VIII НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ СТУДЕНТІВ ТА МОЛОДИХ ВЧЕНИХ ФАКУЛЬТЕТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

СУЧАСНІ ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

ЗБІРНИК ТЕЗ

25 травня 2019 р

КИЇВ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
VIII НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ СТУЕНТІВ ТА МОЛОДИХ ВЧЕНИХ

СУЧАСНІ ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

25 травня 2019 року

ЗБІРНИК ТЕЗ

м. Київ

Науково-технічна конференція «Сучасні інфокомунікаційні технології» Збірник тез. К.ДУТ, 2019 – 51 с.

Даний збірник містить тези учасників конференції, представлених на VIII Науков -технічній конференції студентів та молодих вчених Навчально-наукового інституту інформаційних технологій «Сучасні інфокомунікаційні технології», яка проводилась 25 травня 2019 р. в Навчально-науковому інституті інформаційних технологій Державного університету телекомунікацій, м.Київ.

Робоча мова конференції – українська.

У збірнику представлені тези доповідей VIII Науково-технічної конференції студентів та молодих вчених Навчально-наукового інституту інформаційних технологій «Сучасні інфокомунікаційні технології». Розглянуті сучасні проблеми розвитку науки і техніки та визначено шляхи їх вирішення.

Вчений секретар конференції
Сайдакова Н. Ф.
моб.тел.+38(097)7568934
e-mail: nata.saydakova@ukr.net

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Державний університет телекомунікацій
Факультет Інформаційних технологій

ПРОГРАМНИЙ КОМІТЕТ

Бондарчук А.П. – к.т.н., доцент, декан факультету Інформаційних технологій Державного університету телекомунікацій

Онищенко В.В. – д.т.н., завідуюча кафедри Інженерії програмного забезпечення Державного університету телекомунікацій

Вишнівський В.В. – д.т.н., завідувач кафедри Комп'ютерних наук Державного університету телекомунікацій

Шушура О.М. – к.т.н., завідувач кафедри Системного аналізу Державного університету телекомунікацій

Сторчак К.П. – к.т.н. завідувач кафедри Інформаційних систем і технологій Державного університету телекомунікацій

ЗМІСТ

Векслер Л.Б.
студентка групи ІМД-42

ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ У ОСВІТНЬОМУ ПРОЦЕСІ: GOOGLE FORMS

Як свідчить світовий і вітчизняний досвід, результативність функціонування сучасного освітнього закладу будь-якого типу визначається багатьма показниками, серед яких важливе місце займає ступінь упровадження в навчальний процес інформаційно-комунікаційних технологій (ІКТ). Це, у свою чергу, співвідноситься з формуванням комп'ютерно орієнтованого навчального середовища, яке забезпечує розвиток предметних і ключових компетентностей, створює умови для подальшої успішної навчальної і професійної діяльності випускника загальноосвітніх навчальних закладів. Державний стандарт базової і повної загальної середньої освіти визначає інформаційно-комунікаційну компетентність як ключову і передбачає внесок кожно-го навчального предмета у її формування. Для компетентнісного навчання історії, яке потребує якісної візуалізації, аналізу різноманітних подій і процесів, проблема науково обґрунтованого впровадження інформаційно-комунікаційних технологій є особливо актуальною. Щодо безпосередньої програми Google Forms, то здійснене дослідження має на меті розглянути аспекти зручності використання сервісу для роботи в історичній сфері діяльності.

Написання цієї статті було пов'язане з досягненням таких цілей:

— сформувати уявлення про основні теоретичні дані про хмарні сервіси (на прикладі хмарного сервісу Google Forms);

— визначити основні переваги та недоліки програми, сформувати практичні аспекти використання Google Forms у роботі історика.

Хмарний сервіс — це модель забезпечення мережевого доступу до обчислювальних ресурсів (мереж передачі даних, серверів, пристроїв зберігання даних, додатків і сервісів тощо). Першим, хто вжив словосполучення —«cloud computing», був Ерік Шмідт — генеральний директор компанії —«Google». До хмарних технологій належать сервіси електронної пошти, карти місцевості, он-лайн-редактори документів та графічних матеріалів тощо.

За допомогою сервісу можна створювати анкети, запрошувати на заходи, здійснювати розсилки для тих, хто підписався у анкетуванні.

Також існує можливість збирати статистичні дані, аналізувати результати опитувань і тестувань.

Google офіційно представила сервіс нотаток Forms, який передбачає роботу з формами у «хмарі», результати опитувань та тести. Однак найперше завдання програми — поліпшити взаємодію між респонден-том та

опитувачем.

Сервіс Google Forms дозволяє збирати статистику опитувань, дає можливість здійснювати розсилку тестування електронною поштою і отримувати результати. Всі вони у вигляді текстового повідомлення, а також у вигляді зображення.

Якщо більш детально, то програма дозволяє проводити опитування, зручно їх надсилати респондентам і збирати відповіді, а також створювати статистику на їх основі.

Важливим аспектом діяльності історика є робота з тестами, опитуваннями. Саме тому завдяки Google Forms історик має можливість у будь-який зручний для себе час проводити зрізи знань та отримувати статистику на їх основі.

ДЖЕРЕЛА

1. Хмарні обчислення [Електронний ресурс]. — Режим доступу : https:// uk.wikipedia.org/wiki/%D0%A5%D0%BC%D0%B0%D1%80%D0%BD%D1%96_%D0%BE%D0%B1%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D 0%BD%D1%8F.

2. [Електронний ресурс]. — Режим доступу : http://www.google.com.ua/intl/ ru/forms/about/. 3. [Електронний ресурс]. — Режим доступу : https://support.google.com/docs/ answer/87809?hl=ru.

4. Google Docs [Електронний ресурс]. — Режим доступу : https:// uk.wikipedia.org/wiki/Google_Docs#Google_.D0.A4.D0.BE.D1.80.D0.BC. D0.B0.

Векслер Л.Б.
студентка групи ІМД-42

ІНФОРМАЦІЙНО-ОСВІТНЄ СЕРЕДОВИЩЕ ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ

У зв’язку зі змінами, які відбулися у суспільному житті та, зокрема, в освіті, вкрай актуальними є питання інформатизації освітнього простору навчальних закладів. У результаті зростання інформаційних потоків постає потреба синхронізації навчального процесу, створення єдиного інформаційного середовища, спроможного його врегулювати.

Враховуючи потреби, можливості та вимоги студента щодо отримання та опрацювання інформації, у ВНЗ потрібно створити належну систему інформування студентів, забезпечити той рівень доступу до інформації, який задовольнить як потреби студентів, так і безпосередньо навчальних закладів.

Інформаційно-освітнє середовище ВНЗ можна вважати якісним за таких умов:

- наявність організаційної структури, у якій накопичуються та зберігаються інформаційні ресурси та надаються інформаційні послуги;

- наявність відповідної матеріальної бази, необхідної для створення інформаційно-освітнього середовища, використання нових інформаційних технологій (електронні каталоги, доступ до мережі Інтернет тощо) та ліцензійного програмного забезпечення;
- інформаційна грамотність учасників цього середовища.

Отже, важливим фактором якості інформаційного забезпечення є інформаційна інфраструктура навчального закладу. Створення такої інфраструктури є запорукою успішного впровадження інформаційних технологій в освіту на всіх її рівнях, що дозволяє комп'ютеризувати навчальну, виховну, управлінську та будь-яку іншу діяльність навчального закладу.

Векслер Л.Б.
студентка групи ІМД-42

Near field communication

NFC – це скорочення від «Near field communication», що означає «комунікація ближнього поля», або «ближня безконтактна зв'язок». Термін відноситься до змістового поля передачі даних і платіжних операцій, адже і сам цей метод є формою безконтактного платежу, який повинен бути максимально надійним і безпечним.

NFC – це стандарт для бездротової передачі даних, заснований на технології RFID.

Як уже згадувалося, абревіатура NFC означає «Near Field Communication», тобто зв'язок між двома елементами, які розташовані близько один до одного. Щоб передача в принципі була здійсненна, пристрої повинні розташовуватися на відстані кількох сантиметрів.

Це, в свою чергу, дає NFC найбільша перевага: він добре захищений від злому ззовні. Зрештою, щоб вкрасти ваші дані, потенційні хакери повинні будуть наблизитися до вас.

Хоча швидкість передачі 424 Кбайт – з нижче, ніж у Bluetooth – її цілком достатньо, щоб відправляти невеликі обсяги даних, наприклад, інтернет-посилання, за частки секунди. Таким чином, NFC забезпечує швидкий, простий і безпечний спосіб передачі даних на мобільний телефон без яких-небудь серйозних ризиків з точки зору безпеки, на відміну від альтернативних способів передачі даних.

Сфери застосування NFC

Оскільки NFC потрібен для передачі даних на короткі відстані, цей спосіб оплати особливо підходить для здійснення відносно невеликих переказів і тому часто використовується в області «мікроплатежів».

Обмін даними між смартфонами або планшетами: тут NFC сьогодні досить поширений. Наприклад, якщо ви з'єднаєте два Android-пристрої з чіпом NFC, то зможете перенести дані одним клацанням миші – це можуть бути, наприклад, посилання, контактна інформація або навіть фотографії.

Безготівковий платіж: багато супермаркетів пропонують платіжне обслуговування, яке працює з NFC. Досить прикласти до терміналу смартфон або кредитну карту з підтримкою NFC – з'єднання встановлюється і списується потрібна сума. Це абсолютно безпечно і набагато швидше, ніж традиційні методи.

Передача інформації за допомогою тегів NFC: також можливо, що в майбутньому NFC-чіпи можуть бути використані в рекламі – через них можна буде також передавати інформацію, наприклад, відповідний запис у календарі або посилання на веб-сайт. Зацікавлені особи зможуть приватно купувати теги NFC і програмувати їх для смартфона за допомогою спеціальних команд.

NFC в київському метро

Смартфон як вхідний квиток: також легко уявити, що квитки, наприклад, на концерт, можна буде просто зняти на смартфон, а при вході – тільки прикласти його до зчитувального пристрою. У Києві з 2015 року NFC-оплата проїзду у метро. Слід зазначити, що цього року під час конференції Google I/O, система оплати NFC у київському метрополітені була визнана однією з найпрогресивніших у світі. У ряді прогресивних також були компанії з Сіднею, Лондона та Чікаго.

Також пропонують можливість безконтактного платежу європейські банки, хоча їх поки небагато, а в деяких коледжах і університетах Європи студенти можуть використовувати чіпи NFC в своїх посвідченнях для передачі невеликих сум грошей.

Література:

1. Near Field Communication (NFC) Technology and Measurements
https://ru.wikipedia.org/wiki/Near_Field_Communication

2. Near Field Communication (NFC) Technology and Measurements
https://tmginfo.net/2018/05/shho-take-komunikaciya-blizhnogo-polya/

Чудеса В. О.
студент групи ТСД-42
Коршун Н.В.
професор кафедри телекомунікаційних систем та мереж д.т.н., доцент

АНАЛІЗ РОЗВИТКУ ЛОКАЛЬНИХ МЕРЕЖ НА БАЗІ ТЕХНОЛОГІЇ Wi-Fi

За прогнозами фахівців, в 2019 році загальна кількість проданих мобільних пристроїв перевищить три з половиною мільярди, з них один мільярд - це «звичайні» мобільні апарати, другий – смартфони і півтори планшети та пристрої які підтримують Wi-Fi з`єднання. У минулий 2018-й рік більшість всих мобільних пристроїв стала мати можливість роботи з Wi-Fi. Таким чином, найближчим часом користування мобільними пристроями і портативною технікою стане масовим і повсюдним.

У найближчі кілька років можна очікувати подальшого розвитку лінійки Wi-Fi рішень.

За останній час IEEE стандартизовані наступні специфікації:

- IEEE 802.11mb - технічне обслуговування стандарту;
- IEEE 802.11aa - Робастное потокове аудіо і відео;
- IEEE 802.11ac - забезпечення високошвидкісної передачі для діапазонів нижче 6 ГГц (2013 рік);
- IEEE 802.11ad - забезпечення високошвидкісної передачі для діапазону 60 ГГц (2012 рік);
- IEEE 802.11ae - управління якістю;
- IEEE 802.11af - Wi-Fi з використанням когнітивного радіо.

Очікується стандартизація специфікацій:

- IEEE 802.11ai - забезпечення ефективного початкового доступу;
- IEEE 802.11ah - освоєння діапазонів нижче 1 ГГц.

В якості ефективного механізму забезпечення інформаційної безпеки в сучасних рішеннях Wi-Fi використовуються рішення специфікації IEEE 802.11i і механізми встановлення автентичності EAP; обидва рішення мають сертифікати Wi-Fi Alliance's Wi-Fi Protected Access 2 (WPA2) -Enterprise certification. Технологія WPA2 заснована на стандарті IEEE 802.11i і являє собою 128-бітове AES-шифрування з перевіркою достовірності на основі попередніх ключів (PSK) або стандарту 802.1x RADIUS, що добре підходить для реалізації функцій управління авторизацією, аутентификацией і адміністрування (AAA).

Майже всі бездротові мережі мають справу з широким розмаїттям термінальних пристроїв, як за допомогою SIM-карти (наприклад, смартфони), і без обходиться їм (наприклад, планшетні комп'ютери, ноутбуки і нетбуки). Саме з цієї причини, що Wi-Fi гарячих точок доводиться підтримувати нове покоління альтернативних і аутентифікації EAP-SIM механізмів, таких як протокол X.509. рис. 1 представлений прогноз проникнення термінальних пристроїв в Wi-Fi мережі.

Рис. 1. Прогноз проникнення термінальних пристроїв в Wi-Fi

Таким чином, за останні роки технологія Wi-Fi зазнала ряд поліпшень, що дозволило створювати досить недороге обладнання, яке за рахунок високої швидкості передачі (до 600 Мбіт/с) і доступного широкого спектра (до 500 МГц) є цілком конкурентоспроможним на тлі стільникових мереж 2G/3G/4G.

Перелік використаної літератури:

1. Dunat, J. C., Elicegui, L., & Bonnet, C. Impact of inter-cell interference in a IEEE 802.11 a network with overlapping cells// Power.- 2014.- Ns 20.- p.20.

Антоненко А. А.
студент групи ІМД-41

МОДЕЛЮВАННЯ ТА РОЗРОБКА АНТЕННОГО ПІДСИЛЮВАЧА УКХ ДІАПАЗОНУ ЧАСТОТ ДЛЯ ЗБІЛЬШЕННЯ ДАЛЬНОСТІ РАДІОМОНІТОРИНГУ

На сьогоднішній день управління складними системами не можливе без використання засобів зв'язку. В даний час найбільш використовуваним і перспективним, вважається ультракороткохвильовий (УКХ) діапазон, тому що він насичений різними системами зв'язку з великою різноманітністю послуг і можливостей. Це призводить до потреби моніторингу за цими засобами . За допомогою радіомоніторингу можна визначити місцезнаходження джерел і перехопити повідомлення які дозволяють визначити характер дій і стан об'єктів випромінювання. На сьогоднішній день є необхідність підвищення дальності радіомоніторингу.

В даній роботі ми розглядаємо актуальність розробки антенного підсилювача, для ведення радіомоніторингу на великих відстанях, обираємо радіоприймальни й пристрій та тип антени, який будемо використовувати. Також проведемо розрахунок дальності радіозв'язку. В другому розділі ми

обираємо підсилювач електричних сигналів , обираємо структурну та функціональну схеми та транзистор, який би повністю відповідав нашим вимогам , розробляємо принципову схему антенного підсилювача, проводимо всі необхідні розрахунки для подальшої роботи. В третьому розділі ми моделюємо роботу розробленого підсилювача за допомогою системи автоматизованого програмування і переконуємося в тому, що підсилювач виконує свої функції і ми бачимо підсилений в декілька разів сигнал.

Отже, виконавши поставлені завдання, у дипломній роботі було проаналізовано засоби радіовипромінювання в УКХ діапазону з огляду на те, що він насичений різними системами зв'язку з великою різноманітністю послуг і можливостей, розроблено та перевірено на працездатність антенний підсилювач.

Використана література

1. Черникова Б.Л., Чернишова О.В. Распространение радиоволн. Учебник для вузов связи/ – Москва: издательство “Радио и связь”, 1984. – 272с.

2. М. Т. Иванов, А. Б. Сергиенко, В. Н. Ушаков. Теоретические основы радиотехники: Учеб. пособие / Под ред. В. Н. Ушакова. — М.: Высш. шк., 2002. — 306 с.
3. Воскресенский Д.И., Гостюхин В.Л., Максимов В.М., Пономарев Л.И. Устройства СВЧ и антенны, Радиотехника, 2006. — 376 с.

Єденач О.В.
студент групи КСД-42

ВІДМІННОСТІ МІЖ ТЕХНОЛОГІЯМИ 4G ТА LTE

В останні 5 років бездротові технології передачі даних зробили величезний крок вперед. Якщо пару років тому все задовольнялися мережею третього покоління і лише у великих містах була добре поширена мережа 4G, то на сьогоднішній день високошвидкісний інтернет для телефонів і планшетів доступний на більшій території України. У даній статті ви дізнаєтеся відповіді на всі ваші запитання з приводу LTE і 4G - це одне і те ж чи ні, як їх розрізняти і що вибрати.

Ви напевно помічали, що в описі смартфонів/планшетів з підтримкою мережі четвертого покоління постійно використовується приставка Long Term Advanced. Також справа йде і з операторами. Компанії в усіх назвах і характеристиках вказую-ть 4G ЛТЕ. Через це у користувачів і клієнтів виникає думка, що це одне і те ж. Ви-робники телефонів і провайдери ж не акцентують увагу на подібності та відміннос-ті. Насправді, ніякого обману з боку компаній в цьому немає. Використання двох понять разом потрібно тільки для залучення покупців. З одного боку, 4G і LTE на-лежать одному поколінню, з іншого ж - в них є кілька відмінностей, які слід знати кожному користувачеві. Почнемо з визначення цих двох понять і розберемося, яка різниця між ними.

Що таке 4G?

Розшифровується абревіатура як 4generation, тобто четверте покоління. У 2008 році цей стандарт був визнаний конвенцією з розвитку бездротових техноло-гій в Женеві. Максимальна обіцяна пропускна здатність даного виду зв'язку стано-вить 1Гб / с (для стаціонарних абонентів) і 100Мб / с (для рухомих абонентів). В четверте покоління входить два типи технології бездротового інтернету - це LTE і WiMAX 2. Однак перші появи технології в масах не задовольняли творців і корис-тувачів, адже швидкість значно відрізнялася від заявленого максимуму в гіршу сто-рону. Однак під впливом маркетингу і необхідність просування новинки в маси, те-хнологія продавалася під виглядом повноцінного 4G. Щоб розібратися, в чому різ-ниця між LTE і 4G, потрібно знати, що ЛТЕ є проміжним етапом розвитку бездро-тового зв'язку. Повноцінне покоління 4G з'явилося з виходом так званого 4G+ або LTE Advanced, яке подається під оболонкою «розігнаного» інтернету. Але насправ-ді, саме таку швидкість і повинен показувати звичайний 4G стандарт. І це далеко не межа для четвертого покоління бездротової мережі.

Що таке ЛТЕ?

Тепер розглянемо ЛТЕ, як окремий вид передачі даних по повітрю. Абревіа-тура розшифровується як Long Term Evolution, що перекладається як довгостроко-вий розвиток. ЛТЕ є першим етапом розвитку 4G на самому початку його появи. Характеристики та можливості цієї мережі не відповідають вимогам Міжнародного союзу електрозв'язку, однак для залучення людей виробники використовують ЛТЕ під виглядом повноцінного 4G. Згодом союз схвалив використання цих двох понять в одній маркування, через що вона існує донині. Коли технології дозволяють домог-тися заявлених швидкостей, оператори стали пропонувати повноцінний 4Г (або як його назвав МСЕ - True 4G) за 4G+ або Advanced. Тепер ви знаєте головна відмінні-сть 4G від LTE. Зрівнятися за параметрами з ЛТЕ може технологія HSPA+. Напевно багато хто помічає, що іноді при поганому сигналі з'являється значок H+. Цей тип бездротового зв'язку відноситься до третього покоління (3G) і пропонує більш ск-ромну швидкість передачі даних. Порівняння швидкостей: 4g vs LTE Головна проб-лема технології ЛТЕ в тому, що вона забезпечує дуже низьку швидкість віддачі в порівнянні з «справжнім 4G»: 4G LTE Advanced пропонує швидкість віддачі до 60Мб/с, а звичайний - максимум 10 Мб/С; пропускна здатність на 4G ЛТЕ станови-ть приблизно 150Мб/с, в той час, як для Advanced ця цифра може наближатися до 1Гб/с; середні сталі швидкість прийому становить 29Мб/с і 30-50Мб/с відповідно.

Що краще: 4G або LTE?

Якщо порівнювати за швидкостями, то відповідь буде очевидний. Однак від-мінності між LTE і 4G полягають не тільки в швидкості, але і в зоні покриття. Друга проблема - це необхідність відповідного девайса. У більшості випадків причиною низької швидкості служать не тільки збої в мережі, але і слабкі пристрої користува-чів, які не дають можливості

технології проявити себе. Вибирати ЛТЕ або 4g необ-хідно з вищеописаних параметрів. Більшості користувачів вистачає можливостей ЛТЕ 4G. Поки Advanced не набуде широкого поширення, яке буде порівняти з 4G, переходити на нього не має сенсу.

Кузьмич В. В.
студент групи ТСД-42

Data Over Cable Service Interface Specifications (DOCSIS)

Розглянуто етапи розвитку технології . Наведені основні переваги DOCSIS як технології, що забезпечує надання високошвидкісної передачі даних по гібридним опто-коаксіальним мережам, а також перспективи розвитку даної технології в Україні.

Інтернет передається по телефонним, телевізійним, оптоволоконним кабелях і по кручений парі. Вибір залежить від наявної мережевої інфраструктури і фінансової доцільності. Цей стандарт передбачає передачу даних абоненту в мережі кабельного телебачення з максимальною швидкістю до 42 Мбіт / с. (При ширині смуги пропускання 6 МГц і використанні багатопозиційної амплітудної модуляції 256 QAM) і отримання даних від абонента зі швидкістю до 10,24 Мбіт / с. Він покликаний змінити поширені раніше рішення на основі фірмових протоколів передачі даних і методів модуляції, несумісних один з одним, і повинен гарантувати сумісність апаратури різних виробників. Власне версій DOCSIS існує декілька:
DOCSIS 1.0; DOCSIS 1.1; DOCSIS 2.0; DOCSIS 3.0; EURODOCSIS.
EuroDOCSIS регламентує прийнятий для Європи розподіл частот прямого і зворотного каналу, та обумовлює роботу зі смугою 8 МГц . Стандарт DOCSIS 1.1 додатково передбачає наявність спеціальних механізмів, що поліпшують підтримку IP-телефонії, зменшують затримки при передачі мови (наприклад, механізми фрагментації і збірки великих пакетів, організації віртуальних каналів і завдання пріоритетів). DOCSIS має пряму підтримку протоколу IP з нефіксованим довжиною пакетів, на відміну від DVR-RC, який використовує ATM Cell transport для передачі IP пакетів (тобто, IP пакет спочатку переводиться в формат ATM, який потім передається по кабелю, на іншій стороні проводиться зворотний процес). Фіксування розмір ATM пакетів не дозволяє працювати таким службам, як Voice over IP (передача голосової і відеоінформації) - недолік, якого позбавлений DOCSIS. До того ж, більшість IP пакетів не більше ATM пакетів, тому для передачі одного IP пакета доводиться використовувати два ATM пакети, що призводить до втрат в 30-50%, чим і обумовлена менша ефективність і продуктивність цього стандарту. Для передачі даних в технології DOCSIS 3.0 використовується не один канал передачі, а одночасно чотири. До появи стандарту DOCSIS 3.0 смуга на одного користувача в Downstream-каналі становила приблизно не більше 15 Мбіт / с, в Upstream-каналі - не більше 5 Мбіт / с. Головна відмінність від DOCSIS 2.0 у тому, що в DOCSIS 3.0 канали на кабельному модемі можна об'єднувати, тим самим збільшуючи швидкість доступу в

чотири рази. акож в DOCSIS 3.0 з'явилася підтримка multicast, IPv6, шифрування AES тощо.

Ще кілька переваг останньої версії DOCSIS:

• підтримка інтернет-протоколу IPv6 (розроблений для вирішення проблеми з нестачею IP-адрес по протоколу IPv4 і сьогодні активно тестується і впроваджується в Україні та за кордоном);

• підтримка багатоадресної (multicast) передачі даних;

• можливість шифрування трафіку модема за алгоритмом AES (Advanced Encryption Standard) із застосуванням 128 бітових ключів, завдяки чому підвищується рівень безпеки при використанні Інтернету, і багато іншого.

Передача даних «зверху вниз» - до користувача, або в Downstream-каналі - виконується передавальним пристроєм головного обладнання, який називається CMTS - Cable Modem Termination System; у спрощеному випадку вся смуга ділиться між всіма користувачами, які в даний момент отримують дані, тому доступна в кожен момент часу смуга для конкретного користувача може «плавати» в широких межах. Передача інформації «знизу вгору» (в Upstream-каналі) може виконуватися кабельним модемом, який відповідає технічним вимогам, що пред'являються. Підприємством, або сертифікований на відповідність стандарту DOCSIS, а як протокол доступу реалізована процедура МДВР (Багатостанційний доступ з тимчасовим поділом каналів) або МДКР (Багатостанційний доступ з кодовим поділом каналів). До появи стандарту DOCSIS 3.0 полоса на одного користувача в Downstream-каналі становила приблизно не більше 25 Мбіт / с, в Upstream-каналі - не більше 10 Мбіт / с. Це обумовлено неможливістю виділення всіх тайм-слотів на один абонентський пристрій. Основні переваги DOCSIS

1)Ця технологія підключення до інтернету по телевізійним кабелям.

2)Вона спрощує доступ в мережу абонентам в приватних будинках, куди дорого прокладати оптоволокно.

3)За швидкістю інтернет через DOCSIS перевершує ADSL.

4)Більшість версій специфікацій стандарту забезпечують асиметричну швидкість передачі даних.

5)Швидкість від 42 Мбіт / с до 340 Мбіт / с в прямому каналі в залежності від версії. Смуга ділиться між усіма абонентами, що обмінюються даними.

На Україні DOCIS почав впроваджуватись ще з 2002 року. Сьогодні в Україну вперше починають впроваджувати DOCSIS 3.0, який відрізняється від попередніх поколінь цього стандарту чималою кількістю переваг та додаткових можливостей. З 2010 року в Україну прийшов DOCSIS 3.0. Поки цей стандарт запроваджено тільки компанією ВОЛЯ (інші провайдери працюють в основному на DOCSIS 1.1 і DOCSIS 2.0). Поява в Україні DOCSIS 3.0 говорить про те, що наш телекомунікаційний ринок продовжує рости і розвиватися, причому найкращим чином - за рахунок впровадження інновацій, - зазначає Збільшення пропускної здатності каналів передачі даних дуже важливо для кінцевих споживачів послуг телебачення та Інтернету.

Література:

1. https://habr.com/ru/post/102429/
2. *А.П. Бондарчук, Г.С. Срочинська, М.Г. Твердохліб Основи інфокомунікаційних технологій: посібник. Київ, 2015. 35 с.*
3. https://ru.wikipedia.org/wiki/DOCSIS
4. *Э. Таненбаум, Д. Уэзеролл Компьютерные сети. 5-е изд. Москва, 2012. 206 с.*

Сергієнко М.О.
студент групи КСД-42

ПОРІВНЯННЯ ТА ОСОБЛИВОСТІ ВИКОРИСТАННЯ МЕРЕЖ Wi-Fi 2.4 ГГЦ І 5 ГГЦ

Технологія WiFi одна з найперспективніших на сьогоднішній день в області комп'ютерної зв'язку. WiFi (Wireless Fidelity) - в перекладі з англійської - «бездротова відданість». Технологією Wi-Fi називають один з форматів передачі цифрових даних по радіоканалах.

Протокол Wireless Fidelity був розроблений в 1996 році. Перший час він за-безпечував користувача мінімальною швидкістю передачі даних. Але через приб-лизно кожні три роки впроваджувалися нові стандарти Wi-Fi. Вони збільшували швидкість прийому і передачі даних, а також злегка збільшували ширину покриття. Кожна нова версія протоколу позначається однією або двома латинськими буква-ми, наступними після цифр 802.11. Деякі стандарти Wi-Fi є вузькоспеціалізовани-ми - вони ніколи в смартфонах не використовувалися.

Технологія основується на базі стандартів IEEE 802.11.

b / g / n / ac - це чотири (основних) режими роботи бездротової мережі Wi-Fi 802.11. Відрізняються вони максимальної швидкість передачі даних:

- 11a - 54 Мбіт / с *, 5 ГГц стандарт.
- 11b - Покращення до 802.11 для підтримки 5,5 і 11 Мбіт / с *.
- 11g - 54 Мбіт / с *, 2,4 ГГц стандарт (зворотна сумісність з b).
- 11n - 2,4-2,5ГГц (150 Мбіт / с *); 5 ГГц (600 Мбіт / с *). Зворотна сумісність з 802.
- 11ac - сучасний стандарт IEEE. Швидкість передачі даних - до 6,77 Гбіт / с для пристроїв, що мають 8 антен. Затверджено в січні 2014 року.

Це максимально можливі швидкості з'єднання в ідеальних умовах. Реальні швидкості будуть менше і складуть близько 25 Мбіт / с для 802.11g і до 70-80 Мбіт/с для 802.11n.

Першорядним відмінністю між частотами бездротового з'єднання 2,4 ГГц і 5 ГГц є дальність дії сигналу. При використанні частоти 2,4 ГГц сигнал передається на більш далеку відстань, в порівнянні з частотою 5 ГГц. Це пов'язано з основними характеристиками хвиль і відбувається в результаті того, що при високій частоті хвилі затухають швидше.

Другою відмінністю є кількість пристроїв, що діють на даних частотах.

На частоті 2,4 ГГц бездротової сигнал більш схильний до перешкод, ніж при використ-танні частоти 5 ГГц.

Більш старий стандарт 11g працює виключно на частоті 2,4 ГГц, більшість користувачів в світі також до сих пір використовує саме його. Частота 2,4 ГГц має менші можливості при виборі каналу, тільки три з яких не перетинаються один з одним, в той час, як частота 5 ГГц має 23 непересічних канала.

Безліч інших пристроїв також працюють на частоті 2,4 ГГц, в більшій мірі це мікрохвильові печі і бездротові телефони. Дані пристрої вносять перешкоди в час-тотну середу, що в подальшому знижує швидкість з'єднання по бездротовій мережі. В обох випадках, вибір частоти 5 ГГц є найкращим варіантом, оскільки у розпоряд-женні користувача є більша кількість каналів для ізолювання своєї мережі від ін-ших мереж, і на даній частоті діє менше джерел перешкод.

Однак частоти радарів і військові частоти також використовують частоту 5 ГГц, тому бездротове з'єднання 5 ГГц також може відчувати перешкоди. Багато країн вимагають, щоб бездротові пристрої, що діють на частоті 5 ГГц, підтримува-ли динамічний вибір частоти (DFS - Dynamic Frequency Selection) і регулювання випромінюваної потужності (TPC - Transmitting Power Control).

Єденач О.В.
студент групи КСД-42

РІЗНИЦЯ МІЖ HTTP І HTTPS ТА ЇХ ВПЛИВ НА SEO ПРОСУВАННЯ

Зовсім недавно HTTPS протокол був актуальним тільки для сайтів з проведенням транза-кцій і обробкою особистих даних користувачів. Зараз вже цей протокол стає практично стан-дартом для всіх. На це вплинув анонс Google про HTTPS, як про фактор, що позитивно впливає на ранжування в пошуковій видачі. Крім того кілька останніх досліджень від гігантів SEO ринку на великих обсягах даних показали, що в ТОПі в основному сайти з захищеним шифруванням. Ймовірно через пару років, питання який з протоколів вибрати взагалі стане неактуальним.

HTTP це протокол передачі гіпертексту. Він є базовим протоколом, який ви-користовується в всеміровой павутині, і цей протокол визначає, як повідомлення форматируются і передаються, і які дії веб-сервери і браузери повинні виконувати у відповідь на різні команди.

HTTP vs HTTPS: розуміння основ

HTTP: HyperText Transfer Protocol

Протокол передачі гіпертексту (Hypertext Transfer Protocol / HTTP) - це систе-ма доставки і прийому інформації через Інтернет. HTTP - це «протокол рівня додат-ка», який по-іншому означає, що він зосереджений на тому, як інформація може на-даватися користувачеві. Але цей варіант не турбується про те, як інформація доста-вляється з точки А в точку В.

Він вважається «безструктурним» - це означає, що він не прагне нічого

вик-ликати з попередньої веб-сесії. Цінність відсутності структурності полягає в тому, що для доставки потрібно менше інформації, а це означає підвищену швидкість за-вантаження сайту. Причому перевірка швидкості сайту повинна здійснюватись пе-ріодично, так як швидкість завантаження є важливим фактором працездатності веб сайтів.

Коли корисний HTTP?

У більшості випадків HTTP використовується для доступу до HTML-сторі-нок. Раніше це був варіант для більшості сайтів, що не розміщували приватні дані (наприклад, інформацію про кредитну картку) для налаштування своїх сайтів.

HTTPS: Secure HyperText Transfer Protocol

HTTPS, іншими словами, "надійний HTTP" (secure HTTP) був створений для забезпечення безперебійної авторизації і проведення захищених транзакцій. Обмін приватною інформацією повинен бути захищеним, щоб запобігти несанкціонова-ному доступу та завдяки таким протоколом це можливо.

У більшості випадків HTTPS схожий на HTTP, оскільки він використовує ті ж базові протоколи. Клієнт HTTP або HTTPS, такий як веб-браузер, підключається до сервера через стандартний порт. Але захищений протокол пропонує додатковий рівень конфіденційності, оскільки він використовує SSL-сертифікат для передачі даних.

Для будь-яких задумів і цілей HTTPS - це той же HTTP, але просто більш без-печна його версія.

Щоб пояснити це в більш технічному ключі, основна відмінність полягає в тому, що він автоматично використовує 443 TCP-порт. Тому HTTP і HTTPS є дві різні комунікації.

HTTPS діє спільно з протоколом Secure Sockets Layer (SSL), що дозволяє йо-му безпечно надавати інформацію (це і є те найважливіше відмінність, на якому ак-центує увагу Google).

HTTPS це кращий варіант, оскільки він зосереджений на тому, щоб користу-вач не тільки візуально розумів захищеність своїх даних, а й реально мав при пере-дачі даних з точки А в точку В поліпшений рівень безпеки і конфіденційності.

Користувачі дуже часто використовують поняття HTTPS і SSL в якості сино-німів, що далеко не завжди правильно. HTTPS є захищеним протоколом, оскільки використовує для передачі даних шифрування з'єднання SSL.

Думка Google про HTTPS

Ні для кого не секрет, що Google більше любить захищені і сертифіковані сайти.

Причина такого ставлення - факт, що користувачі отримують гарантію шиф-рування своїх даних с додатковим рівнем конфіденційності. Але слід розуміти, що отримання захищеного сертифіката може стати причиною додаткових проблем (са-ме через це йому дається вищий рейтинг).

Коли веб-сайт проходить через всі етапи отримання сертифіката, користувач стає третьою стороною. Коли ваш браузер виявляє захищений сайт, він перевіряє дані сертифіката, щоб встановити, чи є сайт тим, що декларується.

Згідно із заявою, яке зроблено на самому початку, Google сьогодні використ-товує HTTPS як один з факторів ранжирування. Завдяки аналізу інформації стає зрозуміло, що веб-сайти з HTTPS мають перевагу в порівнянні з HTTP-URL-адре-сами. Саме тому перемикання на нього принесе вигоду всім компаніям, незалежно від того чи використовуються конфіденційні дані чи ні.

Також відзначають, що інформація, яка надається за допомогою HTTPS, пе-редається більш надійно через протокол безпеки транспортного рівня (TLS). Він га-рантує три основних рівня безпеки:

1. Шифрування. При шифруванні змінюється інформація, щоб зберегти її на-дійність.
2. Цілісність даних. Інформація не може бути виявлена або пошкоджена під час доставки, якщо її не розкриють.
3. Аутентифікація встановлює, що у ваших користувачів є зв'язок з сайтом.

Google оголосив, що веб-ресурси з HTTPS, отримають невелику перевагу при ранжируванні саме через цих питань конфіденційності.

Тим не менш, саме вплив HTTPS не так значно в порівнянні з іншими факто-рами ранжування (наприклад, високоякісним контентом).

Переваги переходу на HTTPS

Цінність протоколу HTTPS будується ще й на наступних факторах.

1. Збільшення рейтингу

Стверджується, що Google підтвердив невелике підвищення рейтингу сайтів з HTTPS. Як і більшість ранжирують сигналів, досить складно виділити його окре-мо, проте про нього все-таки потрібно пам'ятати. Перевагою ситуації є значення пе-реходу на HTTPS, яке повинно збільшуватися протягом певного часу.

2. Реферальная інформація

Коли трафік доставляється на HTTPS-сайт, зберігаються конфіденційні рефе-ральні дані. Це відбувається по-іншому, ніж при отриманні трафіку по протоколу HTTP. В останньому випадку потік відвідувачів сприймається не як реферальний, а як прямий.

3. Конфіденційність і приватність

- HTTPS впливає на конфіденційність декількома способами:
- Він перевіряє, чи є сайт тим, з яким повинен зв'язатися сервер.
- Він запобігає зміни з боку інших користувачів.
- Це робить ваш сайт більш конфіденційним для користувачів.

- Він шифрує будь-які комунікації, включаючи URL-адреси, які забезпе-чують такі речі, як історія переглядів і номери кредитних карт.

Можливі проблеми при переході на HTTPS

Переконайтеся, що ви повідомили Google, що перемістили свій сайт з HTTP на HTTPS.

Google дає такі поради для безболісного оновленні до HTTPS:

- Виберіть тип сертифіката, який ви хочете: стандартний, багатодоменному або груповий;
- Використовуйте 2048-бітові сертифікати ключів;
- Використовуйте відносні URL-адреси для джерел, розташованих на тому ж довірчому домені;
- Чи не блокуйте сканування свого HTTPS-сайту за допомогою robots.txt;
- Дозвольте індексацію сторінок вашого сайту пошуковим системам, де це можливо. Уникайте мета-тега robots без індексу.
- Google також оновив інструменти Google Webmaster Tools, щоб краще уп-равляти HTTPS-сайтів, і зробив звітність по ним.
- Обережно стежте за своїм переходом з HTTP на HTTPS через доступні ін-струменти Google Webmaster Tools.

Список кроків, які слід виконати, щоб перейти на захищений протокол:

- Отримайте CSR: вам потрібно створити запит на підпис сертифіката (Certificate Signing Request / CSR) на веб-сервері.
- Виберіть серверне програмне забезпечення, що використовується для ст-ворення CSR.
- Виберіть алгоритм дайджесту повідомлень, який ви найбільше хочете ви-користовувати.
- Виберіть період дії сертифіката.

Деякі хостингові сервіси допомагають клієнтам встановлювати і налаштову-вати SSL сертифікати на сервері. Щоб дізнатися, чи доступна вам така послуга, на-пишіть на підтримку вашого хостера.

Татарченко П. О.
студент ДУТ

- АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ПОБУДОВИ СИСТЕМ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ СЕРВЕРАМИ ПІДПРИЄМСТВА ТЕХНІЧНОЇ ПІДТРИМКИ

В процесі дослідження вирішувались наступні завдання : аналіз систем управління конфігураціями,побудова мережі управління серверами підприємства технічної підтримки та розробка сценарію для

автоматизації адміністрування даними серверами. Об’єкт дослідження – розробка сценарію для системи управління конфігураціями Absible.

- Предмет дослідження – засоби автоматизації системи управління та адміністрування виробничого процесу підприємства.

- Мета роботи – розробка комп’ютерної системи автоматизації та адміністрування серверів технічної підтримки підприємства для автоматичного розгортання стандартних конфігурацій сервера, керування викликами та збору статистичної інформації в процесі діяльності підприємства технічної підтримки.

У роботі проведено дослідження серверної і мережевої структури підприємства, що займається розробкою та інтеграцією програмних продуктів для підприємства, а також запропоновано локальну мережу і серверну структуру підприємства, на якому буде впроваджуватися даний програмний комплекс.

Проведений аналіз двох систем оркестрації – Puppet та Ansible та існуючі підходити до створення маніфестів та сценаріїв даних систем оркестрації.

Виконано опис системи управління та адміністрування серверів підприємства, аналіз програмного забезпечення комп'ютерної системи управління та адміністрування серверів підприємства, тестування сценарію технології Ansible серверів підприємства технічної підтримки.

Виконано аналіз розвитку систем оркестрації серверів, наведено схеми побудови серверної структури організації та структуру локальної мережі і серверів клієнтської сторони, зазначені принципи побудови комп’ютерних систем моніторингу Zabbix та Grafana, що дають моливість вчасно проінформувати про можливі збої в роботі підприємств клієнтів, виконано огляд сервісу Bacula, що відповідає за автоматизацію збору бекапів та можливість відновлення даних, описано системи захисту даних в системах керування конфігураціями в linux–серверах.

Проведено дослідження та розробку технологій управління та адміністрування серверів, узагальнені задачі серверної інфраструктури системи управління конфігураціями, виконано аналіз засобів захисту інформації в фізичних та хмарних серверних системах, розроблені принципи побудови комп’ютерних систем керування конфігураціями та система контролю версій для сценаріїв Ansible, виконано розробку структури організації для адміністрування та управління серверами підприємства технічної підтримки.

Виконано опис системи управління та адміністрування серверів технічної підтримки, виконано оцінку програмного забезпечення

комп'ютерної системи управління та адміністрування серверів підприємства та тестування сценарію технології Ansible серверів підприємства.

Розроблено комп'ютерну систему управління та адміністрування серверів підприємства, що доволяє підвищити показники швидкості налаштування у 3,4 рази порівняно з ручним налаштуванням, зменшити кількість залучених спеціалістів до налаштування технічної підтримки «під ключ», забезпечено гнучкість при зміні структури організації та масштабуванні серверної інфраструктури.

Веселков К.О.
студент ННІЗДН

ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДИКИ ГЕОГРАФІЧНОГО МІСЦЕЗНАХОДЖЕННЯ НА БАЗІ ДОДАТКУ GEOHIGH2

У сучасному світі дуже часто користувачі Інтернет-ресурсів використовують різні додатки у своєму мобільному телефоні. Існуючі програми охоплюють широкий спектр необхідних людині можливостей, а також просто цікавих доповнень.

В даний час існують мобільні додатки, які доповнюють картинку з камери мобільного телефону інформацію про те, що знаходиться в даному напрямку і яка відстань до цього місця. Більш того, доводиться заздалегідь вибирати, яку категорію місць потрібно показувати.

Для того, щоб проаналізувати працездатність методики геотаргетинга з урахуванням висотних особливостей, було досліджено і реалізовано мобільний додаток GeoHigh2. Основний активністю додатки GeoHigh2 є визначення будівель, які видно користувачеві з поточного місця розташування і доповнення зображення, що надходить з камери пристрою текстовими вставками з інформацією по видимим домівках. У поточній версії програми GeoHigh2 текстова інформація є адресою кожного видимого будинку.

Щоб оцінити працездатність розглянутої методики була проведена серія тестів. Алгоритм проведення кожного тесту:

1. Завдання конкретного місця розташування, напрямку погляду і висота над поверхнею землі для користувача мобільного додатка GeoHigh2;
2. Визначення очікуваної інформації (реально видимих будівель) в заданих умовах;
3. Запит інформації про видимі будівлях, яку обчислює і надає мобільний додаток GeoHigh2 в тих же умовах;
4. Збереження інформації, отриманої від програми, в формі знімка екрана (скріншот);
5. Зіставлення отриманої від програми GeoHigh2 інформації та очікуваних результатів.

Серія складалася з 20 тестів, проведених в різних точках Печерського району міста Києва. Критерієм оцінки для даного виду тестування є кількість тестів, в яких результати розмітки мобільним додатком і реальної розмітки будівель збіглися. Також цікаві часткові збіги розмітки. У табл. 1 наведені результати серії якісних тестів.

На рис.1 наведені приклади знімків екрана програми GeoHigh2 для різних тестів. Перші два малюнки відображають результати тестів, які показали успішні результати. У першому випадку рис.1а, будівля визначено правильно з висоти людського зросту (практично з рівня землі). У другому випадку рис.1б, та ж сама будівля визначена правильно з висоти другого поверху. Слід зазначити, що висоту розташування користувача над рівнем землі додаток не визначає самостійно, а запрошувати на початку використання програми у користувача.

Таблиця 1 - Результати тестів з використанням додатку GeoHigh2

Результат тесту	Кількість тестів	Відсоток від загальної кількості тестів
Тест повністю успішний - всі будівлі визначено правильно	21	70%
Тест повністю неуспішний - проблема з визначенням азимута	7	23%
Тест частково успішний - частина будівель визначено правильно, частина не визначено зовсім	2	7%
Загальна кількість проведених тестів	30	100%

а) *б)* *в)* *г)* *д)*

Рис.1 Приклади знімків екрана програми GeoHigh2 для різних тестів.

На рис.1в, наведено приклад результату частково успішного тесту. Найближче будівля визначено і відзначено правильно. А будівля, розташована за ним не спостерігалося.

В даному випадку рис.1в, позначається недосконаліть способу обчислення висоти будинків. З метою простоти апробації основного алгоритму висоти всіх будівель обчислюються виходячи з кількості поверхів. Висота поверху задається середнім значенням в 3 метри. Але на практиці висота поверхів в будинках варіюється в дуже великих межах. Результати тестовий приклад програми не справляється в деяких випадках. У тих випадках, коли висота другого будівлі помітно більше, ніж висота найближчого будинку, алгоритм показує хороші результати. На рис.1г, показаний приклад успішного тесту з визначенням двох будівель в зоні видимості.

Слід зазначити і зовсім неуспішні приклади роботи програми GeoHigh2. У 5 з 20 тестах будинку були розмічені абсолютно неправильно. На рис.1д, наведено приклад неуспішного тесту. Тут наведено той же будинок, що і в одному з попередніх тестів рис.1а, Але номер будинку позначений неправильно. Замість адреси «вулиці Експанандна 2» додаток позначило адресу «вулиці Басейна 28».

Ситуація неправильного визначення адреси відбувається через те, що програма отримує невірні показання кута азимута від датчиків. Надалі, можна використовувати показання кута азимута, які надходять від супутників GPS, а не від сенсорів самого пристрою Хоча GPS датчики мають свої недоліки, які не дозволяють їм працювати адекватно в деяких ситуаціях, наприклад, близько висотних будівель [1,2]. За результатами проведеної серії тестів була доведена працездатність досліджуваної методики. Крім цього, серія якісних тестів показала, що алгоритм визначення видимих будівель вимагає деякий коригувань для більш точного виконання своєї роботи. В цілому основний алгоритм визначення видимих будівель з урахуванням висотних особливостей працює стабільно. Це дає хорошу основу для можливих поліпшень його показників та розвитку додатку.

Перелік посилань:

1. Программирование под Android. 2-е изд./З. Медникс, Л. Дорнин, Б. Мик, М. Накамура. – СПб.: Питер, 2013. – 560 с.

2. Salychev. O.S. Applied Inertial Navigation: problems and solutions. — M.: BMSTU Press, 2004. — 304 с.

Герцюк М. М.
студент групи ПДМ-51

ДОСВІД ВИКОРИСТАННЯ ТЕОРЕМИ БАЄСА, ЯК МЕТОДУ ФІЛЬТРАЦІЇ СПАМУ

Проблема фільтрації спаму є актуальною через велику кількість несанкціонованих листів і невисоку ефективність основних методів фільтрації спаму. З метою підвищення результативності та ефективності фільтрів спаму використовуютьсь різні математичні методи оцінки листа. У даній роботі висвітлюється метод використання теореми Баєса, що дозволить підвищити ефективність фільтрації спаму.

На даний час існує декілька методів фільтрації e-mail листа, як спаму. Цими методами є:

- фільтрація з використанням «чорних списків» відправників, IP-адреси, тощо;
- фільтрація з використанням формальних ознак листа, таких як наявність масової розсилки, розмір листа, об’єм символів, тощо;
- аналіз змісту листа [1].

Серед вищенаведених методів можна виділити метод аналізу змісту листа, метою якого є фільтрація листів за присутністю деяких ключових слів. В основі фільтрації лежить використання теореми Баєса. Особливістю цього методу є те, що даний метод працює з ймовірностями, і не має обмеження у вигляді двох варіантів «так/ні»[2]. Це дає можливість відфільтрувати спам-листи, які не підпадають під інші методи фільтрації, але по факту є спамом. Потенційно, фільтрація листа складається в декількох етапів:

1. знаходження ключових слів, що потенційно можуть характеризувати спам;

2. визначення ймовірності цього листа, як спаму;

3. якщо ймовірність настання двох подій буде вищою за критерій фільтру, то цей лист помічається, як спам, а статистична база даних спаму поповнюється.

В якості прикладу можна проаналізувати лист, який має таку фразу «Congratulation! You won 10 000 000$».

Нехай, статистична вибірка показала, що слова «congratulation»та «won» разом зустрічаються у 97% спаму, такого типу фрази – з ймовірністю у 60%, а критерій фільтру 90%.

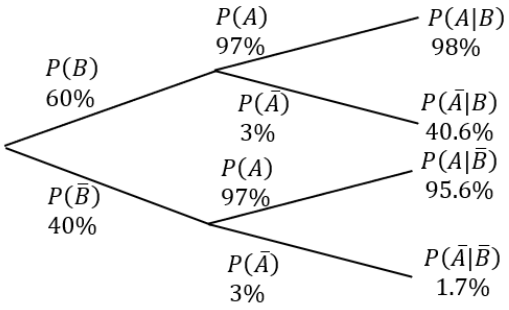
Приймемо подію, де зустрічаються «спам-слова», як подію А, а подію з іншими словами, як подію В.

Використаємо альтернативну форму з теореми Баєса [3], та отримаємо такий результат:

$$P(A|B) = \frac{P(A) \times P(B|A)}{P(A) \times P(B|A) + P(\bar{A}) \times P(\overline{B|A})} = \frac{0.97 \times 0.6}{0.97 \times 0.6 + 0.03 \times 0.4} = \frac{0.582}{0.594} = 0.98 = 98\%$$

Як видно 98%>90%, а отже даний лист можна вважати спамом.

Для глибшого розуміння фільтрації такого типу листів, як спаму побудуємо деревну схему Баєса, наведену нижче.



Як бачимо, якщо в інший лист потраплять слова «congratulation» та «won» разом, але при цьому фраза буде іншою, то такий лист так само буде помічено, як спам.

Якщо ж повідомлення не буде містити цих слів, то воно в будь-якому випадку не буде відфільтроване.

Посилання

1. К. Кузьма, В. Зівенко Аналіз методів фільтрації електронної пошти від спаму – Геометричне моделювання та інформаційні технології - №1 – 2017. Режим доступу: http://mdu.edu.ua/wp-content/uploads/gmit084.pdf. Дата звернення: 06.04.2019.

2. Простое объяснение теоремы Байеса/Хабр – Режим доступу: https://habr.com/ru/post/408775/ – Спам-фильтр. Дата звернення: 06.04.2019.

3. Теорема Баєса – Вікіпедія. Режим доступу: https://uk.wikipedia.org/wiki/Теорема_Баєса#Альтернативна_форма – Форми – Події – Альтернативна форма. Дата звернення: 06.04.2019.

Олішевський А.А.
студент групи ІМД-41

РОЗРОБКА ТА ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ 5G

5G – це вже п'яте покоління мобільного зв'язку. Основною відмінністю від інших поколінь є швидкість передавання даних. Якщо на першому поколінні швидкість була лише 2 кбіт/с, то технологія 5G передбачає швидкість на рівні 1 гбіт/с.

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, що буде реалізовано на основі багатоелементних цифрових антенних решіток. 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.
- Підвищення спектральної ефективності на основі різних варіантів неортогональних за частотою (N-OFDM) сигналів.

Негативні наслідки впровадження 5G

Спектр частот, який використовує технологія 5G, досить близький до спектру пасивного дистанційного зондування, що використовують для прогнозування погоди та стеженням за Землею. Відповідно, технології 5G можуть створити перешкоди, що значно ускладнить їхню роботу.

Водночас, деякі дослідники говорять і про загрозу для людського здоров'я, зокрема через вплив радіації. Радіочастоти високої потужності можуть призвести до значного підвищення температури тіла людини, однак жодних серйозних досліджень щодо шкідливого впливу 5G на людину досі немає.

Існує і ще одна проблема використання нової технології – шпигунство. Значна кількість обладнання 5G є китайського виробництва, а іноземні користувачі всерйоз побоюються шпигунства з боку цієї держави, а тому запроваджують обмеження на використання їхніх товарів. Найбільше про інформаційну загрозу з боку Китаю говорить президент США Дональд Трамп.

1.Мобільна технологія 5-го покоління. Режим доступу: https://www.electronics-notes.com/articles/connectivity/5g-mobile-wireless-cellular/technology-basics.php

2.Негативні наслідки нової мережі. Режим доступу: https://ieeexplore.ieee.org/document/6515173?arnumber=6515173

Ступник А. С.
студентка групи ІМД-42

ДОСЛІДЖЕННЯ МЕРЕЖІ ДОСТУПУ ЗА ТЕХНОЛОГІЄЮ IMT-2020 ДЛЯ ЗАБЕЗПЕЧЕННЯ МУЛЬТИМЕДІЙНИХ ПОСЛУГ

Телекомунікаційна галузь з кожним роком невпинно розвивається. Це стосується як засобів мобільного зв'язку, так і різновидом нових можливостей, які оператор надає абонентам.

У сфері телекомунікацій, застосування обробки сигналів дозволяє новим поколінням систем досягти продуктивності, близької до теоретичних меж, а в області мультимедіа - обробка сигналів базової технології

Швидко зростає спектр мультимедійних послуг у сучасних

телекомунікаційних системах, яке стало можливим лише завдяки досягненням технологій та алгоритмів обробки сигналів

Одним з найбільш великих проектів 2019р є концепція IMT-2020. За основу покладено ідею створення нового покоління сімейства стільникового зв'язку, систем бездротового доступу і супутникового зв'язку. Основні вимоги, пропоновані до стандартів сімейства IMT-2020 –забезпечення глобального роумінгу і універсальні рішення для мереж різного класу (мікростільникових, стільникових і супутникових). На сьогоднішній день, у багатьох країнах світу технологія 5G вважається найбільш перспективною.

Результуюча мережа може бути використана у дистанційному навчанні. Перелік послуг, які можуть бути надані, чудово підходять для організації науково – освітньої мережі, а саме відео- та аудіо- конференції, відкриті вебінари і відеозаписи з загальнодоступних веб-ресурсів, голосовий зв'язок між абонентами, обмін повідомленнями під час подорожі, доступ до глобальної мережі, зберігання даних на серверах, віртуалізація і автоматизація виробничих процесів, розумні міста,завантаження даних на високих швидкостях.

Література

https://ubr.ua/ukraine-and-world/technology/kak-internet-5g-izmenit-ekonomiku-planety-3881373
https://www.androidcentral.com/5g
https://observer.com.ua/5g/

Лапиняускас В. А.
студент групи ТСД-42й

СИСТЕМИ РЕЗЕРВУВАННЯ ДАНИХ

Розглянуто системи резервування даних та їх важливість для підприємств. Наведені основні методи резервного копіювання та відновлення інформації.

Роль та важливість системи зберігання визначаються постійно зростаючою цінністю інформації у сучасному суспільстві; можливість доступу до даних і управління ними є необхідною умовою для виконання бізнес-процесів.

Вся інформація, яка зберігається піддається багатьом ризикам та може бути втрачена безповоротно. Неможливо на 100% захистити важливу інформацію від усіх цих ризиків.

На багатьох підприємствах знехтують важливістю резервного копіювання даних, що в крайніх випадках може до великих збитків. Втрачені апаратні, обчислювальні ресурси підлягають відновленню, як в свою чергу інформаційні ресурси, за відсутності резервних копій відновити практично неможливо.

Як показують дані світової статистики, в якості основних причин втрати інформації виступають некоректна робота апаратних засобів (44%) і людські помилки (32%), в основному тих, хто має максимальний рівень доступу до систем зберігання даних підприємства. 14% всіх випадків втрати інформації пов'язано з помилками програмного забезпечення, інші 7% виникають в зв'язку з появою комп'ютерних вірусів, а через стихійних лих - лише 3%.

Збої призводять до призупинення бізнес-процесів і втрати даних, тим самим ставлять під питання функціонування підприємства в цілому. Звідси, єдиним способом для надійного збереження необхідних даних виступає періодичне створення резервних копій інформації. Система зберігання даних призначена для організації надійного зберігання даних, а також відмовостійкого, високопродуктивного доступу серверів до пристроїв зберігання.

В даний час існують такі методи щодо забезпечення надійного зберігання та відмовостійкого доступу до даних - це дублювання, копіювання, резервне копіювання.

Так, для захисту від відмов окремих дисків використовуються технології RAID, які застосовують дублювання даних, що зберігаються на дисках. Для захисту від логічного руйнування даних, викликаних збоями в обладнанні, помилками в програмному забезпеченні або невірними діями обслуговуючого персоналу, застосовується резервне копіювання, яке теж є дублюванням даних. Для захисту від втрати даних внаслідок виходу з ладу пристроїв зберігання з причини техногенної або природної катастрофи, дані дублюються в резервний центр.

Відмовостійкість доступу серверів до даних досягається дублюванням шляхів доступу. Згідно даної ідеї, дублювання полягає в наступному: мережа будується як дві фізично незалежні мережі, ідентичні по функціональності і конфігурації. Відмова обладнання, зміна конфігурації або регламентні роботи на одній з мереж не впливають на роботу іншої. У дисковому масиві відмовостійкість доступу до даних забезпечується дублюванням RAID-контролерів, блоків живлення, інтерфейсів до дисків і до серверів.

Для захисту від втрати даних віддзеркалюються ділянки кеш-пам'яті, що беруть участь в операції запису. Шляхи доступу серверів дублюються. Для перемикання з каналу, який вийшов з ладу, на резервний, а також для рівномірного розподілу навантаження між усіма каналами зв‘язку, на серверах встановлюється спеціальне програмне забезпечення.

Необхідну продуктивність доступу серверів до даних можна забезпечити створенням виділеної високошвидкісної транспортної інфраструктури між серверами і пристроямизберігання даних. Використання сучасних дисків з достатнім об'ємом кеш-пам'яті і продуктивності, що не мають "вузьких місць", з внутрішньою архітектурою обміну інформацією між контролерами та дисками, дозволяє здійснювати швидкий доступ до даних.

Оптимальне розміщення даних по дисках різного об‘єму і продуктивності, з потрібним рівнем у залежності від класів додатків (СУБД, файлові сервіси і т.д.), є ще одним способом збільшення швидкості доступу до даних.

Література:

1. https://habr.com/ru/post/136785/
2. https://www.ukraine.com.ua/faq/rezervnoe-kopirovanie.html#!8
3. https://technari.com.ua/ru/services/about-company/articles/what-is-backup

Жежкун С.А.
студент групи ІМД-42

ОГЛЯД СУЧАСНОГО СТАНУ РОЗУМНИХ БУДИНКІВ, АНАЛІЗ ПЕРЕВАГ ТА НЕДОЛІКІВ

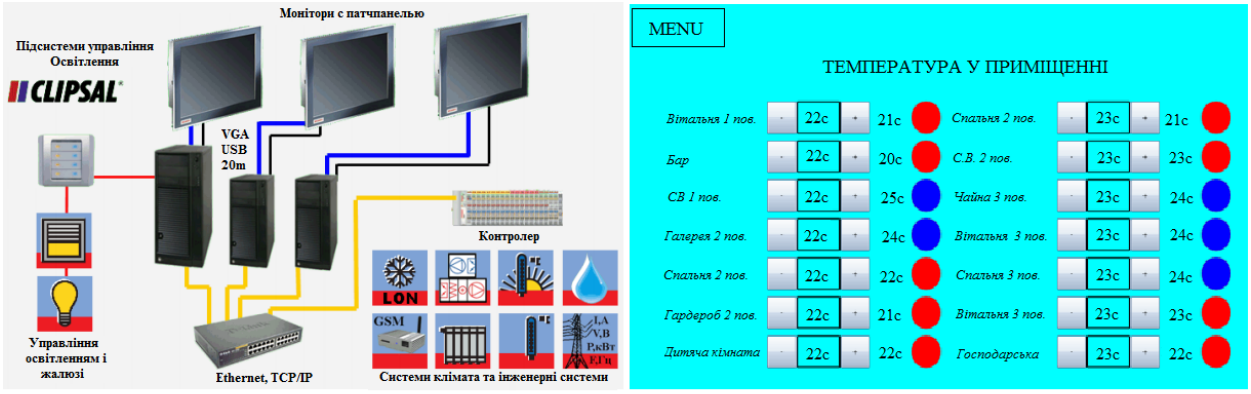
В сучасному світі системи розумного будинку отримали велику популярність останнім часом. Розумний дім є автоматизована будівля сучасного типу, що організована для зручності людей за допомогою високотехнологічних пристроїв.

Сучасний «розумний дім», який зображено на рис.1, втілив у собі безліч інноваційних розробок, які зробили його унікальним з безпеки і комфортабельності. Наявність всіх цих розробок дозволяє сьогодні втілювати мрії в життя, тепер власнику житла зовсім необов'язково турбуватися про свій будинок, адже він завжди під контролем обладнання, яке не дає збоїв і працює цілодобово весь рік, навіть коли нікого немає в будинку. Зараз на ринку є чимало компаній, що пропонують свої послуги в сфері проектування «розумних будинків», при виборі тієї чи іншої компанії, необхідно бути впевненим у професіоналізмі співробітників, щоб надалі не випробовувати проблем з технікою [1].

Рис.1 – Сучасний розумний будинок

«Розумний» будинок - це сукупність різних смарт-девайсів від різних компаній, які об'єднані єдиним софтом та вимогами виробника.

Рішення від Clipsal, яке зображено на рис.2,*а*. У спільному інтегрованому рішенні на частку «Clipsal» покладено основні комунікаційні функції – централізована технологія управління, спостереження і диспетчеризації усіма пристроями. Таким чином, все, що стосується життєздатності інженерних систем, економії електроенергії, функціонування охоронно-пожежної сигналізації, комфорту і зручності в управлінні будівлею вирішується завдяки ультра функціональну, легко масштабується, однією з найнадійніших систем управління. Являє собою невеликі модулі з сенсором, які підключаються до просто електроніці і управляють їй за рахунок вбудованого алгоритму, інтерфейс системи зображено на рис.2,*б*. Переваги: низька вартість, масштабованість системи, немає потреби купувати техніку з вбудованими функціями взаємодії. Недоліки: відносно складне налаштування, низька взаємодія компонентів один з одним [2]. Порівняння рішень наведено у табл. 1.



а) б)

Рис. 2 - Управління та Інтерфейс система Clipsal

Таблиця 1 – Порівняння сучасних систем розумний будинок

Параметр	**Meizu**	**Allone**	**Clipsal**
Вартість	Середня	Висока (разом з модулями)	Невелика за модуль, середня за систему в цілому
Установка	Проста	Проста	Потребує попереднього налаштування
Налаштування	Не потребує	Через веб-сервіс	Через прошивку
Готові модулі	Мало	Багато	Не потребує
Масштабованість	Масштабується	Масштабується, але залежить від розміру	Масштабується
Взаємодія	Через смартфон	Через сам пристрій	Через хмарний додаток
Функціонал	Базовий	Майже необмежений	Майже необмежений

Перелік посилань:

1. Аркадьева З. А., Промислова автоматізація: Учеб. пособие для вузов / З. А. Аркадьева, А. М. Безбородов, И. Н. Блохина и др. Под ред. Н.С. Егорова.- М.: Высш. шк., 2015.- С. 426-430

2. Сопер М. Э. Практические советы и решения по созданию «Умного дома»/ - М. Э. Сопер М.: НТ Пресс, 2017. - 432 с.

Огороднік О.А.
студент групи АРЗМ-71

МЕТОДИ ТА ЗАСОБИ РАДІОПЕЛЕНГУВАННЯ

Аналіз літератури показав, що в останні роки все більшого застосування знаходить амплітудно-фазове або кореляційно-інтерферометричне радіопеленгування, що проводиться шляхом часової кореляційної інтерферометрії комплексних напруг сигналів для кожної антени з подальшим обробленням вимірів та оцінюванням пеленга.

Сучасні кореляційно-інтерферометричні часові радіопеленгатори використовують нерухомі антени. Найпростіший кореляційний радіопеленгатор складається з рознесених на певну відстань d антен А1, і А2, двоканального радіоприймального пристрою (РПП) зі спільним гетеродином, лінії затримки, час затримки якої можна регулювати, корелятора та пристрою оброблення даних і визначення пеленга (рис. 1.) [2].

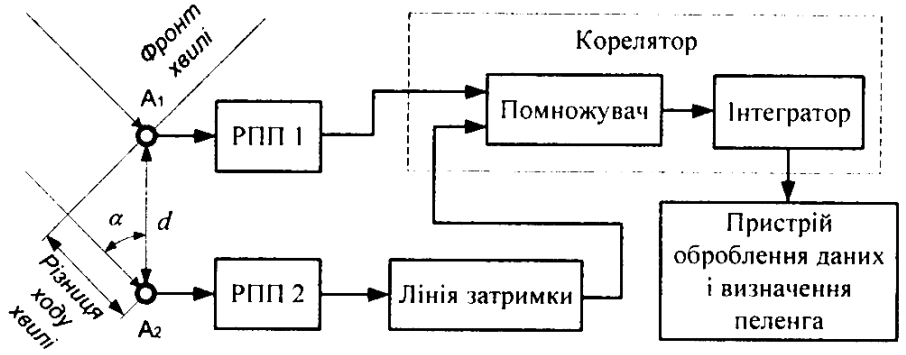


Рисунок 1 - Структурна схема кореляційно-інтерферометричного радіопеленгатора з нерухомою антенною системою

Сигнали з виходів обох РПП надходять на входи корелятора, причому, один – безпосередньо, а другий – через лінію затримки. Радіопеленгування проводиться за максимумом напруги на виході корелятора, який отримується коли взаємна кореляція між вихідними напругами РПП 1 і РПП 2 максимальна, наприклад, у випадку коли різниця Δt часу поширення сигналів від ДРВ до обох антен компенсується часом $\tau_{ЛЗ}$ регульованої лінії затримки. Таким чином, за оціненим числовим значенням часу $\hat{\tau}_{ЛЗ}$, яке можна визначити за максимальним рівнем напруги на виході корелятора шляхом регулювання вручну або автоматично часу лінії затримки, можна визначити кут α між напрямком на ДРВ і напрямком антенної бази d із виразу:

$$\cos\alpha = \frac{c \cdot \hat{\tau}_{ЛЗ}}{d} \qquad (1.1)$$

де c – швидкість поширення електромагнітного випромінювання у вільному просторі;

d – антенна база;

$\hat{\tau}_{ЛЗ}$ – оцінка значення часу затримки поширення сигналів від джерела до двох антен.

В ряді випадків виникає необхідність радіопеленгування з більшою точністю об'єктів, радіовипромінювання яких має не когерентний, а шумовий характер. До подібних об'єктів відносяться, наприклад, сигнали із стрибкоподібною зміною частоти, шумові завади, сигнали з лінійною частотною модуляцією і широкосмугові псевдовипадкові сигнали. В таких випадках, використовуючи кореляційно-інтерферометричний радіопеленгатор з досить великою антенною базою, можна досягти високої чутливості і точності радіопеленгування. При цьому, завдяки тому, що функція взаємної кореляції для сигналів шумового характеру монотонно зменшується при збільшенні Δt, ДС кореляційно-інтерферометричного радіопеленгатора виявляється однозначною і бічні пелюстки в ній відсутні. Антени А1 та А2 можуть мати як кругову ДС так і гостру. В останньому випадку для забезпечення слідкування за джерелом радіовипромінювання повинно бути передбачено синхронний поворот ДС.

В роботах [2] розглянуто варіанти побудови кореляційно-інтерферометричних радіопеленгаторів, що відрізняються способом вимірювання значення функції взаємної кореляції. Типовими варіантами побудови пеленгаторів є визначення затримки сигналу на проміжній частоті та на частоті модуляції.

Кожен з наведених варіантів методу кореляційно-інтерферометричного радіопеленгування має свої переваги та недоліки і може застосовуватися відповідно до поставлених задач та умов їх виконання. Але спільним їх недоліком є недостатня швидкодія, що визначається послідовним багатоітераційним алгоритмом пошуку напрямку на ДРВ.

Аналіз показав, що в цілому кореляційні інтерферометри на сьогодні є найперспективніші серед радіопеленгаторних систем, що зумовлено їхніми наступними суттєвими перевагами [1]:

– якісне радіопеленгування практично будь-яких видів радіосигналів, у тому числі, широкосмугових зі складними видами модуляції;

– можливість оброблення та розрізнення одночасно двох або декількох сигналів в одному частотному каналі, причому як когерентних (у процесі приймання багатопроменевого випромінювання одного й того ж ДРВ), так і некогерентних (у процесі приймання радіосигналів від декількох ДРВ, спектри яких перекриваються);

– наявність ефективних методів зменшення інструментальних похибок, зумовлених взаємним впливом антенних елементів і місцевих умов, які можуть враховуватися для будь-яких типів антенних решіток;

– відсутність обмежень на конфігурацію антенних решіток (АР) радіопеленгатора, що дозволяє застосовувати складні решітки з широкою зоною

однозначного радіопеленгування і високою розрізнювальною здатністю як у горизонтальній, так і у вертикальній площинах;

– більша, ніж у фазових радіопеленгаторів, стійкість до впливу когерентних радіозавад і завад у сумісному каналі.

Крім перерахованих переваг, кореляційні інтерферометри допускають поширене застосування методів цифрового оброблення сигналів на всіх стадіях визначення пеленгу.

Оптимальне визначення напрямку на ДРВ в умовах великої апріорної невизначеності забезпечує кореляційно-інтерферометричний метод радіопеленгування. Кореляційні інтерферометри на сьогодні є найбільш перспективними. Однак суттєвою невирішеною проблемою їх реалізації при пеленгуванні ДРВ з широкосмуговими шумоподібними випромінюваннями є недостатні точність та швидкодія радіопеленгування.

Література:

1. Слободянюк П.В, Благодарний В.Г., Ступак В.С. Довідник з радіомоніторингу / Під. заг. ред П.В. Слободянюка. – Ніжин: ТОВ «Видавництво «Аспект-Поліграф», 2008. – 588 с.

2. Белавин О.В. Основы радионавигации. Учебное пособие для вузов. Изд. 2-е, перераб. и доп. М., Сов. Радио, 1977. 320 с.

Шиловець Д. В.
факультет Телекомунікацій

Технологія Passive Optical Network(PON)

Розглянуто технологію пасивної оптичної мережі. Наведені основні перваги і недоліки які дозволяють оцінити ефективність технології та її майбутнє використання в Україні.

Інформаційні структури в останній десяток років зробили крок дуже далеко вперед - сьогодні вже нікого не здивуєш безлімітним широкосмуговим інтернетом на швидкостях 10Mbps і більше.. Швидкість доступу в Інтернет безперервно зростає. Розгортання нових широкосмугових мереж стимулюється вимогами сучасних додатків, таких як відео за запитом або IP-телефонія. Оскільки якість існуючих мідних кабелів не дозволяє надавати послуги широкосмугового доступу по всім парам кабелю і ціна на мідь зростає, оптичні кабелі стають все більш привабливими при виборі рішень для мереж доступу. Відповідно, підвищується інтерес до розгортання оптичних мереж доступу з прокладанням кабелю до будинку абонента - FTTH (Fiber to the Home). Однією з технологій, на базі яких проводиться розгортання мереж FTTH, є технологія пасивної оптичної мережі - PON.

PON (англ. Passive Optical Network - пасивна оптична мережа) - це швидко розвивається, найбільш перспективна технологія широкосмугового мультисервісного множинного доступу з оптичного волокна, що використовує хвилевий поділ трактів прийому / передачі і дозволяє реалізувати одно волоконну деревоподібну топологію «точка-багато точка» без використання активних мережевих елементів в вузлах розгалуження.

Іншими словами, мало волокон, відсутність проміжного активного обладнання, нульове (ну, майже нульове) вплив погодних умов, зручна WDM система передачі даних від «фабрики по виробництву інтернету» до клієнта і назад по одному волокну. Активне обладнання в цій мережі є тільки на стороні провайдера (в чистій, сухій і прохолодною серверній стійці) і на стороні абонента (на горищі, в передпокої, на старому-доброму стовпі та ін.). Ідеально як для віддалених малонаселених пунктів, так і для міського приватного сектора. Технологія PON ідеально підходить для покриття великої території з різною щільністю забудови: від багатоповерхових районів до котежних містечків, де переваги технології розкриваються в повній мірі. Передача та прийом в обох напрямах здійснюється, я правило, по одному оптичному волокну, але на різних довжинах хвиль (1310 та 1490 нм). У стандартній оптичній мережі PON на стороні провайдера зв'язку використовуються OLT (Optical Line Terminal) - оптичний лінійний термінал - L2 світч, що має Uplink порти (для підключення до L3 комутатора) і Downlink порти (для побудови PON мережі), а в якості абонентських пристроїв застосовуються ONT (Optical Network Terminal) ONU (Оптична Мережева Одиниця) - повноцінний VLAN світч невеликого розміру. ONU стандартно має один оптичний 1G порт (Uplink) і один 1G або 4 0.1G мідних порту (Downlink). Існує кілька стандартів PON, а саме:

-APON (ATM PON) - історично перший стандарт PON G.983. Транспортний протокол - ATM. Спадний потік - 1550 нм, 155 Мбіт / с. Висхідний потік - 1310 нм, 155 Мбіт / с.

-BPON (Broadband PON) - розвиток стандарту APON ITU G.983. Транспортний протокол - ATM. Спадний потік - 1550 нм, 622 Мбіт / с, в більш пізніх версіях - 1490 нм (1550 нм звільнено для відео). Висхідний потік - 1310 нм, 622 Мбіт / с.

-GPON (Gigabit PON) - стандарт PON ITU G.984. Найбільший інтерес до обладнання даного стандарту проявляють в США. Транспортний протокол - GFP (Generic Framing Protocol). Спадний потік - 1490 нм, 2,4 Гбіт / с або 1,2 Гбіт / с. Висхідний потік - 1310 нм, 1,2 Гбіт / с або 622 Мбіт / с.

-EPON (Ethernet PON) або GEPON (Gigabit Ethernet PON) - стандарт PON IEEE 802.3ah. Найбільший інтерес до обладнання цього стандарту спостерігається в азіатських країнах (Китай, Японія, Корея, Малайзія і т.д.). Транспортний протокол Ethernet. Спадний потік - 1490 нм, до 2,5 Гбіт / с. Висхідний потік - 1310 нм, до 2,5 Гбіт / с.

Технологія PON незважаючи на свою привабливість має свої переваги та недоліки. Основні переваги PON:

-Економія волокон. До 128 абонентів на одне волокно, протяжність мережі до 60 км.

-Ефективне використання смуги пропускання оптичного волокна.

-Швидкість до 2,488 Гбіт / с по низхідному потоку і 1,244 Гбіт / с по висхідному.

-Надійність. У проміжних вузлах дерева знаходяться тільки пасивні оптичні

розгалужувачі, які не потребують обслуговування.
-Масштабованість. Деревоподібна структура мережі доступу дає можливість підключати нових абонентів найекономічнішим способом.
-Можливість резервування як всіх, так і окремих абонентів.
-Гнучкість. Використання ATM як транспорт дозволяє надавати абонентам саме той рівень сервісу, який їм потрібен. Дані по мережі передаються у вигляді осередків ATM. Можливі симетричний і асиметричний режими роботи.

Недоліки технології PON:
-PON - технологія із загальною середовищем передачі даних, тому окремі потоки інформації доводиться шифрувати. Це може знижувати корисну швидкість передачі, а також не захищає інформацію від злому на фізичному рівні.
-В системі важко виявити неполадки на ділянці між сплітерами і кінцевою точкою - ONT. Важливо мати на увазі, що при виборі професійного установника, який зможе якісно встановити, відстежувати стан і забезпечувати повноцінний сервіс, проблеми з мережею мінімізуються.

В даний час пасивні мережі на основі оптичного волокна набувають все більшого поширення. Мідні кручені пари не витримують конкуренції з PON за обсягами, швидкості і дальності передачі даних, помехозащищенности і масштабованості. Якщо спочатку перевагу часто віддавалася вітопарним кабелям через дорожнечу оптичного сировини і обладнання, то зараз за капітальними витратами і трудомісткості монтажу системи розрізняються незначно. Як і раніше популярним є будівництво суміщеного виду мереж - FTTH, де мідна пара використовується тільки на ділянці від комутатора до абонента. Однак динаміка все більше зміщується в бік PON, в тому числі і завдяки тому, що установка пасивної мережі допускає модифікацію без втручання в архітектуру системи і перекладки кабелю. Майбутнє PON багатообіцяюче. В Україні таких проектів поки небагато (елітні будинки, котеджні селища), але все зміниться, тому що вигоди і перспективи технології пасивних оптичних мереж очевидні. Серед основних переваг PON - здешевлення обслуговування мереж (за рахунок відсутності активного обладнання на проміжку від OLT до абонентського відводу) і висока швидкість передачі даних.

Література:

1. https://neoi.ru/pon
2. http://www.comizdat.com/index_.php?id=5245&in=komi_articles_id
3. *А.П. Бондарчук, Г.С. Срочинська, М.Г. Твердохліб Основи інфокомунікаційних технологій: посібник. Київ, 2015. 56 с. - 57 с.*
4. *Э. Таненбаум, Д. Уэзеролл Компьютерные сети. 5-е изд. Москва, 2012. 273 с.*

Кнауб С. Е.
студент групи СЗЗМ-71

КОНТРОЛЬ ЯКОСТІ ЗАВАД В СУЧАСНИХ СИСТЕМАХ ВІБРОАКУСТИЧНОГО ЗАШУМЛЕННЯ

Здобування конфіденційної мовленнєвої інформації завжди було, є й буде одним із головних завдань військового, політичного, промислового, комерційного та інших видів шпигунства, оскільки вона містить оперативні дані щодо діяльності організацій чи осіб і надає можливість оцінити відношення співрозмовників до предмету розмови. Важливою задачею при захищенні мовленнєвої інформації від витоку технічними каналами є об'єктивна оцінка ефективності заходів захисту та рівня захищеності, яка проводиться при атестаційних випробуваннях та в процесі оперативного контролю.

Акустичні хвилі, поширюючись від джерела, впливають і на огороджувальні елементи конструкцій приміщень. Вібрації, поширюючись по конструкціях будівель, створюють канали витоку мовленнєвої інформації. При цьому, як експериментально встановлено, звукопоглинаючі покриття майже не впливають на поширення віброколивань в жорстких конструкціях. Вібраційні коливання можуть мати значну амплітуду та поширюватись по жорстким комунікаціям на значні відстані і можуть бути перехоплені стетоскопами, лазерними засобами акустичної розвідки тощо.

Особливості мовленнєвих сигналів, що визначають дальність їх поширення, полягають у наступному:

- мовленнєвий сигнал являє собою процес сплескового характеру з частотним діапазоном від 50 Гц до 10 кГц;
- тривалість сплесків - від 15 до 150 мс;
- сплески згруповані в пачки по 2-8 штук в кожній з проміжками між пачками від 10 мс до 1 с;
- наявність в спектрі сигналу основного тону з частотою 75-800 Гц;
- наявність в спектрі сигналу формант, частоти яких найчастіше лежать в діапазонах f_1 = (300 ... 1000) Гц, f_2 = (1000 ... 2000) Гц, f_3 = (2000 ... 3000) Гц, f_4 = (3000 ... 4000) Гц, f_5 = (4000 ... 5000) Гц.

Експериментальними дослідженнями встановлено, що мовленнєві сигнали, поширюючись по елементах огороджувальних конструкцій приміщення, загасають з різними швидкостями. Більш високочастотні складові спектра загасають швидше, і мовленнєвий сигнал спотворюється. Для забезпечення захисту мовленнєвої інформації у виділеному приміщенні можуть застосовуватися, в першу чергу, пасивні методи, які реалізуються при будівництві будівель, і активні методи, засновані на створенні в елементах конструкцій маскувальних сигналів зі спектром частот, що перекриває частоти мовленнєвих сигналів [1].

Оцінка ступеня захищеності мовленнєвої інформації у виділеному

приміщенні здійснюється на базі методів оцінки звукоізоляції приміщень з подальшим визначенням розбірливості мовленнєвих сигналів, що поширюються по огороджувальних елементах конструкцій приміщень, в місцях її можливого перехоплення.

Акустичні хвилі, які утворюються в виділеному приміщенні в результаті мовленнєвої діяльності, впливають на огороджувальні елементи конструкцій приміщень з рівнями звукового тиску порядку 70 дБ в частотному діапазоні від
50 Гц до 10 кГц. При цьому акустичні хвилі впливають на огороджувальні елементи конструкцій приміщень під різними кутами і має місце наявність багаторазово відбитих акустичних хвиль.

Оскільки суттєвий вплив на погіршення сприйняття мовленнєвої та іншої акустичної інформації мають різного роду шумові завади, і методи захисту акустичної інформації ґрунтуються на забезпеченні такого співвідношення між корисним сигналом і шумом, при якому сприйняття інформації певною мірою було б неможливим, то в якості критерію захищеності використовують відповідність нормам відношення сигнал/шум, виміряного в контрольних точках можливого перехоплення інформації.

Захист мовленнєвої інформації від витоку акустичними каналами з використанням як пасивних, так і активних методів захисту може виявитися або недостатньою, або надлишковою через неадекватність застосованих моделей можливих каналів витоку мовленнєвої інформації, моделей джерела мовленнєвого сигналу та моделей оцінки ступеня захищеності.

Моделювання джерела мовленнєвого сигналу у вигляді "білого" шуму із заданим діапазоном частот і заданим рівнем звукового тиску в 70 дБ не враховує сплескового характеру мовленнєвого сигналу. Розрахунок ступеня захищеності мовленнєвої інформації в виділеному приміщенні на базі методу оцінки розбірливості мови (в його різних варіантах) вимагає оцінки достовірності та визначення довірчих інтервалів.

Отже, однією з актуальних проблем в подальшому розвитку систем акустичного та віброакустичного зашумлення розмов у захищеному приміщенні є забезпечення ефективного та безперервного контролю за якістю завадових коливань.

У всіх сучасних системах активного зашумлення у тій чи іншій мірі впроваджено елементи (пристрої, системи), що дозволяють контролювати та регулювати параметри завад.

В доповіді розглядається система контролю, побудована за модульним принципом, яка дозволяє забезпечити всеосяжний постійний контроль працездатності всіх елементів системи захисту і безперервний моніторинг стану акустичних і віброакустичних каналів витоку мовленнєвої інформації.

Загальні модулі системи:

- модуль збору та обробки інформації з винесених датчиків акустичного та віброакустичного контролю (дистанційний комунікатор);

- модуль дистанційного групового управління генераторами завад;
- модуль активного захисту (генератори завад та віброакустичні випромінювачі).

Література

1. В. К. Железняк, И. Б. Бураченок, Д. С. Рябенко. Критерии оценки защищенности от утечки речевых сигналов / Весці Нацыянальнай акадэміі навук Беларусі. Серыя фізіка-тэхнічных навук. 2017. №1. С. 122–128.

Сергієнко М.О.
студент групи КСД-42

ЕВОЛЮЦІЯ СТАНДАРТУ USB

USB (Universal Serial Bus (універсальна послідовна шина)) - інтерфейс для підключення пе-риферійних пристроїв. Спочатку використовувався в комп'ютерах, але надалі набув широкого поширення і зараз можна зустріти в автомобілях, стереосистемах, телевізорах та інших видах техніки і складних приладах.

Стандарт USB розробили сім компаній: «Compaq», «Digital Equipment», IBM, Intel, «Microsoft», NEC і «Northern Telecom». З листопада 1994 до листопада 1995 року було анонсовано кілька версій протоколу (USB 0.7, 0.8, 0.9, 0.99, 1.0 Release Candidate). Влітку 1996 року на ринку з'явилися перші комп'ютери з портами USB.

Існує три основні формати USB-конекторів:

- стандартний формат, призначений для робочого столу або портативного об-ладнання (наприклад, USB флеш-драйвери);
- міні-USB, призначені для мобільного обладнання (в даний час не рекомендуються тільки міні-B, які використовуються багатьма камерами);
- мікро-USB, для мобільного обладнання (більшість сучасних мобільних теле-фонів).

USB 1.0

Версія представлена в січні 1995 року.

Технічні характеристики:

- високошвидкісне з'єднання — 12 Мбіт/с;
- максимальна довжина кабелю для високошвидкісного з'єднання — 3 м;
- низькошвидкісне з'єднання — 1,5 Мбіт/с;
- максимальна довжина кабелю для низькошвидкісного з'єднання — 5 м;
- максимальна кількість пристроїв підключення (враховуючи концентратори) — 127;
- можливе підключення пристроїв із різними швидкостями обміну інформа-цією;
- напруга живлення для периферійних пристроїв — 5 В;
- максимальний струм споживання на один пристрій — 500 мА.

USB 1.1

Випущена в вересні 1998. Виправлені проблеми, виявлені у версії 1.0, в осно-вному, пов'язані з концентраторами. Перша масова версія.

USB 2.0

Версія USB 2.0 випущена в квітні 2000 року, вона відрізняється від USB 1.1 лише підвищеною швидкістю передачі та незначними змінами в протоколі передачі даних для режиму Hi-Speed (480 Мбіт/с).

Сигнали в 4-провідникових кабелях USB 1.0 – USB 2.0 передаються двома екранованими провідниками на 2-й та 3-й контакти штекера.

Існує три швидкості роботи пристроїв USB 2.0:

- Low-speed 10—1500 Кбіт/с (використовується для інтерактивних пристроїв: клавіатури, мишки, ігрові контролери);
- Full-speed 0,5—12 Мбіт/с (аудіо/відео пристрої);
- Hi-speed 25—480 Мбіт/с (відео пристрої, пристрої зберігання інформації).

USB OTG

Технологія USB On-The-Go розширює специфікації USB 2.0 для легкого з'єд-нання периферійних USB-пристроїв безпосередньо між собою без задіяння комп'ю-тера. Прикладом застосування цієї технології є можливість підключення фотоапа-рата напряму до принтера. Цей стандарт виник через об'єктивну потребу надійного з'єднання особливо поширених USB-пристроїв без застосування комп'ютера, якого в потрібний момент може й не бути під руками.

Бездротовий USB

Офіційна специфікація протоколу була анонсована в травні 2005 року. Дозво-ляє організовувати бездротовий зв'язок із високою швидкістю передачі даних: до 480 Мбіт/с на відстані 3 метрів та до 110 Мбіт/с на відстані 10 метрів. Для бездротового USB часом використовують абревіатуру WUSB. Розробник протоко-лу, USB-IF, віддає перевагу офіційній назві протоколу Certified Wireless USB.

USB 3.0

В листопаді 2008 року робоча група USB 3.0 Promoter Group заявила про заве-ршення робіт над специфікацією нового високошвидкісного інтерфейсу USB 3.0, названого SuperSpeed USB. USB 3.0 є наступним етапом еволюції технології USB. Новий інтерфейс забезпечує максимальну швидкість передачі даних в 10 разів біль-шу, ніж USB 2.0 (тобто 10 × 480 Мбіт/с = 4,8 Гбіт/с). Інші важливі властивості — покращені показники енергоефективності та збільшений максимальний струм жив-лення периферійного пристрою до 900 мА. Крім того, розробниками заявлена зво-ротна сумісність USB 3.0 із попередньою версією — USB 2.0, причому роз'єми но-вого стандарту прийнято виділяти синім кольором пластику (інколи — червоним).

USB 3.1

9 вересня 2013 року USB 3.0 Promoter Group опублікувала специфікації онов-леного стандарту — USB 3.1, зі швидкістю передачі до 10 Гбіт/с. Після виходу стан-дарту USB 3.1 організація USB-IF оголосила, що роз'єм USB 3.0 з швидкістю 5 Гбіт/с (SuperSpeed) тепер будуть класифікуватися як USB 3.1 Gen 1, а нові роз'єми USB 3.1 (SuperSpeed USB 10Gbps) — як USB 3.1 Gen 2. В USB 3.1 Gen 2, окрім збі-льшення швидкості до 10 Гбіт/с, були знижені затримки кодування до 3 % перехо-дом на схему кодування 128b/132b.

USB 3.2

22 вересня 2017 некомерційна організація USB Implementers Forum (USB-IF) опублікувала специфікацію стандарту USB 3.2, заключна ревізія для USB 3.x. Оно-влення принесе вдвічі більшу швидкість передачі даних у порівнянні з USB 3.1 зав-дяки двом лініям на 5 Гбіт/с або 10 Гбіт/с, тобто в результаті 10 або 20 Гбіт/с. Сучас-ні кабелі USB-C, вже підтримують такий «двохлінійний» режим.

USB PowerShare

Функція USB PowerShare дозволяє виконувати зарядку пристроїв USB чи їх живлення від такого комп'ютера чи ноутбука, в якого відключене живлення або ко-ли він — у режимі сну/гібернації тощо. Якщо роз'єм USB підтримує функцію PowerShare, то позначається він додатково блискавкою.

USB 4

У USB 4 буде новий базовий протокол, заснований на Thunderbolt 3. Макси-мальна швидкість буде до 40 Гбіт/с, збережеться зворотна сумісність з USB 3.2, USB 2.0 і Thunderbolt 3. Очікується, що остаточна специфікація стандарту буде опублікована в середині 2019 року.

Вергун А.І.
студент групи ПДМ-51

ПРОБЛЕМИ ІСНУЮЧИХ РІШЕНЬ СЕРЕД СИСТЕМ «ІНТЕРНЕТУ РЕЧЕЙ» В ПРОМИСЛОВОСТІ

Анотація:

У даній статті мова йде про проблеми існуючих рішень в системах Промислового Інтернету речей. Проведений аналіз існуючих систем . Запропоновано реалізацію вирішення проблеми масштабованого, енергоефективного впровадження Промислового Інтернету речей.

Основна частина:

З рівнем розвитку технологічного прогресу та зі зростанням кількості сенсорних приладів, які використовуються в промисловості виникли потреби в існуючих системах, які будуть займатись контролем процесу та збором інформації. Основні проблеми, які досі існують при впровадженні існуючими рішеннями систем «Інтернету речей» в промисловості, пов'язані з: витратами під час управління мережею, масштабованістю та зоною покриття самої мережі.

Рішення для Індустріальних мереж Інтернету речей можна поділити на два табори. Перший - це рішення з використанням приладів з відносно малою зоною покриття.

Другий - з використанням приладів з великою зоною покриття.
Системи з малою не великою зоною покриття були першими для управління бездротовою сенсорною мережею. Недоліками цієї реалізації є великі витрати на установку мережі та складне масштабування мережі відповідно до збільшення зони покриття. Також тяжкою задачею є забезпечення функціонування та адміністрування цієї мережі та її адміністрування. Масштабування даної мережі є проблематичним, оскільки зростає складність управління вузлами в мережі.
Також гострою проблемою для таких мереж являється необхідність підключення високошвидкісного інтернету, що можливо забезпечити в урбаністичних районах, але складно в далеко віддаленій або сільській місцевості.
Іншим підходом для вирішення проблем мереж близької дії були використані стільникові мережі. Їхніми перевагами являється широкий діапазон дії, як перевага також є використання вже існуючих стандартів, таких як GSM та GPRS.
Основною проблемою цих систем є те, що вони створювались без урахування вимог Індустріального Інтернету речей. Сенсорна мережа потребує величезної кількості пристроїв з низькою пропускною спроможністю, які надсилають короткі повідомлення тільки один раз за певний обмежений проміжок часу.
Однак існує низка різних платформ, що виконують парадигму LP-WAN. Ці пропозиції використовують як і широкий діапазон покриття, що забезпечується стільниковими технологіями, так і низьким енергоспоживанням WSN. Багато рішень LP-WAN знаходяться на ранній стадії розробки, а інші вже розпочали свою архітектуру. LoRaWAN, Sigfox і Ingenu в даний час є платформами LP-WAN з найбільш готовими і оптимальними рішеннями.
LP-WAN використовує топологію зірки, де всі кінцеві вузли безпосередньо підключені до базової станції. LP-WAN модем встановлюється на цих пристроях. У деяких випадках шлюзи можуть бути використані для підключення кластера вузлів до базової станції (утворює топологію зірки зірок). Що стосується з'єднання кінцевих вузлів з мережею та базовою станцією, більшість із запропонованих платформ використовують діапазони частот ISM.
Для того щоб знизити енерговитрати, більшість реалізацій фокусуються на підключенні до висхідної лінії зв'язку, тому низхідна лінія суттєво обмежується, отже час, необхідний для отримання даних є меншим.
Підсумовуючи, перевагами LP-WAN є:

- Масштабованість
- Широкий діапазон покриття
- Заощадження роумінгу та на встановленні мережі
- Низькі енерговитрати

Отже, серед запропонованих реалізацій вирішення проблеми стабільного, дешевого та масштабованого впровадження Промислового Інтернету речей, найбільш вигідним являється використання LP-WAN мереж, які в свою чергу дає якісну перевагу над своїми конкурентами. Основним недоліком таких мереж є використання нових або мало поширених стандартів.

Використана література

1. Як влаштований промисловий інтернет речей https://www.it.ua/knowledge-base/technology-innovation/promyshlennyj-internet-veschej
2. M. T. Lazarescu, "Design of a WSN platform for long-term environmental monitoring for IoT applications", IEEE J. Emerg. Sel. Topics Circuits Syst., IEEE, vol. 3, no. 1, pp. 45-54, Mar. 2013.
3. What is LPWAN and the LoRaWAN Open Standard? https://www.iotforall.com/what-is-lpwan-lorawan/
4. Introduction to IoT communication protocols https://www.iotforall.com/what-is-lpwan-lorawan/

Петлицький В.В.
студент групи ПДМ-51

РОЗРОБКА ОРГАНАЙЗЕРУ ФІНАНСІВ

Анотація

Інформаційна система фінансового менеджменту становить безперервний і цілеспрямований відбір відповідних інформаційних показників, які необхідні для здійснення аналізу, планування та підготовки ефективних управлінських рішень за всіма напрямами фінансової діяльності. Інформаційна система фінансового менеджменту покликана забезпечувати необхідною інформацією не тільки управлінський персонал та власників самого підприємства, але й задовольняти інтереси широкого кола зовнішніх її користувачів.

Основна частина

Необхідність створення фінансового органайзеру була викликана в економії часу користувачів по роботі з фінансовим плануванням, а також автоматизацією фінансового аспекту користувача. Настільні додатки перестали бути статичними, з не зручним інтерфейсом, а оперативність відновлення інформації на їхніх вікнах стала запорукою успіху багатьох комерційних проектів.

Предмет дослідження – робота фінансового органайзеру. Фінансовий органайзер - це програмне забезпечення, що дозволяє користувачам вносити в додаток свої витрати, категорії витрат, слідкувати за своїми змінами в фінансовому становищі, слідкувати за прибутком, відтоком капіталу, планувати свою діяльність з урахуванням усіх фінансових аспектів життя.
Мета роботи полягає у створенні автоматизованої системи управління фінансами.

Принцип роботи фінансового органайзеру полягає в зборі інформації щодо витрат та прибутків користувача, на основі якої програмне забезпечення допомагає відслідковувати, запам’ятати інформацію, знайти закономірності в управлінні фінансовими операціями, побудувати динамічні графіки, дати користувачу пораду в регулюванні свого фінансового становища. Після авторизації в системі, користувач бачить розділи, пов’язані з фінансовими операціями, наприклад комунальні платежі, доходи, витрати і

тд. Все що потрібно зробити користувачу, так це записати свою витрату та обрати категорію витрат, у разі необхідності додати коментар витрати. Після цього в базу даних будуть внесені дані про витрату/дохід. Система автоматично порахує відношення витрат до доходів за конкретні періоди часу, а також надасть користувачу більш детальну інформацію про його фінансові операції.

Практичне значення одержаних результатів полягає у тому що фінансовий органайзер пропонує насамперед зручний інтерфейс для додавання інформації, будову наочних динамічних графіків, вбудований розумний помічник для управління фінансами.

Перелік використаної літератури

1. Джеймс Ван Хорн Фінансовий менеджмент
2. ОСОБЛИВОСТІ ОБЛІКУ КОМУНАЛЬНИХ ПЛАТЕЖІВ В ОРЕНДОВАНИХ НЕЖИТЛОВИХ ПРИМІЩЕННЯХ Балан О.С., Мартиненко О.С.
3. C#.NET and the WPF LISTVIEW Richard Thomas Edwards
4. Windows Presentation Foundation Development Cookbook Kunal Chowdhury

Золотухіна О.А.
к.т.н., доцент
Виноградний І.
студент групи ППЗМ-71

ДОСЛІДЖЕННЯ ТА ВПРОВАДЖЕННЯ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ДЛЯ ФРОНТЕНД ДОДАТКІВ

Дослідження балансування навантаження в програмно-конфігурованих мережах(SDN).

Суть проблеми:

У сьогоднішньому світі у відповідь на нові потреби людей створюються все нові послуги, можливості та технології, які намагаються відповідати високим вимогам, що встановлюються споживачами. Найбільшої швидкості розвитку на сьогодні набувають мережі стільникового зв’язку. Впровадження нових сервісів і все більш активна передача разом з голосом даних і мультимедії інформації призводить до значного збільшення обсягів трафіку в мережах мобільного зв'язку. Зростання трафіку вимагає від операторів використання нових підходів до побудови мереж, які повинні забезпечувати економічну передачу великих обсягів трафіку та підтримку нових послуг а також забезпечення виконання потреб користувачів, які зростають з кожним роком все більше. Можливості концепції SDN. Орієнтуючись на перспективи розвитку концепції IoE (Internet of Everything) головною задачею оператора зв’язку є забезпечення інтелектуальної обробки та доставки послуг, що здійснюється на основі даних – це означає, що підключення мають працювати постійно, а сервіси відповідати з

практично нульовими затримками в часі, що призводить у свою чергу до надання сервісу поза часовими і просторовими обмеженнями. Для вирішення цієї задачі, а також для забезпечення еластичності, масштабованості та гнучкості мереж операторів зв'язку пропонується програмно-конфінурована мережа (SDN - Software Defined Network). Стандартне уявлення про мережу представляє її у вигляді двох площин – площини даних і площину контролю. Площина даних займається обробкою пакетів з призначеним локальним станом пересилання. У свою чергу, в процесі роботи мережі перед площиною контролю стоїть безліч задач і цілей: роутінг – за який відповідають розподілені алгоритми маршрутизації; ізоляція трафіку: ACL, VLAN та фаєрволли; трафік інежинерінг. Проблема в відсутності модульності, що призводить до того, що навіть за наявності добре продуманого протоколу маршрутизації, рішення про передачу пакетів в тому чи іншому напрямку приймається кожним роутером самостійно . Концепція програмно-конфігурованих мереж забезпечує програму контролю, яка виходячи із завдань, що ставлять перед собою оператори висловлює вимоги до політики і правил передачі і може створювати механізми пересилки практично будь-якої складності. SDN також має рівень на якому відбувається віртуалізація мережі, де групи фізичних пристроїв представлені у вигляді одного або декількох віртуальних пристроїв, кожен з яких виражає ту чи іншу політику в мережі, що значно спрощує процеси масштабування мережі і взагалі застосування цих самих політик до груп пристроїв (див. рис.1). Мережева операційна система здійснює переклад цих вимог на мову зрозумілу для мережевих пристроїв.

Одним із ключових викликів в сценаріях маршрутизації є досягнення балансування навантаження. В даний час процедура балансування трафіку між маршрутизаторами для настройки переадресації маршрутів відбувається вручну. Так, якщо модель руху трафіку змінилася, конфігурація за маршрутами повинна бути змінена відповідно до нової моделі вручну. Для збільшення ефективності цього сегмента необхідне рішення для оптимізації балансування навантаження. Технологія SDN відіграє ключову роль у пропонованому рішенні, що дозволяє автоматизувати балансування трафіку навіть у багатовекторних шлюзах. Передумовою для даного розрахунку маршруту є те, що кожен вузол має інформацію про топологію мережі. Для забезпечення узгодженості та запобігання петель маршрутизації, незалежно від того, який протокол використовується для розрахунку маршруту, про топологію на кожному вузлі повинна бути узгоджена по всій мережі і розрахунок маршруту, використовуваний кожним вузлом, повинен бути однаковим.

Для узгодження роботи контролерів в кластері пропонується викристовувати систему, яка обчислює шляхи для послуг залежно від фактичного обсягу трафіку. Якщо обсяг трафіку збільшується наприклад на ступінь, оригінальний шлях не може задовольнити новим вимогам, у такому випадку нова логіка автоматично перемикає трафік на новий шлях і навпаки. Також, розрахунок шляху більше не обмежується принципом найкоротшого шляху. Крім надання централізованих глобальних можливостей розрахунку, пропонована система

використовує стандартні інтерфейси для зв'язку з передавальними пристроями. Дана логіка може бути використана для управління трафіком на кордоні мережі, або всередині самої IP мережі.

Пропонується 3 етапи:

1. Заміна граничних маршрутизаторів.
2. Заміна ключових транзитних маршрутизаторів.
3. Поступова заміна маршрутизаторів, що залишилися.

Гулін В.О.

студент групи ПДМ-51

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ВИКОРИСТАННЯМ СУЧАСНИХ ТЕХНОЛОГІЙ ШИФРУВАННЯ. ВИКОРИСТАННЯ ЕЦП І MOBILE ID

Анотація:

У даній статті мова йде про застосування сучасних технологій шифрування при розробці програмного забезпечення на прикладі ЕЦП і Mobile ID.

Показано сучасний стан ЕЦП і Мобайл ID на ринку України.

Велике місце займає розгляд самої технології шифрування документації.

Основна частина:

У сучасному світі люди цінують час, легкість використання чого-небудь, зручність взаємодії з різним технологіями і побутовими речами. Так робота з документацією займає багато часу, є дуже важливою і вимагає величезної захищеності. Будь-який витік інформації веде за собою великі проблеми. І якщо раніше криптографія і шифрування здавалося долею виключно спеціальних служб, то зараз їх необхідно застосовувати в бізнесі.

Що ж таке шифрування? Це перетворення інформації, що робить її нечитаною для сторонніх. При цьому довірені особи можуть провести дешифрування і прочитати вихідну інформацію. Існує безліч способів шифрування / дешифрування, але секретність даних заснована не на таємному алгоритмі, а на тому, що ключ шифрування (пароль) відомий тільки довіреним особам.

На допомогу при роботі з документацією приходить електронний цифровий підпис. Електронні підписи полегшують життя керівникам, співробітникам відділу кадрів і менеджерам в різних галузях. Технологія дозволяє цим працівникам збирати підписи від клієнтів і співробітників і управляти ключовими документами і записами з мінімальними зусиллями. Більше немає необхідності друкувати, надсилати поштою або сканувати фізичні копії документів. Проте, рішення для електронного підпису не

отримали широкого розповсюдження, але основна технологія використовується для стимулювання інновацій навіть в деяких з найжорстокіших секторів бізнесу.

Підвидом електронних підписів є цифровий підпис. Цифрові підписи є одними з найбільш важливих компонентів програми електронного підпису, і вони можуть забезпечити безпеку, юридичну силу і ефективність управління записами при використанні методу електронного підпису. Таким чином, створення електронного підпису не повинно відбуватися без підтримки цифрового підпису.

Цифровий підпис - це конкретна технічна реалізація електронного підпису, що включає криптографічні методи з використанням ключів підпису, пов'язаних з підписала стороною. Цифровий підпис посилається на підписаний документ або транзакцію, так що будь-яка наступна модифікація може бути виявлена.

Для забезпечення конфіденційності сполучення застосовується шифрування. Для шифрування і дешифрування повідомлення використовується пара ключів - Відкритий і закритий ключі. Вони використовуються і для формування електронного цифрового підпису (ЕЦП). Для шифрування повідомлення використовується Відкритий ключ одержувача і Закритий ключ відправника. Отримане зашифроване повідомлення розшифровується одержувачем з використанням свого Закритого ключа і Відкритого ключа відправника.

Mobile ID - це електронний цифровий підпис (ЕЦП в мобільному). Mobile ID можна використовувати у корпоративних ринках, державних установах, електронної комерції, охороні здоров'я, освіті, фінансових установах. Завдяки Mobile ID, ЕЦП можна використовувати де завгодно: на телефоні, планшеті, смартфоні. Не потрібно відвідувати установи, що б скористатися послугами цифрового підпису. Для використання підпису не потрібно мати спеціальне обладнання, тільки SIM-карту з підтримкою Mobile ID. Видається Унікальний ПІН-код для авторизації та підпису. Для використання Mobile ID, наприклад, розробнику сайту, який хоче дозволити своїм користувачам авторизуватися через Mobile ID, потрібно звернутися до сертифікаційного центру, у неї є база даних всіх користувачів Mobile ID, їх телефонні номери і особисті коди, зробити виклик веб-сервісу, написату купу класів та налаштовувати купу параметрів, але для полегшення цього процесу існує багато бібліотек, котрі дозволяють використовувати mobile ID дуже швидко, та просто. Після цього можно налаштувати Mobile ID як для авторизації, так і для використання ЕЦП.

На цей час послугу Mobile ID в Україні, надають такі оператори: Київстар, Vodafone.

Від початку 2019 року всі електронні адміністративні послуги та сервіси створюють із можливістю електронної ідентифікації за допомогою технології MobileID.

З огляду на сучасний стан інформаційних технологій, це найкращий метод підписи для забезпечення цілісності та походження електронного документа.

У разі успішної реалізації даного проекту держава зможе використовувати його в якості основи для надання різних адміністративних послуг. У перспективі, через mobile ID можна буде отримати всі послуги, доступні також і через цифровий електронний паспорт, через систему авторизації bank ID, захищену електронно-цифровий підпис.

Використана література

1. Margaret Rouse, Digital signature, https://searchsecurity.techtarget.com/definition/digital-signature
2. Офіційна сторінка Київстар присвячена Mobile ID, https://kyivstar.ua/ru/sme/mobile-id
3. Сторінка у вікіпедії присвячена електронному цифровому підпису, https://en.wikipedia.org/wiki/Digital_signature
4. Дуброва Ярослава, Застосування електронного цифрового підпису в публічних закупівлях, https://i.factor.ua/ukr/journals/bb/2016/june/issue-24/article-19093.html

Стрілецький Д.Ф.
студент групи ПДМ-51

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ РОБОТИ З ШИФРОВАНИМИ БАЗАМИ ДАНИХ

У даній статті мова йде про зберігання інформаційнійних масивів даних в файлову організацію та організацію баз даних. Описані принципи організації даних в баз даних. Частина присвячена розподіленим базам даних, в тому числі Blockchain Основна частина: Відомі два підходи до організації інформаційних масивів: файлова організація та організація у вигляді бази даних. Характерна риса файлового підходу − вузька спеціалізація як обробних програм, так і файлів даних, що служить причиною великої надлишковості, тому що ті самі елементи даних зберігаються в різних системах. Оскільки керування здійснюється різними особами (групами осіб), відсутня можливість виявити порушення суперечливості збереженої інформації. База даних може бути визначена як структурна сукупність даних, що підтримуються в активному стані та відображає властивості об’єктів зовнішнього (реального) світу. В базі даних містяться не тільки дані, але й описи даних, і тому інформація про форму зберігання вже не схована в

сполученні "файл-програма", вона явним чином декларується в базі. База даних орієнтована на інтегровані запити, а не на одну програму, як у випадку файлового підходу, і використовується для інформаційних потреб багатьох користувачів. З розвитком інформаційного забезпечення систем автоматизованої обробки інформації, прагненням забезпечити виконання нових режимів обробки даних у реальному часі і з мультидоступом до схованих даних позначилась нова тенденція до складення інформаційного забезпечення розподілених баз даних. Один з прикладів розподілених баз даних є Blockchain. Blockchain це база данних, записи до якої здійснюються за рахунок криптографічних алгоритмів з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел. Транзакції Bitcoin - це підписаний розділ даних, який транслюється в мережу і записуються в блоки. Вона посилається на попередні транзакції і переводить певну кількість BTC (Bitcoin-монет) на зазначений відкритий ключ (Bitcoin-адреса).

Використана література

1. Pedro Franco. The Blockchain. Understanding Bitcoin: Cryptography, Engineering, and Economics. 2. Melania Swan Blockchain: Blueprint for a New Economy. – Krause Publication 3. Організація баз даних: практичний курс: Навч. посіб. для студ./А.Ю. Берко, О.М. Верес; Нац. Ун-т «Львів. політехніка».

Бондарчук А.П.
д.т.н., доцент
Сорокін Д.
аспірант
Сеньков О.
аспірант
Дібрівний О.
аспірант

ДОСЛІДЖЕННЯ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ LTE ДЛЯ РОЗУМНОГО ВИРОБНИЦТВА ТА ПРОМИСЛОВОСТІ (PRIVATE LTE & SMART MANUFACTURING)

Перспективи та шляхи розвитку приватних мереж на базі технологій 4-5 поколінь дуже великі. набубільш яскравими є:

I. Приватні мережі в стандартах 4-5G, як крок до розвитку автоматизації промисловості та модернізації приватних та державних підприємств;

II. З появою стандарту 4-5G виникає необхідність в зміні фокусу, від класичної форми надання сервісів клієнтам B2C – до створення нових

сервісів промислової необхідності (мається на увазі будівництво та розгортання приватних мереж LTE, 5G, в вугільній, енергетичній, гірничо-збагачувальної та інших галузях економіки);

III. Використання приватного радіодоступу 4-5G – як транспортну мережу для підключення пристроїв NB-IoT;

IV. Проблеми, що стримують розвиток приватних мереж LTE, 5G в Україні:

a. Відсутність нормативної бази – як інструмента, що регулює діяльність приватних мереж, які використовуються з метою забезпечення промислової необхідності всіма необхідними сервісами в стандарті LTE, 5G;

b. Відсутність технологічної нейтральності, при використанні частотного спектру для розгортання приватної мережі в стандарті LTE, 5G;

c. Відсутність вільного частотного спектру, для вільного використання в приватних мережах LTE, 5G, який не створюватиме перешкод для мобільних операторів;

Великі виробники телекомунікаційного обладнання вже сьогодні готові поставляти обладнання не тільки профільним телекомунікаційним компаніям та операторам, а і великим корпоративним клієнтам які потребують нових сервісів при розгортанні мереж Private LTE. Тобто, мова йде про LTE корпоративного рівня, побудованих локально. Для цього може використовуватись частина спектра мобільних операторів, або виділений спектор державним регулятором; В мереж Private LTE – мова йде, переважно про використання технології NB-IoT, тобто, все це призначене для промислового інтернет речей та телеметрії, а також промислово необхідного сервісу PtT (push to talk). Очікується затребуваність цих рішень в гірничодобувній промисловості, на транспорті, в ЖКГ. Мережа Private LTE дозволяє об'єднати M2M-пристрої в закриту локальну мережу всередині компанії. Такі рішення вже реалізовані такими компаніями як Ericsson (золотодобувна шахта в Швеції), RedLine (горно-збагачувальна шахта в Канаді), а також інші вендери у ряді корпоративних клієнтів, що вирішують питання розумних міст (Smart City).

Обсяг світового ринку що потребує інвестицій в сектор приватних мереж (Private LTE), для клієнтів B2B очікується досить великого зростання і може перевищити 2,5 млрд дол., до 2023 року очікується його зростання в середньому на рівні 28% щорічно. Перевагою приватних LTE-мереж в порівнянні, наприклад, з Wi-Fi, є підвищена надійність і безпека, а також низькі затримки. У перспективі аналогічним чином будуть пропонуватися мережі Private 5G, більш того, це стане основним вектором впровадження 5G, оскільки саме в B2B-сегменті набагато більше інноваційних сценаріїв

використання, ніж для B2C-ринку, для якого це поки лише підвищена пропускна здатність абонентського каналу передачі даних.

Литература:

1. *Gubbi J. et al. Internet of Things (IoT): A vision, architectural elements, and future directions //Future generation computer systems. – 2013. – Т. 29. – №. 7. – С. 1645-1660.*
2. *Бондарчук А. П. Когнітивні технології та головні напрями розвитку ІКТ //Вісник Державного університету інформаційно-комунікаційних технологій. – 2013. – №. 1. – С. 57-62.*
3. *Sun Y., Huang Y. X., Chen L. M. A centralized LTE private wireless network architecture for smart grid communication network //Applied Mechanics and Materials. – Trans Tech Publications, 2014. – Т. 687. – С. 2363-2366.*
4. *Davis J. et al. Smart manufacturing, manufacturing intelligence and demand-dynamic performance //Computers & Chemical Engineering. – 2012. – Т. 47. – С. 145-156.*

Асеева Л.А.
аспирант

АНАЛИЗ ПОДХОДОВ К КЛАССИФИКАЦИИ СОСТАВЛЯЮЩИХ ОПАСНОСТИ ПРИ ПОСТРОЕНИИ СИСТЕМ КИБЕРЗАЩИТЫ ПРЕДПРИЯТИЙ

Проведен анализ основных составляющих опасности в системе информационной безопасности предприятий, к которым отнесены атаки, угрозы и уязвимости. На основе современного состояния исследований рассмотрены распространенные списки и существующие классификаторы атак и уязвимостей, которые позволяют профессиональному сообществу использовать их для описания и исследования составляющих опасности. Результаты работы могут быть применены для анализа существующих угроз и описания составляющих системы управления информационной безопасности предприятия.

ANALYSIS OF THE DANGER COMPONENT CLASSIFICATION IN THE CONSTRUCTION OF ENTERPRISE CYBERSECURITY SYSTEMS

Asyeyeva L.A., PhD student, State University of Telecommunications, Kiev

The analysis of the main components of the danger in the system of information security of enterprises, which include attacks, threats and vulnerabilities, is considered. On the basis of the current state of research, common lists and existing classifiers of attacks and vulnerabilities that allow the professional community to use them to describe and study the components of danger are described. The results of the work can be applied to analyze existing threats and describe the components of the enterprise information security management system.

Принятие мер для реализации так называемой триады целей информационной безопасности, предполагающей обеспечение конфиденциальности, целостности и доступности информации, является основным подходом в создании систем кибербезопасности. Чтобы создавать и совершенствовать эффективные системы информационной безопасности предприятий необходимо проанализировать основные составляющие опасности.

Целью данной работы является анализ основных составляющих опасности при построении системы информационной безопасности предприятия. Для достижения поставленной цели в работе рассмотрены некоторые разновидности атак, уязвимостей и угроз, являются основными составляющими кибербезопасности, приведены и описаны распространенные списки и классификаторы, позволяющие профессиональной сообществу использовать их для описания и исследования составляющих опасности.

Результаты работы могут быть положены в основу анализа существующих угроз информационной безопасности и описания составляющих системы управления информационной безопасности отдельного предприятия и разработки комплекса мер по их предупреждению.

Литература

1. Kevin Granville "Recent cyberattacks". feb. 5,2015 URL: https://www.nytimes.com/interactive/2015/02/05/ technology/recent-cyberattacks.html?_r=1

2. James A. Lewis "Rethinking Cybersecurity: Stratedy, Mass Effect and States".CSIS. Jan. 2018. 50c.

3. Cve details. URL: https://www.cvedetails.com/vulnerability-search.php

4. CWE List .View the List of Weaknesses URL: https://cwe.mitre.org/data/index.html Apr. 13 2018.