р. - 1,5; 2003 р. - 1,5; 2004 р. - 1,4; 2005 р. - 1,4.

Необхідно зазначити, що скільки існує та розвивається вітчизняний сегмент Інтернету, впадає в око один не дуже приємний факт - складається враження, що "існує та розвивається" він тільки у Києві. В інші регіони протягнено лише невеличкі джерела виділених каналів від крупних київських провайдерів. Але не слід забувати, що перші виділені канали, наприклад, з'явились не в Києві, а в Харкові, що помітна частина найкращих інформаційних ресурсів України знаходиться не тільки у Києві, але й в Одесі, Донецьку, Дніпропетровську.

Щодо сегмента електрозв'язку, то рівень телефонізації в Україні на сьогодні у два рази нижчий, ніж у країнах Центральної та Західної Європи. Із загальної кількості діючих у телефонній мережі АТС 21,1% належать електронним та квазіелектронним, решта - морально застарілим аналоговим. Щільність телефонного зв'язку, як вже зазначалося, становить близько 20,1 телефонів на 100 осіб. Кількість основних телефонних номерів складає в Україні близько 9 млн., з яких 86,6% встановлено у міських телефонних мережах, 13,4% - у сільських. Подальша телефонізація населених пунктів з низьким показником кількості телефонних номерів через низьку платоспроможність у таких регіонах триває повільно - в цілому по країні показники телефонізації зростають за рахунок, знову ж таки, Києва та інших великих міст. Взагалі, характерною особливістю української телекомунікаційної галузі є значне відставання за часом по застосуванню нових технологій між Києвом та іншими регіонами країни. Наприклад, мобільний зв'язок у Харкові з'явився через 2-3 роки після його появи у Києві, а в деяких великих містах з населенням в 25 і більше тис. людей він відсутній і досі. Мобільним зв'язком покрито усього біля 25% території України. Слід зазначити також, що ринок телекомунікацій в Україні характеризується високим рівнем монополізму. "Укртелеком", "Утел", UMC, "Укрпошта" - їх сумарна частка у структурі даних послуг становить 90 %. Як вважає Інтернет Асоціація України, зараз практично всі недержавні учасники телекомунікаційного ринку у тій чи іншій мірі потерпають від монопольного становища ВАТ "Укртелком". Для світового телекомунікаційного ринку характерні процеси інтеграції та глобалізації, тому що в цілому світовий ринок стає все більш інтегрованим. А Україна, нажаль, часто не може налагодити роумінг у масштабах країни. Україна повинна мати стратегічних партнерів. Ці партнери повинні бути у Європі, Америці, Азії. Бажаним для України є входження до одного з глобальних об'єднань. Проблемою розвитку телекомунікацій в Україні також є наявність близько 70% аналогових АТС від їхньої загальної кількості. На модернізацію вітчизняних комунікацій потрібно близько 19 млрд. дол.

Отже, як бачимо, стан галузі телекомунікацій України особливо не вражає, але оскільки, як було зазначено раніше, розвиток телекомунікацій має величезну роль у загальному економічному розвитку країни, то як урядовим, так і неурядовим організаціям

необхідно вживати усіх можливих заходів щодо сприяння такому розвитку, зокрема, аби підвищити конкурентоспроможність України в цій галузі.

Карась Юрій Юрійович
Державний університет телекомунікацій
Начально-науковий інститут менеджменту та підприємництва
м. Київ

ВПРОВАДЖЕННЯ 5G

Поки Україна готується до впровадження безпроводових технологій четвертого покоління 4G, провідні світові виробники телекомунікаційного обладнання переходять від теоретичної до практичної частини на шляху розвитку технологій 5G. Чим зумовлений вибір даного напрямку? Адже 4G здатний забезпечити безпроводовий доступ до мережі на швидкості близько 100 Мбіт/с і досить високу пропускну здатність мережі. Однак в найближчому майбутньому цього може виявитися недостатньо.

Очікується, що глобальний мобільний трафік зросте в десять разів в період з 2016 до 2022 року. Цей процес зумовлений масовим поширенням мобільного потокового відео, а також зростанням кількості підключених до мережі «розумних» пристроїв. Число останніх, як передбачається, до 2022 року досягне 18 млрд. Таким чином, значно зросте навантаження на мережу і вимоги до швидкості передавання даних. Крім цього, критично важливими якостями мережі залишаться енергоефективність і економічність. Все це є передумовами для появи нових рішень, які будуть об'єднані у концепції 5G.

Незважаючи на те, що вимоги до 5G все ще знаходяться на стадії розроблення в Міжнародному союзі електрозв'язку та консорціумі 3GPP, існує попередня домовленість, відповідно до якої технології 5G повинні забезпечувати:
розширення мобільного широкосмугового доступу (eMBB - enhanced Mobile Broadband);
наднадійний зв'язок з малою затримкою (URLLC - Ultra-Reliable Low latency Communications);
масову комунікацію «розумних» пристроїв і машин (mMTC - massive Machine Type Communications).

eMBB є мобільним широкосмуговим доступом, покращеним за рахунок збільшення ємності та покриття мережі, збільшення пікової та середньої швидкостей передавання даних, а також швидкості передавання даних на кордоні стільника.
URLLC є обов'язковою вимогою для нових критично важливих послуг (промисловий Інтернет, інтелектуальні мережі, захист інфраструктури, інтелектуальні транспортні системи (ITS)).

mMTC служить для забезпечення роботи 5G в умовах підключення величезної кількості пристроїв і датчиків Інтернету речей (IoT).
3GPP розглядає два шляхи, якими може розвиватися радіодоступ, оснований на технології 5G. Один з них полягає в еволюції LTE, інший - у доступі за допомогою New Radio (NR).
Шлях розвитку на основі LTE передбачає зворотну сумісність з технологіями 4G, які будуть вдосконалюватися відповідно до вимог, що висуваються до 5G.
Застосування NR не передбачає зворотної сумісності з технологіями 4G, що дозволяє впроваджувати більш фундаментальні зміни, такі як орієнтація спектра на більш високі частоти (1 - 100 ГГц). Проте, в ході розроблення NR врахована можливість масштабування, що дозволить в результаті користуватися і тими частотами, які на сьогоднішній день зайняті під LTE.

Втім, на сьогодні шлях розвитку мереж на основі безпроводових технологій четвертого покоління LTE є найбільш логічним. Близький до завершення реліз LTE Rel-15, який, разом з Rel-14, включає в себе низку поліпшень і нових функцій. Найбільш важливими з них є зменшення затримки, збільшення швидкості передавання призначених для користувача даних, а також пропускної здатності мережі за рахунок застосування FD-

MIMO (Full-Dimension MIMO). Крім того, в LTE Rel-14 і Rel-15 передбачено поліпшення підтримки mMTC, URLLC і ITS.

Література:

1. www.ericsson.com

Карась Юрій Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

СВІТОВІ ТЕНДЕНЦІЇ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Перспективи розвитку нашої цивілізації багато в чому залежать від того, наскільки швидко і адекватно людство проникне в сокровенні таємниці інформації, усвідомлює переваги і небезпеки, пов'язані зі становленням суспільства, заснованого на виробництві, розповсюдженні та споживанні інформації і званого інформаційним. Суть змін, що відбуваються, що охопили сферу діяльності людини, в самому загальному вигляді полягає в тому, що матеріальна складова в структурі життєвих благ поступається місцем інформаційної. І хоча ми за інерцією все ще продовжуємо підраховувати складові основу традиційного багатства тонни, метри, декалітри виробленої продукції, стає очевидним, що економічна міць держави визначається вже далеко не цими показниками.

Кілька років тому передача даних за допомогою комп'ютерів цікавила тільки фахівців і досвідчених користувачів. В даний час використання локальних і глобальних комп'ютерних мереж стає настільки ж рутинною і поширеним, як і ПК. Якщо вам необхідна електронна пошта, використання інформаційних ресурсів Internet та інших інтерактивних комерційних інформаційних служб, наприклад, CompuServe, віддалене з'єднання домашнього ПК з локальною мережею на роботі, пересилання файлів в інше місто, то ласкаво просимо в світ комп'ютерної передачі даних. В даний час використання комп'ютерних комунікацій не вимагає спеціальних знань - навіть п'ятирічний малюк може «подорожувати» по Всесвітній павутині (World Wide Wed) до того, як навчиться їздити на велосипеді. Що зумовило бурхливий ріст комп'ютерних комунікацій? В основному два чинники – спрощення використання засобів передачі даних за допомогою комп'ютера і наявність величезних інформаційних ресурсів в глобальних мережах. Багато ділових людей і організації виявили, що вони повинні використовувати у своїй діяльності комп'ютерні комунікації (електронну пошту, інтерактивні інформаційні служби і т.д.) не тільки для своїх співробітників, але і для широкого кола споживачів своєї продукції через електронні дошки оголошень (BBS - Bulletin Board System), телеконференції інтерактивних інформаційних служб або через вузли Всесвітньої Павутини Internet. Обсяг і способи інформування споживачів за допомогою засобів комп'ютерних комунікацій докорінно змінилися за останні рік - два. Якщо раніше ця інформація в основному призначалася для фахівців, то тепер вона розрахована на саму широку аудиторію.

Етапи розвитку телекомунікаційних технологій:

У числі основних етапів розвитку телекомунікаційних технологій слід назвати:

- Телеграфні та телефонні мережі (докомп'ютерної епоха);
- Передача даних між окремими абонентами по виділених і комутованих каналах з використанням модемів;
- Мережі передачі даних з комутацією пакетів: дейтаграмні або використовують віртуальні з'єднання (типу X.25);
- Локальні обчислювальні мережі (найбільш поширені - Ethernet, Token Ring);
- Цифрові мережі інтегрального обслуговування (ISDN) - вузькосмугові, а потім широкосмугові;

- Високошвидкісні локальні мережі - Fast Ethernet, FDDI, FDDI II (розвиток FDDI для синхронної передачі мовної та відеоінформації);
- Високошвидкісні розподілені мережі Frame Relay, SMDS, ATM;
- Інформаційні супермагістралі.

Література:

1.Сучасні тенденції розвитку засобів телекомунікації, м. Сімферополь.

Петренко Алина Миколаївна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м.Київ

ВИКОРИСТАННЯ НОВІТНІХ ТЕХНОЛОГІЙ У ТЕЛЕКОМУНІКАЦІЯХ

Головним напрямком перебудови менеджменту і його радикального удосконалення, пристосування до сучасних умов стало масове використання новітньої комп'ютерної і телекомунікаційної техніки, формування на її основі високоефективних інформаційно-управлінських технологій.

Особливе значення має впровадження інформаційного менеджменту, значно розширювальної можливості використання компаніями інформаційних ресурсів. Розвиток інформаційного менеджменту зв'язано з організацією системи обробки даних і знань, послідовного їх розвитку до рівня інтегрованих автоматизованих систем управління, що охоплюють по вертикалі і горизонталі всі рівні і ланки виробництва і збуту.

Технологія – це комплекс наукових і інженерних знань, реалізованих у прийомах праці, наборах матеріальних, технічних, енергетичних, трудових факторів виробництва, способах їх з'єднання для створення продукту чи послуги, що відповідають визначеним вимогам.

Технологія нерозривно зв'язана з машинізацією виробничого чи невиробничого, насамперед управлінського процесу. Управлінські технології ґрунтуються на застосуванні комп'ютерів і телекомунікаційної техніки.

Відповідно до визначення, прийнятому ЮНЕСКО, інформаційна технологія – це комплекс взаємозалежних, наукових, технологічних, інженерних дисциплін, що вивчають методи ефективної організації праці людей, зайнятих обробкою і збереженням інформації; обчислювальну техніку і методи організації і взаємодії з людьми і виробничим устаткуванням, їхні практичні додатки, а також зв'язані з усім цим соціальні, економічні і культурні проблеми. Самі інформаційні технології вимагають складної підготовки, великих первісних витрат і наукомісткої техніки. Їхнє введення повинне починатися зі створення математичного забезпечення, формування інформаційних потоків у системах підготовки фахівців.

В останні десятиліття менеджмент в найбільш розвинутих країнах, зокрема, у США і Японії, на творчі інформаційні технології вищого рівня охоплюють повний інформаційний цикл – вироблення інформації (нових знань), їх передачу, переробку, використання для перетворення об'єкта, досягнення нових більш вищих цілей.

Інформаційні технології третього рівня означають вищий етап комп'ютеризації менеджменту, дозволяють задіяти ЕОМ у творчому процесі, з'єднати силу людського розуму і міць електронної техніки.

Література:

1.Библиотека управляющего персоналом: мировой опыт. Современный менеджмент: теория и практика: обзорная информация. // Сост. Яровой В.И. под ред. Г.В.Щекина. - К.: МЗУУП, 1994.

Нечитайло Богдан Сергійович

Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

СУЧАСНІ ТЕЛЕКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ У КОРПОРАТИВНОМУ УПРАВЛІННІ

Корпоративне управління – це комплекс управлінських дій, що компанія повинна здійснити, щоб досягти свою ціль або завоювати гарну репутацію і довіру кредиторів і інвесторів. Інвестори, перш ніж прийняти рішення про співробітництво й інвестиції в яке-небудь підприємство, аналізують його положення. Підвищення управлінської культури тісно пов'язано з використанням сучасних телекомунікаційних і інформаційних технологій.

У сучасному світі перед компаніями, які займаються тим чи іншим бізнесом, постійно виникають ті самі питання: як краще й ефективніше організувати обмін інформацією усередині компанії, а також з партнерами і клієнтами; як дотриматись безпеки передачі даних і забезпечити високої надійності зв'язку; як при цьому не упускати переваг нових технологій і мінімізувати свої витрати.

Такі питання виникають у будь-якій країні світу і перед компаніями різних сфер діяльності, незалежно від розміру чи кваліфікації. Усі перераховані проблеми мають «телекомунікаційну складову». Адже будь-який бізнес не може існувати без обміну інформацією. Від того, наскільки ефективно й оптимально побудована корпоративна мережа зв'язку і буде деякою мірою залежати успіх чи неуспіх компанії у веденні бізнесу в цілому.

Необхідно самостійно проаналізувати сучасне устаткування, підготувати приміщення, у яких установити і настроїти апаратне і програмне забезпечення. Рішення цих проблем займає тривалий період часу, є витратним, не гнучким, не технологічним, тому що реалізується, у кінцевому рахунку, не професійним телекомунікаційним оператором.

Інший варіант - це вдатися до послуг оператора зв'язку, що може запропонувати такій компанії-клієнту готове рішення. Подібний підхід виявляється оптимальним і відповідає вищевикладеним вимогам. Саме тому компанії всі частіше для рішення комплексної задачі створення універсальної корпоративної мережі зв'язку прибігають до послуг телекомунікаційних провайдерів.

Для оператора зв'язку такий аутсорсинг також дуже цікавий і вигідний, оскільки розширює сферу його діяльності і дозволяє йому одержувати додаткові доходи.

Технологія Інтернет також має безпосереднє відношення до систем корпоративного управління. Ось декілька областей, у яких Інтернет використовується в даний час найбільш продуктивно: маркетинг, прямі продажі, зв'язки з громадськістю, взаємодія з партнерами.

Використовуючи високошвидкісну магістральну мережу зв'язку компанія може мати виділений доступ в Інтернет, який володіє наступними перевагами:

- високошвидкісне з'єднання з міжнародною частиною Інтернет;
- доступність послуг не тільки у великих містах, але й у будь-яких інших населених пунктах, через які проходить залізниця;
- висока надійність наданих послуг за рахунок резервування магістралей IP мережі.

Історія автоматизації управління підприємствами обчислюється десятиліттями. Але останнім часом при стрімкому розвитку телекомунікаційних технологій у компаній з'являються нові можливості по оптимізації корпоративних систем керування.

Література:

1.Каратыгин С. Телекомуникационные технологии для менеджмента. В 2-х томах. - М.: ABF, 1995.

Григоренко Олександр Олександрович
Державний університет телекомунікацій

Навчально-науковий інститут менеджменту та підприємництва
м. Київ

ІННОВАЦІЙНІ ШЛЯХИ РОЗВИТКУ В СФЕРІ ТЕЛЕКОМУНІКАЦІЙ

Для більшості країн сфера телекомунікацій є одним із найбільш важливих секторів світової та національної економіки. Ця сфера потужно розвивається та впливає на розвиток суспільства та економіки в цілому. Телекомунікаційні підприємства надають широкий спектр сучасних телекомунікаційних послуг, якісні характеристики які відповідають високим потребам споживачів.

Такі вітчизняні та закордонні вчені як: Д.В.Богатирьов, С.В. Вахнюк, М. І. Крупка, С.В. Онишко, В.М. Орлов, О.В. Савчук, О.О. Саверченко, Л.П.Сай, Л.А. Стрій, Ю.С. Шипулина розглядали у своїх роботах широке коло питань, що пов'язане з формуванням механізму керування сферою телекомунікацій України, фінансовим забезпеченням інноваційного розвитку та моделюванням динаміки інноваційних процесів.

Невирішеною проблемою залишається формування організаційно-економічних механізмів інноваційного розвитку сфери телекомунікацій, що обумовлює актуальність досліджуваного питання. Компанії проводять активну інноваційну політику і виводять на ринок нові товари і послуги для підтримки конкурентоспроможності. Це пояснюється високою наукоємністю галузевої продукції в порівнянні з іншими галузями життєвим циклом товару, а також відносно обмеженими можливостями по диференціації вже існуючих продуктів через їх високу стандартизацію.

Для успішного здійснення змін в галузі телекомунікації потрібно удосконалення законодавчої бази. Важливим етапом є визначення телекомунікаційних ринків. При цьому необхідно враховувати, що на першому місці знаходиться висока якість надання телекомунікаційних послуг, на другому - бездоганне обслуговування клієнтів, на третьому - лідирування на ринку, що також відображає безупинний процес підвищення якості продуктів та обслуговування. Інноваційна діяльність телекомунікаційних компаній робить великий вплив на традиційні галузі світової економіки, висуваючи нові технологічні вимоги до продукції, організації виробництва, внутрігалузевої комунікації та управління персоналом. Формування організаційно-економічних механізмів інноваційного розвитку сфери телекомунікацій повинно бути пов'язане з відновленням основних виробничих фондів, які є головним джерелом збільшення обсягів виробництва, а також створення умов для надання телекомунікаційних послуг на рівні світових стандартів.

В сучасних умовах господарювання, які характеризують розвиток ринкових відносин, диверсифікація як стратегія не носить системного характеру та не виступає постійно супутньою альтернативою. Досвід країн з розвиненою ринковою економікою показує, що диверсифікація повинна розглядатися компанією навіть тоді, коли вона займає лідируюче положення в галузі. Підприємства України, взявши до уваги досвід світових компаній, які успішно диверсифікують свою діяльність, почали впроваджувати стратегії диверсифікації у всіх галузях економіки. Таким чином, логічним початком в процесі диверсифікації, як в результаті розвитку світової економіки, є матеріалізація інновацій, а результатом - втілення в життя стратегічних пріоритетів технічної політики.

Аналіз сучасних підходів до розвитку ринку телекомунікацій дозволяє зробити висновок про те, що найбільш ефективним напрямком є поєднання інноваційних підходів. Успіх реалізації даних інноваційних підходів залежить значною мірою від професіоналізму керівництва компаній в плані створення необхідної організаційної структури, здатної стимулювати творчу ініціативу персоналу, генерувати безліч нових ідей і оптимізувати процес реалізації інноваційних проектів .

Література:

1. Ефективність диверсифікації діяльності телекомунікаційного підприємства [Електронний ресурс] / Є.М. Стрельчук, Н.А. Калугіна // Економіка: реалії часу. Науковий журнал. - 2014. - № 2 (12). - С.28-33. - Режим доступу до журн.: http://economics.opu.ua/files/archive/2014/n2.html.

2. Удосконалення інноваційної діяльності підприємства галузі електрозв'язку [Електронний ресурс] / І.А. Дяченко // Технології та дизайн. - 2014. - № 1. - Режим доступу: nbuv.gov.ua/jpdf/td_2014_1_12.pdf.

Шарій Тимофій Олегович
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

ПРОБЛЕМИ РОЗВИТКУ ПІДПРИЄМСТВ ТЕЛЕКОМУНІКАЦІЙ

В умовах динамічного розвитку ринкової економіки зростають вимоги до соціально-економічної адаптованості та відповідного рівня функціонування усіх галузей та сфер економіки України. Прогресивний розвиток науки, техніки і технологій, інноваційність та висока наукомісткість сучасного виробництва висувають особливі вимоги до шляхів розвитку інформаційно-телекомунікаційної сфери .

Сфера телекомунікацій як складова сфери зв'язку та інформатизації має стратегічне значення для сталого розвитку й стабільного функціонування виробничої і соціальної інфраструктури України, що призначена для задоволення потреб фізичних та юридичних осіб, органів державної влади в телекомунікаційних послугах. Формування моделі структури проблем управління телекомунікаційними підприємствами допоможе послідовно й деталь- но проаналізувати суперечності та проблеми для їх подальшого розв'язання.

Підхід до вирішення суперечностей і проблем повинен бути цілеспрямований та структурований. У процесі глобалізації національної економіки і в період трансформації ринкових відносин в Україні сфера телекомунікацій як складова сфери зв'язку та інформатизації є головною «артерією», що постачає, обробляє, допомагає споживати інформацію і потребує швидкого реагування на соціально-економічні протиріччя, що виникають, та їх загострення у вигляді проблем. Це можливо зробити, якщо комплексно підійти до системи управління об'єктом телекомунікацій та питання структури. Зробивши більш ефективним механізм антикризового управління підприємством для стабільного його функціонування за умов поетапного системного підходу: аналіз та діагностика протиріч, їх структуризація, групування щодо виявленої проблемної спрямованості з урахуванням можливості виникнення кризового стану підприємства і загрозою банкрутства; формування проблем відповідно до часових обмежень вирішення проблем за їх спрямованістю, пріоритетністю й ресурсним потенціалом; визначення базового варіанту структури проблем та їх кінцево-цільової спрямованості та зразок оцінки соціально-економічної ефективності базового варіанта структури; розробка можливих профілактичних засобів запобігання повторенню проблем чи загостренню протиріч.

Це потребує певних дій з боку системи управління підприємствами телекомунікацій в Україні для мотиваційного впливу за допомогою вирішення проблем системи управління на усіх соціально-економічних рівнях об'єкта та приведення останнього на бажаний фінансово- економічний та соціальний рівень. Але це вимагатиме певних, конкретних обмежень на виробництві й використання трудових і матеріальних ресурсів.

Література:

1. Чекаліна М.А. Принципи стратегічного планування на підприємстві/ М.А. Чекаліна // Вісник ОДУ. – 2009. – № 1. – С. 83-89.
2. Кузьмінов А.В. Узгодження мотиваційних впливів на ефективність механізму управління телекомунікаціями регіону: дис. ... канд. екон. наук: 08.07.04 / А.В. Кузьмінов, Одеська національна академія зв'язку ім. О.С. Попова. – Одеса, 2005. – 224 с.
3. Економіка телекомунікацій: навч. посіб. [для студентів вищих навчальних закладів]; за заг. ред. В.М. Орлова. – О.: ОНАЗ ім. О.С. Попова, 2014. – 512 с.

Цапко Єлизавета Євгенівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

ЩО ТАКЕ 4G?

Четверте покоління мобільного зв'язку – 4G, fourth generation або LTE (Long Term Evolution). Найпоширеніша у світі технологія бездротової передачі даних. Стандарт виник у минулому десятиліттi, робота над його створенням розпочалася ще в 2004 році. Перші комерційні запуски 4G-мереж розпочалися в 2009-2010 роках. У 2012 році у 48 країнах світу працювало 108 мереж 4G/LTE.

За даними Ericsson, на кінець першого кварталу 2017 року у світі нараховувалося 2,1 млрд LTE-користувачів. У 189 країнах світу працювала 591 мережа четвертого покоління. Якщо 3G Україна запустила у 2015 році - із запізненням щонайменше на десять років, то відставання із запровадженням 4G/LTE уже складає сім-вісім років. Із 5G наш уряд також не квапиться, на відміну від Південної Кореї та Японії. Ці країни пообіцяли запустити мережі п'ятого покоління впродовж наступних одного-двох років.

Очевидно операторам, щоби після отримання 4G-ліцензій запустити нову технологію, потрібно буде кілька місяців. Наприклад, 3G-тендер відбувся в лютому 2015 року, а вже в травні-червні цього ж року оператори оголосили про запуски своїх перших мереж третього покоління у найбільших містах України.

Велика трійка операторів – Київстар, Vodafone Україна та lifecell – звісно ж, найбільше зацікавлені в отриманні 4G-ліцензій. Але уряд неодноразово заявляв про можливість взяти участь у торгах інших гравців. Як буде насправді – залишилося зачекати, коли буде оголошений та проведений розпродаж радіочастот. НКРЗІ заявила, що спочатку виставить на продаж радіочастоти в діапазоні 2600 Мегагерц (МГц). Саме ці радіосмуги, як запевнили державні мужі, найбільше готові до тендеру. Однак три згадані оператори зацікавлені насамперед в купівлі ліцензій на 1800 МГц. Вірогідно, цей тендер пройде другим.

Чому спектр 1800 МГц для операторів цікавіший, ніж 2600 МГц? Чим вища частота, тим менший радіус покриття однієї базової станції (БС). Відповідно, у "вищому" діапазоні треба буде наставити значно більше БС, ніж у "нижчому". А більше БС дорівнює більше витрат.

Як і у випадку з 3G, оператори будуватимуть свої 4G-мережі, починаючи з найбільших міст України – там, де найбільший платоспроможний попит. Серед перших кандидатів - міста-мільйонники. Це, звісно ж, Київ, Дніпро, Одеса, Харків, Львів. Далі 4G розповсюджуватиметься дещо меншими містами. Для того, щоби ваш смартфон зміг підключитися до четвертого покоління мобільного зв'язку, він має бути відповідно оснащеним. Це можна перевірити в налаштуваннях. Згідно даних найбільших операторів, більшість сучасних смартфонів, які потрапляють на прилавки українських крамниць останніми роками, підтримують 4G. Однак ви можете переконатися, чи зможете користуватися новим стандартом зв'язку – коли він з'явиться – вже зараз.

Наприклад, четверте покоління мобільного зв'язку підтримують усі iPhone, починаючи з 5-ї серії, а також смартфони Samsung, випущені з 2016 року.

5G – це назва технології, яка слідуватиме за 4G-мережами, що вже існують. Незважаючи на активне тестування, його стандартизація очікується не раніше 2020 року. По суті, п'яте покоління – це не один стандарт, а цілий комплекс технологій, як вже наявних, так і абсолютно нових.

Варто розрізняти максимально можливу швидкість з технічної точки зору, і реальну швидкість, яка буде доступна користувачам. Так, під час тестування досягалися пікові показники 25,3 Гбіт/с. Якщо говорити про швидкості комерційних мереж, очікується, що в 5G вони досягнуть 10 Гбіт/с. Для порівняння, максимально можлива швидкість нинішніх

3G-мереж в Україні – 63 Мбіт/с, а реально доступна для абонентів – близько 5-10 Мбіт/с, що залежить від якості покриття мережі, а також навантаження на мережу, яку створюють мобільні абоненти.

Важливо відзначити, що вперше в історії розвитку телекомунікацій швидкість не буде визначальним фактором. Більш важливим стане надійність мереж, нульова затримка і здатність підлаштовуватися під конкретні завдання і потреби додатків.

Досягти таких показників буде можливо завдяки комбінації багатьох факторів. По-перше, планується використовувати більш широкі смуги частот, а удосконалений 5G радіоінтерфейс дозволить пропускати в кілька разів більше даних.

По-друге, швидкість і пропускну здатність збільшить застосування технології Massive MIMO, яка передбачає використання кількох антен на прийомопередавачах. Ця технологія застосовується вже зараз в наявних мережах 4G, але в майбутньому кількість антен буде збільшено. Важливою відмінністю мережі п'ятого покоління буде її можливість «підлаштовуватися» під абонента. На практиці це означає, що 5G буде «дробити» мережу на віртуальні сегменти (network slicing), кожен з яких буде виділено під певні потреби. Це дасть можливість її одночасного максимально ефективного використання для різних додатків – це буде єдина мережа для мільйонів різних потреб.

П'яте покоління – це базис, необхідний для цифрової трансформації бізнесу, суспільства і держави в цілому. Незважаючи на те, що технічні характеристики широкосмугового доступу п'ятого покоління все ще знаходяться на стадії розроблення, вже сьогодні очевидно, що ефект від застосування цієї технології вийде далеко за межі телекомунікаційного бізнесу.

Мобільні мережі стануть важливою частиною інфраструктури для розвитку ключових галузей, а отже, і економіки в цілому. За прогнозами Ericsson, до 2026 року запуск стандарту п'ятого покоління призведе до виникнення зовсім нового ринку обсягом $582 млрд на глобальному рівні.

Наведу кілька прикладів. Завдяки практично нульовий затримці стане реальністю віддалене управління важкою промисловістю, що дозволить підвищити безпеку для співробітників і знизити вартість виробництва.

Також, дистанційною може стати хірургія, можна сказати, що 5G дозволить передавати по мережах не тільки інформацію, але й практичні вміння, розвиваючи новий напрям – Internet of Skills.

Ми станемо свідками розвитку розумних транспортних систем – зрештою, нас чекає безпілотне автомобільне майбутнє – вже у 2020 році на дорогах світу, в цілому, буде колесити 10 млн розумних транспортних засобів.

І це лише кілька прикладів. Для простих користувачів нові технології будуть означати ще більшу швидкість доступу до інтернету 24/7 в будь-якому місці. Високоякісний розважальний центр буде завжди в нашій кишені.

Література:

1. *www.cikavosti.com*
2. *www.politeka.net*
3. *www.nv.ua*

Четверикова Тетяна Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

АНАЛІЗ МОДЕЛЕЙ УПРАВЛІННЯ РЕСУРСАМИ ТА НАВАНТАЖЕННЯМ КАНАЛІВ ПЕРЕДАЧІ В ТЕЛЕКОМУНІКАЦІЯХ

Проблема створення і забезпечення ефективного функціонування та управління ресурсами та навантаженням каналів передачі телекомунікаційних систем досить часто постає перед організаціями та корпораціями із розвиненою розподіленою інфраструктурою. Вкладаючи свої кошти ці компанії сподіваються на якісну роботу таких інформаційних систем та очікують зменшення витрат на експлуатацію, зниження вартості обслуговування користувачів, що дозволить закласти основу для більш ефективної діяльності самої компанії та їх клієнтів. Клієнти своє бачення роботи такої структури погоджують із компанією на рівні вимог, до яких належать: вартість таких послуг, доступність та керованість інфраструктури, цілісність даних, безпека, надійність. Досягнення такого рівня вимог користувачів із найменшими коштами та ресурсами становить сутність проблеми створення і забезпечення функціонування телекомунікаційної системи. Загалом таку комплексну інформаційну проблему розбивають наряд проблем менших розмірів, хоча не набагато простіших. Однією із таких є проблема управління ресурсами і навантаженням телекомунікаційної системи. Тут необхідні гнучкі рішення, які ґрунтуються на оцінюванні та прогнозуванні стану ресурсів, обсягів навантаження і полягають у правильному балансуванні навантаження та ефективному розподілі ресурсів

телекомунікаційної системи. Для прийняття коректних правильних рішень необхідні інструментарій та комплекси методик для вирішення задач підтримки інфраструктури телекомунікаційної системи. Створення такої структури становить достатньо важливу проблему, розв’язання якої вимагає досить глибокого розуміння процесів, які відбуваються в телекомунікаційних системах, функціонування інфраструктури, чіткої постановки конкретних задач аналізу та дослідження, розроблення нових математичних моделей та відповідних методів вирішення задач і реалізацію розроблених методик.

Постановка проблеми

У статті досліджуються та розглядаються питання вирішення задачі аналізу моделей управління ресурсами та навантаженням каналів передачі в телекомунікаційних системах. Необхідно проаналізувати моделі та алгоритми управління телекомунікаційною інфраструктурою організацій і підприємств з урахуванням завантаженості каналів передачі системи. Оскільки моделі залежать від багатьох чинників, то в статті буде проаналізована класифікація потрібних для реалізації системи управління інфраструктурою моделей і алгоритмів із урахуванням цих чинників як ознак класифікації. Потрібні моделі визначаються комбінаціями необхідних параметрів. Одна з ознак параметрів передбачає відмінність моделей у залежності від цілей роботи телекомунікаційної системи – управління інфраструктурою для підтримки власних процесів чи надання послуг зовнішнім клієнтам. Такий поділ буде впливати на вид критерію, який використовується у відповідній моделі. Іншою ознакою є технологічні особливості інфраструктури телекомунікаційної системи, які обумовлені архітектурою її побудови. Загалом ці ознаки будуть впливати на всі елементи моделі. Залежно від етапу життєвого циклу, на якому знаходиться телекомунікаційна система виникають різні задачі. Тому на етапі планування крім технологічних та ресурсних обмежень можуть використовуватись також і інші обмеження, наприклад вартість чи надійність.

Рівень доступних ресурсів буде впливати на складність моделі задачі. Суттєво буде впливати на вид моделей остання ознака – це забезпеченняресурсами. У загальному вигляді необхідно проаналізувати моделі, що складаються з критерію, який потрібно мінімізувати чи максимізувати, ресурсних обмежень, технологічних та інших обмежень. Це дасть змогу більш адекватно під лаштувати параметри до умов функціонування конкретної телекомунікаційної системи та дозволить зменшити час простою системи та уникнути передачі неінформативних даних. Виклад основного матеріалу дослідження

Аналіз моделей, які використовуються для управління ресурсами і навантаженням інфраструктури в телекомунікаційних системах показує, що популярність набувають технології серверної віртуалізації, які дозволяють зменшити вартість придбання серверної частини структури та скоротити витрати на її утримання і використання. Аналіз показує це дає можливість «живої міграції» віртуальних машин між фізичними серверами та дозволяє отримати показники надійності рішень у кластерах.

Пінчук Ольга Валентинівна
Державний університет телекомунікаці
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

РОЛЬ ТА ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Все просто, під телекомунікацією прийнято розуміти весь комплекс технічних засобів, які призначені для передачі інформації на будь-яку відстань. До цього комплексу технічних засобів можна віднести: звук, сигнал, текст, знак, письмове зображення і багато інших видів. Всі ці кошти передаються по кабельній, оптичної, радіо- і інших електромагнітних системах. Система технічних засобів, за допомогою якої здійснюється телекомунікація, називається мережею телекомунікацій. Телекомунікаційна мережа має одну з важливих характеристик всієї розглянутої технології: вона надає можливість отримання необхідної інформації або даних для забезпечення діяльності будь-яких учасників телекомунікації або ж для задоволення особистих потреб користувачів.

Хоч в наш час телекомунікаційні мережі досить розвинені дуже актуальні, але не можна забувати про те, що наше суспільство щодня розвивається, з кожним днем збільшуються різні пізнання і тому на одному місці наука не стоїть і не буде стояти ніколи. Таким чином, телекомунікації також йдуть в ногу з часом і мені хочеться перерахувати перспективні напрямки телекомунікаційних технологій:

1) створення інтелектуальних антенних пристроїв з поліпшеною енергетикою;

2) створення телекомунікаційних систем в дуже маленькому діапазоні хвиль (~ 1 мм) з робочою частотою, яка сягатиме до 100 ГГц;

3) створення нових сигнально- кодованих конструкцій шляхом застосування комбінування методів маніпуляції сигналів і нових методів кодування сигналу з метою збільшення пропускної здатності систем передачі і поліпшення їх енергетики;

4) розробка нових методів проектування та виробництва обладнання телекомунікацій, що забезпечує появу більш потужних машин, які будуть виконувати величезну кількість завдань.

Також не варто забувати, що телекомунікації вже давно є частиною світу комп'ютерних технологій. І можливо, в найближчому майбутньому, повністю зануриться в цей світ. З телебаченням такий процес вже йде повним ходом. Більшість країн використовує цифрове мовлення, яке стрімко буде витісняти аналогове. Також телекомунікаційна індустрія заробляє непогані гроші і на продажу цифрових приставок для звичайних телевізорів, отримує можливість зробити деякі телевізійні канали на платній основі, як і в супутниковому мовленні.

І це ще не всі перспективи майбутнього в даному напрямку! Як ви помітили телекомунікації дуже тісно пов'язані з іншими науковими галузями, такими, як: фізика, енергетика, електроніка, комп'ютерні науки та незабаром мережі будуть охоплювати ще більше галузей.

Важливою проблемою розвитку телекомунікацій сьогодні є нерівномірність розвитку телекомунікацій, для позначення даної проблеми був навіть введений спеціальний термін «digital divide» (розрив на порядок і розподіл з використанням цифрових технологій). Дана проблема актуальна як на національному рівні

(нерозвиненість телекомунікацій в сільській і малонаселеній місцевості в силу нерентабельність надання телекомунікаційних послуг там через низьку щільності населення), так і в глобальному масштабі.

Розвиток телекомунікацій тісно пов'язаний з розвитком економіки - чим вище рівень розвитку економіки, тим вище рівень розвитку телекомунікацій. При цьому існує і зв'язок в зворотньому напрямку, зростання телекомунікаційної галузі, крім збільшення числа робочих місць збільшує ефективність інших галузей економіки.

Найважливішим фактором розвитку телекомунікаційної галузі поряд з технологічними змінами є реформування регулятивного середовища. Аналіз світового досвіду перетворення телекомунікаційної галузі з метою підвищення ефективності та розвитку конкуренції, а також основних сучасних тенденцій, дозволяє виявити основні напрямки реформування галузі:

- зміна структури галузі;
- регулювання приєднання мереж операторів, в тому числі міжоператорських
- тарифів;
- регулювання тарифів для кінцевих користувачів;
- надання соціально-значущих нерентабельних послуг зв'язку;
- зняття обмежень на іноземні інвестиції;
- розподіл обмежених ресурсів (перш за все частотного спектра);
- постійне відстежування нових послуг і створення найбільш сприятливих умов для них відповідність регулятивного середовища сучасним тенденціям розвитку телекомунікацій.

Література:

1. Технічна електроніка в телекомунікаціях: навч. посіб. для студ. спец. 6.050903 «Телекомунікації» Ін-ту телекомунікацій, радіоелектрон. та електрон. техніки / Я. В. Шийка, О. М. Яремко, С. С. Думич ; М-во освіти і науки, молоді та спорту України, Нац. ун-т «Львів. політехніка». Л. : [б. в.], 2011. 146 с. : іл. — Бібліогр.: с. 146 (5 назв).

2. Ефанов А.В., Формирование и тенденции развития телекоммуникационных ТНК //

3. Мировая экономика и международные отношения. – 2006. – №11. – С. 42-47.

4.

Шахмайкін Тимофій Олексійович
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

АНАЛІЗ СУЧАСНОГО СТАНУ ТЕЛЕКОМУНІКАЦІЙ УКРАЇНИ

Проведено дослідження стану розвитку інформаційного та телекомунікаційного ринку України. Встановлено те що тенденції розвитку галузі характеризуються зростанням доходів від всіх форм діяльності. Доведено, що прискореним темпом розвиваються послуги з надання кабельного телебачення , а також доступу до мережі Інтернет. Визначено, що основними сегментами на ринку телекомунікаційних послуг залишаються мобільний, фіксований та широкосмуговий (комп'ютерний) зв'язок, проведено аналіз рейтингу пошукових систем.

Актуальність дослідження даної теми визначається тим фактом, що однією із загальносвітових тенденцій є розвиток інформаційного суспільства. Динаміка цього процесу, його результати для громадян, суспільства та держави значною мірою залежать від обґрунтованості відповідної державної політики та управління, які повинні формуватися на основі достовірної, точної, своєчасної та повної інформації. На сьогодні розвиток інформаційного суспільства, поширення інформаційних технологій(ІТ) в усі сфери життєдіяльності людини та суспільства стали нормою подальшої еволюції цивілізації. Всіма фахівцями усвідомлено, що розвиток ІТ створює засади сучасної економіки та добробуту людини.

Метою статті є дослідження стану розвитку інформаційного та тлекомунікаційного ринку України. Найбільш повне та суттєве тлумачення поняття інформатизації надано у Законі України "Про національну програму інформатизації". В ньому наголошується, що інформація є сукупністю взаємопов'язаних організаційних, правових, політичних, соціально-економічних, наукво-технічних, виробничих процесів, які направлені на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку та використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки». Міжнародний союз електрозв'язку (МСЕ) виділяє триступеневу модель, за якою країни або регіони рухаються у розвитку інформаційного суспільства. Її першим етапом є мережева готовність, яка відображається поширенням інфраструктури ІТ в суспільстві або країні, ступінь доступу приватних осіб, підприємств та організацій до цієї інфраструктури. Другий етап включає інтенсивність, зокрема, ступінь впровадження ІТ. Третій етап характеризується ефективністю використання ІТ в конкретному суспільстві або регіоні.

Україна рухається в розвитку інформаційного суспільства повільними темпами, при поточних темпах ІТ-розвитку відстає від інших країн, що й спостерігається сьогодні. За даними Держкомстату сукупний індекс капітальних інвестицій за період січень– березень 2014 р. у відношенні до відповідного періоду 2013 року склав 103 %, в той же час, в сфері «Інформація та телекомунікації» він дорівнює 92,4 %. Більш того, якщо з цієї сфери вилучити інформаційну або медійну частину, то обсяг капітальних інвестицій у ІТ-сферу складе 1288,4 млн. грн., а це менш ніж 2,5 %. Тенденції розвитку галузі характеризуються зростанням доходів від всіх форм діяльності. За період 2015–2017 рр. доходи збільшились на 13,4 % і склали на грудень 2017 р. 52271,1 млн. грн. Також слід зазначити, що кожного року зростає доля надання послуг населенню. Якщо на 2009 р. доходи від надання послуг населенню складали 40,63 % від загальних доходів від надання послуг, то вже на 2013 р. ця частина зросла до 64,65 % [4]. Прискореним темпом розвитку характеризуються послуги з надання кабельного телебачення, а також доступу до мережі «Інтернет». За результатами міжнародних досліджень, рейтинги України за окремими індексами, що стосуються впровадження інформаційних технологій на 2012 рік склали : – глобальний індекс конкурентоспроможності 2011–2012 рр. (WEF Global Competitiveness Index) – 82 місце (89 – у 2011 р.) із 142 країн; індекс технологічної готовності 2011–2012 рр. (WEF Technological Readiness Index) – 82 місце із 142 країн; індекс мережевої готовності 2011–2012 рр. (WEF Networked Readiness Index) – 75 місце (90 – у 2011 р.) із 142 країн; Е-готовність уряду (Government readiness) – 122 місце із 138 країн; використання урядом ІКТ (Government usage) – 75 місце із 138 країн; рейтинг за електронною готовністю 2010 (EIU eReadiness Ranking) 64 місце із 70 країн; індекс електронного уряду ООН 2012 (UN e-Government Index) – 68 місце (54 – у 2011 р.) із 193 країн. Якщо порівняти рівень проникнення ІТ в Україні з рівнем проникнення у таких країнах, як Росія та США, то наочно можна побачити, що хоча за кількістю користувачів Україна значно відстає, але за темпами розвитку значно випереджає . В Україні для підтримки ІТ-галузі були прийняті закони "Про державну підтримку розвитку індустрії програмної продукції" та були внесені зміни в Податковий кодекс України, що встрановлюють особливий порядок оподаткування для ІТ-сфери. Незважаючи на це, діючі в Україні умови для розвитку іТ-бізнесу за обсягом стимулів для розвитку відповідної галузі значно поступаються тим, що створені у традиційних аутсорсингових локаціях, зокрема в Індії, Росії, Білорусі. Окрім того, практичне застосування відповідних норм Податкового кодексу не відпрацьовано на рівні деталізації, що забезпечувало б безперешкодне використання зазначених пільг. Як наслідок, протягом року після прийняття відповідного законодавства, спеціальним режимом оподаткування для ІТ компаній скористалися близько 200 ІТ компаній з більше ніж 2000, що свідчить про невідповідність наданих стимулів потребам бізнесу.

Отже ступінь розбудови інформаційного суспільства в Україні стримується такими перешкодами: недосконала загальнодержавна політика, політична та економічна нестабільність; недосконаліть законодавства; назька інвестиційна активність; відсутність единої державної технічної та інвестиційної політики; впровадження електронного урядування уповільнено та недостатньо координовано; відсутність мотивації та координації дій операторів телекомунікацій; наявність значного ‘цифрового розриву’ у використанні ІКТ; загострення проблем та ризиків, пов'язаних з інформаційною безпекою.

Література:

1. *Широкополосные беспроводные сети передачи информации/ В.М. Вишневский, А.И. Ляхов, С.Л. Портной, И.В. Шахнович.- М.: Техно-сфера, 2005.- 592 с.*
2. *Энциклопедия WiMAX путь к 4G/ В.М. Вишневский, С.Л. Портной, И.В. Шахнович.- М.: Техносфера, 2009.- 472*
3. *Современные беспроводные сети: состояние и перспективы развития./ И.А. Гепко, В.Ф. Олейник, Ю.Д. Чайка, А.В. Бондаренко. К.:ЭКМО,2009.-672 с.*
4. *Розподілені сервіси телекомунікаційних мереж та повсюдний комп’ютинг і CLOUDтехнології / А.О. Лунтовський, М.М. Климаш, А.І. Семенко.-Львів, 2012.-368 с.*

Григор’єва Ганна Юріївна
Приватний вищий навчальний заклад
«Київський медичний університет»
м. Київ

ОСНОВНІ ЗАСАДИ СИСТЕМИ МЕНЕДЖМЕНТУ ЯКОСТІ У ЗАКЛАДІ ВИЩОЇ ОСВІТИ

Із входженням України до Європейського освітнього простору, однією з необхідних умов підтвердження свого статусу будь-яким українським вищим закладом вищої освіти є наявність системи менеджменту якості (СМЯ). Знаходячи в умовах жорстокої конкуренції заклади освіти відчувають потребу у розробці таких систем, з метою отримання результативності від її впровадження. За таких обставин заклади вищої освіти все частіше намагаються застосувати моделі менеджменту якості [1], що побудовані з дотриманням вимог міжнародних стандартів ISO серії 9000.

Система менеджменту якості підлягає сертифікації і є одним із поширених міжнародних засобів підтвердження якості освітньої діяльності закладу вищої освіти [2].

Сертифікація системи менеджменту якості закладу освіти дає ряд переваг перед іншими, а саме:

- підвищення іміджу та рівня управління закладом освіти;
- має переваги при отриманні грантів, укладанні договорів з інвестиційними кампаніями;
- вийти на світовий рівень з підготовки іноземних громадян.

Основними принципами менеджменту якості освітнього процесу у закладі вищої освіти є:

- орієнтація на споживача освітніх послуг;
- лідерство керівництва і залучення співробітників у процеси менеджменту;
- процесний підхід до керування;
- системний підхід до менеджменту;
- постійне поліпшення системи якості;
- прийняття рішень, що базуються на фактах

Створення та сертифікація системи менеджменту якості у закладах вищої освіти є приорітетним завданням в умовах інтеграції вищої освіти в європейській освітній простір.

Список використаної літератури:

1. І.М.Шоротура, Є.В.Долинський, О.О.Долинська Менеджмент вищої освіти. Навчальний посібний. СПбю: Видавництво Львів, 2014. – 560с.
2. Менеджмент качества у ВУзе / под. ред.. Ю.П.Похолкова,, А.И.Чучалина.- М:Логос, 2010, - 206с.

Наукове видання

«СВІТ ТЕЛЕКОМУНІКАЦІЇ ТА ІНФОРМАТИЗАЦІЇ»

Збірник матеріалів
VI Міжнародної науково-технічної конференції студентства та молоді

Київ, 17 травня 2018 року

Редагування: Соснова Д.Н., Щетініна А.А., Перепелиця Л.С., Лазоренко А.В.

Відповідальні за випуск: Соснова Д.Н., Щетініна А.А., Перепелиця Л.С., Лазоренко А.В.

Подано до друку 06.12.17
Формат 60х84. Папір друкарський. Гарнітура «Time New Roman».

Державний університет телекомунікацій
вул. Солом'янська, 7, м. Київ, 03110, Україна

Для нотаток

Для нотаток