

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ**



**II МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ
«TELECOMMUNICATION: PROBLEMS AND INNOVATION»
22 квітня 2021 року
Збірник тез**

м. Київ

II Міжнародна науково-технічна конференція «Telecommunication: problems and innovation». Збірник тез. – К.: ДУТ, 2021.

Збірник містить тези доповідей учасників конференції, представлених на II Міжнародній науково-технічній конференції «Telecommunication: problems and innovation», яка проходила 22 квітня 2021 р. на кафедрі Телекомунікаційних систем та мереж Навчально-наукового інституту телекомунікацій Державного університету телекомунікацій, м. Київ.

Робочі мови – українська та англійська.

На конференції розглянуті проблеми, інновації та перспективи у сфері телекомунікацій.

СЕКЦІЯ 1

ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ

АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ ПЕРЕДАЧІ МУЛЬТИМЕДІЙНИХ ДАНИХ

Котвицький Олексій Костянтинович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

В основі обміну інформацією лежить три принципи та три види з'єднань систем зв'язку. Такими принципами представлення користувача в мережі зв'язку є: автентичність – це може бути персональний код, або адреса; мобільність – тобто доступ до інформаційних ресурсів з будь-якого місця, зокрема обмін мовними повідомленнями; захищеність – повідомлень від прослуховування та захист персональних повідомлень в мережі яка використовується для передачі повідомлень [1,с.74].



Рис. 1.1. Структура мережі доступу до мультимедійних повідомлень

Для передачі голосових (а в загальному мультимедійних) даних згідно рис. 1.1 спочатку потрібно розглянути ТфЗК або мережі з комутацією каналів. Згадані мережі існували дуже давно і спочатку були аналоговими (передача мови в смузі частот 0,3 до 3,4 кГц) та механічним (за методом здійснення з'єднання), потім прогрес в області цифрової техніки та теорії цифрової обробки сигналів призвів до появи АЦП, що проводили перетворення форми сигналу в часовій області в дискретні вибірки, а відтак в кодову послідовність імпульсів. Згаданий прогрес позначився в телефонії появою основного цифрового каналу (ОЦК частота дискретизації 8кГц і 8 розрядів на вибірку) тобто передачі із швидкістю 64 кбіт/с, та системи передавання з імпульсно-кодовою модуляцією (ІКМ).

Під РРСП розуміють технологію передавання каналів тональної частоти та типових трактів національної системи зв'язку за допомогою радіохвиль у вільному просторі. Не дивлячись на різновиди РРСП загальний принцип їх залишається однаковим.

Мережі з комутацією пакетів появилася значно пізніше і спочатку у вигляді локальних комп'ютерних мереж для організації передачі даних у вигляді пакетів, що містили інформаційні дані та маршрутного заголовка в локальній зоні (у межах відділу організації, підприємства). З появою персонального комп'ютера стала

можливою організація універсального інформаційного місця збільшуючи разом з тим його продуктивність та ефективність інформаційної системи. Створення телефонії на базі існуючих комп'ютерних мереж, об'єднуючи функціональні можливості обробки пакетного потоку, який визначає спосіб обробки телефонних розмов, без сумніву, є найбільш перспективним напрямком розвитку таких мереж. Перш за все тому, що комп'ютерні технології розвиваються швидкими темпами і стають невід'ємною частиною бізнес-процесів. Тому компаніям слід користуватися єдиною системою обміну даними і голосових повідомлень. Однак впровадження пакетної телефонії вимагає певної реорганізації мережі, адже нові сервіси й можливості вимагають нового програмного та технічного забезпечення.

В такому випадку існуючі комп'ютерні мережі можуть розширити свої можливості підпорядкувавши собі ще й телефонний зв'язок, тому для їх об'єднання слід застосувати технологію IP-телефонії [2,с.164].

В основі такого об'єднання лежить можливість використання комп'ютера не тільки у вигляді інструменту для обробки інформації, але як і засіб для комутації і передавання мовних даних. Через пакетний принцип передачі і комутації мовних даних відпадає необхідність кодування і синхронної передачі однакових по тривалості фрагментів мови. Отже практична можливість повної інтеграції голосу і даних поверх загальної інфраструктури обчислювальних мереж привела до появи так званої "пакетної телефонії" – технології передачі аналогових телефонних сигналів по мережах передачі даних з комутацією пакетів.

Описана модель доступу до мультимедійних повідомлень рис. 1.1., є базисною для вивчення (аналізу) і побудови (синтезу) IP-телефонних систем. Асинхронність транзакцій дозволяє з одного боку оптимізувати трафік за рахунок зниження середньої швидкості передачі, з іншого – за рахунок відносної свободи у відтворенні кожної транзакції компенсувати неідеальність каналу передачі.

Інформаційна модель на рис. 1.1 дозволяє змінити стандартну постановку задачі передавання мовного сигналу та задачі конструювання кодека мовного сигналу. Для систем IP-телефонії на відміну від традиційних реалізацій кодеки доцільно будувати із змінною швидкістю кодування.

Для телекомунікаційних мереж технологія на базі протоколу IP є основною. Це протокол мережного рівня, який забезпечує маршрутизацію пакетів в мережі. Він, проте, не гарантує надійну доставку пакетів. Таким чином, пакети можуть пропадати, затримуватися, передаватися по різних маршрутах (а значить мати різний час передачі) і т.д. На основі IP працюють протоколи транспортного рівня TCP і UDP.

Список використаних джерел:

1. Борщ В.И., Донец В.А., Коваль В.В., Лейбзон А.Я., Лесовой И.П. Оптимизация структур больших систем. – К.: Наукова думка, 2016. – 191 с.
2. Ramchandran K., Vetterli M. Best wavelet packet bases in a rate-distortion sense// IEEE Trans, on Image Process. – 2014. – Vol. 2, no. 2. – Pp. 160-175.

АКТУАЛЬНІСТЬ ВИКОРИСТАННЯ ДРОНІВ

*Коркач Микола Валерійович
Навчально-науковий інститут Інформаційних технологій
Державний університет телекомунікацій*

Досить широке поширення безпілотних літаючих апаратів (БПЛА), можливість їх використання навіть фізичними особами привели до появи цілого ряду нових науково-дослідних завдань. В першу чергу виникла необхідність постановки та розв'язання комплексу науково-дослідних завдань в області мереж БПЛА. Масштабне впровадження бездротових сенсорних мереж і необхідність збору інформації з них навіть в умовах знаходження цих мереж в важкодоступних районах привели до необхідності розглядати БПЛА або мережу БПЛА як елементи цих мереж з можливістю виконання функцій, наприклад, головних вузлів сенсорної мережі. При цьому для збору інформації з сенсорних полів з використанням БПЛА повинні використовуватися протоколи бездротових сенсорних мереж, а для передачі інформації в мережах зв'язку загального користування (МЗЗК) - протоколи мереж зв'язку загального користування.

Використання БПЛА фізичними особами вимагає, природно, розробки сучасних моделей і методів для їх ідентифікації [2].

Ринок БПЛА на сьогоднішній день зростає на 20% щороку, а аналітики прогнозують на кінець 2021 року збільшення загальносвітових витрат на робототехніку і безпілотні літальні апарати до \$ 130,5 млрд рис. 1.



Рисунок 1 – Графік продажу квадрокоптерів

Завдяки сильним зусиллям, спрямованим на підвищення продуктивності БПЛА, наприклад, мініатюризацію, енергоефективність тощо, безпілотники стали корисним інструментом, широко поширеним у різних напрямках діяльності людини. Ці пристрої, також відомі як безпілотні літаки, які мають великий попит в таких сферах, як військова, логістична, екологічна, моніторингу або рятувальні заходи [1].

Наприклад, безпілотні літаки усувають необхідність присутності людини для виконання небезпечних завдань, а отже, і ризики, пов'язані з деякими цими діями, різко скорочуються. У сфері телекомунікацій одним з найбільш перспективних

програм безпілотників є використання їх як допоміжного обладнання, спрямованого на розширення можливостей або покриття бездротових систем шляхом розгортання мережі антенно–цифрових комунікацій.

Цікавою стратегією, яка використовується для досягнення цієї мети, є додавання пристроїв для передачі даних, на борту БПЛА. Низьке енергоспоживання і висока кількість елементів зв'язку, які вони підтримують (комунікаційні чіпи, антени тощо) є одними з найцінніших функцій, які пропонують для виконання цього завдання. Таким чином, ці пристрої здатні розгорнути бездротові мережі, що діють як мережеві вузли в рамках архітектури системи, і дозволяють кінцевим користувачам / речам отримувати зв'язок через них.

Перелік літератури:

1. Галелюка І.Б. Моделювання бездротових сенсорних мереж / І.Б. Галелюка // Комп'ютерні засоби, мережі та системи. – 2016. – № 14. – С. 141 – 150.
2. Mobile Wireless Sensor Networks Overview / J. Rezazaden, M. Moradi, A. Samad Ismail // International Journal of Computer Communications and Networks, 2017.

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ WI-FI 6 IEEE 802.11AX ДЛЯ МЕРЕЖ З ВИСОКОЮ ШВИДКІСТЮ ПЕРЕДАЧІ ДАНИХ

*Полтавець Ігор Олексійович,
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

З розвитком інформаційних технологій постає потреба в збільшенні пропускної здатності бездротових мереж. Для створення складних високопродуктивних бездротових мереж, які б дозволили підвищити швидкість і надійність передачі інформації та забезпечити високу щільність абонентів, можуть бути використані точки доступу з підтримкою нового стандарту передачі IEEE 802.11ax, який задовільняє вищеперераховані потреби.

Дослідити нові можливості передачі інформації через бездротову мережу з високою швидкістю передачі даних та умови використання точок доступу з підтримкою стандарту IEEE 802.11ax. При побудові бездротової мережі з високою швидкістю передачі даних необхідно забезпечити достатню пропускну здатність для обслуговування великої кількості абонентів, належне відношення рівня сигналу до рівня шуму по всій зоні обслуговування, ефективне використання ефірного часу та усунення перешкод між точками доступу.

Досягаються поставлені цілі за допомогою переваг які надає використання стандарту IEEE 802.11ax. Стандарт 802.11ax підтримує теоретичну межу швидкості передачі даних до 9 Гбіт в секунду, тоді як в попереднього формату 802.11ac цей показник не перевищує 3,5 Гбіт. В реальності швидкість передачі даних у кінцевого користувача збільшиться на 40%. Зростання швидкості стався внаслідок використання так званої квадратурної амплітудної модуляції (QAM) 1024 - технології передачі цифрового сигналу в аналоговому вигляді.

802.11ax використовує метод доступу OFDMA що забезпечує більшу ефективність шляхом застосування тимчасового і частотного ресурсів, потужності і синхронізації між станціями й користувачами. Хоча максимальна швидкість передачі не збільшується на фізичному рівні, така схема дозволяє чергувати одночасні передачі від великої кількості користувачів, скорочуючи затримку для кожного з них. OFDMA дозволяє нарізати смугу 20, 40, 80 і 160 МГц на додаткові дрібніші підканали з визначеною кількістю піднесучих. Найменший виділений підканал в стандарті 802.11ax становить 26 піднесучих (2 МГц). У каналі 20 МГц є 9 доступних підканалів з 26 піднесучих, що дозволяє використовувати на приймання і передачу до 9 різних кадрів.

На теперішній час економія енергії є важливий параметр для пристроїв. За допомогою системи Target Wake Time пристрої з підтримкою стандарту IEEE 802.11ax можуть синхронізуватися з роутером тільки під час безпосередньо передачі даних. Тобто роутер вмикає Wi-Fi-модуль на пристроях, використовуючи його, тільки коли користувачеві це необхідно. В інший час, наприклад, коли смартфон буде лежати на столі без використання, система Target Wake Time буде відключати модуль Wi-Fi в ньому.

Висновки і перспективи. З розвитком бездротових технологій з'являється можливість створення складних високопродуктивних бездротових мереж, які дозволяють збільшити швидкості передачі, зменшити затримки, підвищити надійність та гарантувати повноцінне паралельне функціонування значної кількості абонентського обладнання.

Підвищення рівня ефективності бездротових мереж дозволить значно збільшити кількості передаваних даних до абонентського пристрою, що виведе якість застосунків, які використовують VR/AR/MR та Ultra HD, на новий рівень. Це призведе до збільшення використання цих технологій у сферах навчання, охорони здоров'я, муніципальної інфраструктури та розважального сектору. Як наслідок стануть потрібними нові застосунки/програми/рішення, що будуть створювати новий користувацький досвід з урахуванням всіх переваг нового стандарту.

Список використаних джерел

1.Evgeny Khorov, Anton Kiryanov, and Andrey Lyakhov. IEEE 802.11 ax: How to Build High Efficiency WLANs. -- [14-19 с.]

МУЛЬТИКАМЕРНИЙ МОНТАЖ ЗА ДОПОМОГОЮ ПРОГРАМИ ADOBE PREMIERE PRO

*Кас'яненко Ігор Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Що таке мультикамерного монтаж? Це один з монтажних режимів програми Adobe Premiere, що дозволяє нам переносити відео в фільм з декількох джерел (в нашому випадку джерела - це доріжки з кліпами). Тобто ми можемо одночасно переглядати відео з декількох доріжок (максимум з 4-х), і,

перемикаючись між ними, вибрати з якою з доріжок відео потрапить в кінцевий фільм.

Оскільки даний метод більш слід розглядати на практиці а не в теорії, то від себе підмічу деякі позитивні та негативні моменти на мій погляд даного методу. Проте даний метод я не використовував жодного разу, оскільки зйомка на декілька камер одночасно велась тільки в деяких проектах або невеликий проміжок часу(наприклад реклама або відео кліп).

На мою думку метод мультикамерного монтажу дуже зручний для максимальної якості підбору ключових кадрів у відео, проте має багато деяких пунктів які слід виконати до роботи з даною функцією, наприклад:

➤ синхронізація всіх відрізків які зняті в один і той самий проміжок реального часу;

➤ чітка послідовність дій як і при звичайному монтажі відео, а саме:

1) пошук матеріалу для монтажу;

2) перегляд матеріалу та видалення поганих дублів, лишнього матеріалу та т.д.;

3) перенесення матеріалу в програму;

4) послідовне(стосовно хронометражу, ідеї чи інших аспектів) перенесення відео матеріалу на timeline програми;

5) створення «блочної» структури матеріалу(наприклад різні історії в відео чи зміна музики це різні блоки, також зміна локації, пори року чи якщо пройшов певний час);

6) «нарізка» матеріалу та формування з нього чернеткову версію вихідного відео;

7) додавання на відео готові «футажі»(не дуже важкі для системи);

8) Sound Design(робота з музикою, звуковими ефектами та т.д.);

9) «футажі», плашки, вставки, картинки та інше вставляємо на потрібні місця;

10) робота з текстами, плашками та іншими візуалами чи графікою;

11) переглядаємо що вийшло та підкоректовуємо якщо потрібно;

12) маркування відео фрагментів для різної корекції кольорів(не завжди потрібно);

13) корекція кольорів;

14) добавляємо всі відео переходи між потрібними сценами чи кадрами;

15) переглядаємо кінцеву версію;

16) рендер;

Дуже важливо підмітити що якщо проблеми з текстами виникають після корекції кольорів то слід прибрати її саме з графіки(часто буває текст по краям дуже різкий та строгий). Також дуже важливо робити корекцію кольорів до пункту №14, оскільки більшість переходів які використовують у відео(наприклад здвиги камери, віддалення чи вліт камери) дуже навантажують і без того систему, а також зазвичай використовують білі кольори при розмиванні картини всередині переходу з яких саме витягувалась інформація для покращення картини при корекції кольорів, що може призвести в кращому

випадку до підвисань та не можливості показати той відрізок часу де перехід більше ніж в 5 кадрів в секунду а в самому гіршому-вильоту та поломки проекту з всією роботою остаточно і не працювання його на далі, роблячи всю роботу заново.

Позитивні:

- економія часу(приблизно на 50-70%);
- можливість вибирати саме потрібний кадр на певному відрізку часу;
- підходить для будь яких задач, як і на професійному рівні(кінофільми, телешоу, прямі ефіри, новини, відео кліпи та т.д.) так і для домашнього використання;
- можливість відтворення всіх 4-х відео доріжок одночасно(велике навантаження на систему);

Негативні:

- велике навантаження на систему яке помножується на кількість відеодоріжок які використовуються в даній функції одночасно;
- краще мати великий екран;
- в більшості випадків слід використовувати проксі сервер(можливість проводити монтаж відео через сервер маючи високу швидкість інтернету);
- якщо відео не синхронізовано за часом чи аудіо то слід буде зробити це;
- при монтажі більше ніж на 4 камери слід буде створювати окремі «секвенції»;
- при корекції кольорів слід докладніше дізнатися як це зробити правильно;
- можливі «вильоти» програми із-за навантажень;

Список використаної літератури:

1. Мультикамерний монтаж в Premiere Pro URL: <https://videomile.ru/lessons/read/multikamerniy-montaj.html> (дата звертання 18.03.2021)

WI-FI 6 – ВАЖЛИВИЙ КРОК У БЕЗДРОТОВЕ МАЙБУТНЄ

*Щербина Анастасія Олегівна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Наступним поколінням стандарту Wi-Fi є Wi-Fi 6, також відомий як 802.11ax, останній крок у подорожі безперервних інновацій. Стандарт ґрунтується на сильних сторонах 802.11ac, одночасно додаючи ефективність, гнучкість та масштабованість, що дозволяє новим та існуючим мережам збільшити швидкість та пропускну здатність у додатках наступного покоління.

Інститут інженерів електрики та електроніки (IEEE) запропонував стандарт Wi-Fi 6, щоб він міг поєднати свободу та високу швидкість бездротового зв'язку Gigabit Ethernet із надійністю та передбачуваністю, що містяться в ліцензованій радіостанції.

Різниця Wi-Fi 6 від 802.11ax

Ні, вони однакові. Wi-Fi Alliance розпочав кампанію, щоб ввести термін "Wi-Fi 6", маючи на увазі стандарт IEEE 802.11ax. Це вказує на те, що це шосте покоління Wi-Fi. Передумовою було спрощення маркетингового повідомлення, щоб допомогти 802.11ax краще позиціонуватись у порівнянні зі стандартами Проекту партнерства третього покоління (3GPP), що використовуються у стільниковій мережі (наприклад, 5G).

Коли буде затверджено Wi-Fi 6?

В даний час Асоціація стандартів IEEE планує ратифікувати остаточну поправку IEEE Wi-Fi 6 в середині 2020 року. Однак, як очікується, Wi-Fi Alliance сертифікує ключові особливості цієї поправки приблизно в серпні 2019 року з додатковими функціями (зокрема роботи в діапазоні 6 ГГц), сертифікованих протягом наступних кількох років.

Переваги Wi-Fi 6

Wi-Fi 6 дозволяє підприємствам та постачальникам послуг підтримувати нові та нові програми на одній і тій же інфраструктурі бездротової локальної мережі (WLAN), одночасно надаючи вищий рівень обслуговування старим програмам. Цей сценарій створює основу для нових бізнес-моделей та розширення впровадження Wi-Fi.

Wi-Fi 6 буде спиратися на успіх 802.11ac. Це дозволить точкам доступу підтримувати більше клієнтів у щільному середовищі та забезпечить кращий досвід для типових мереж бездротової локальної мережі. Це також забезпечить більш передбачувану продуктивність для передових додатків, таких як відео 4K або 8K, додатки для спільної роботи високої щільності з високою роздільною здатністю, бездротові офіси та Інтернет речей. Wi-Fi 6 буде рухати Wi-Fi у майбутньому, оскільки зростання бездротового зв'язку триватиме.

Дивіться нашу технічну довідку: IEEE 802.11ax: Шосте покоління Wi-Fi

Точки доступу Wi-Fi 6

На ринку вже є кілька точок доступу Wi-Fi 6, орієнтованих на тих, хто впроваджує програму та споживачів, які хочуть протестувати новий стандарт. Точки доступу, які звільняються достроково, будуть попередньо стандартними точками доступу, оскільки стандарт ще не був ратифікований. Це означає, що ключові функції, які є частиною Wi-Fi 6, можуть не підтримуватися в деяких із цих початкових, стандартних точок доступу. Однак, коли вони будуть доступні, деякі з цих точок доступу зможуть пройти сертифікацію за допомогою оновлень програмного забезпечення та підтримуватимуться функції Wi-Fi 6. Цей підхід подібний до впровадження попередніх поколінь, таких як 802.11ac та 802.11n. Готові жити бездротові програми нового покоління? Почніть із нашого набору ресурсів Wi-Fi 6.

Розміри технології Wi-Fi 6

Більш щільна модуляція з використанням 1024 квадратурно-амплітудної модуляції (QAM), що забезпечує більш ніж 35-відсотковий пакет швидкості.

Планування на основі ортогонального частотного розподілу частот (OFDMA) для зменшення накладних витрат і затримок.

Надійна високоефективна сигналізація для кращої роботи при значно нижчому показнику інтенсивності отриманого сигналу (RSSI).

Краще планування та довший час автономної роботи пристрою завдяки цільовому часу пробудження (TWT)

Список використаної літератури:

1. What is WIFI 6 // <https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-6.html>

ОСОБЛИВОСТІ ВИКОРИСТАННЯ АВТОКОДУВАЛЬНИКІВ ДЛЯ ЗНИЖЕННЯ РОЗМІРНОСТІ ДАНИХ

Цапро І.В

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

Автокодувальники (autoencoders) - це нейронні мережі, які відновлюють вхідний сигнал на виході мережі. У середині мережі розміщується прихований шар, який представляє собою набір параметрів, що описує модель. Автокодувальники створюються таким чином, щоб не мати можливості точно скопіювати вхідний сигнал на виході. Зазвичай їх обмежують у розмірах параметрів або штрафують активаційними функціями. Вхідний сигнал відновлюється з помилками через втрати при кодуванні, але, щоб їх мінімізувати, мережа змушена вчитися відбирати найбільш важливі ознаки.

Автокодувальники складаються з двох частин: кодувальника g та декодувальника f . Кодувальник трансформує вхідний сигнал в його просторове уявлення: $h = g(x)$, а декодувальник відновлює сигнал по просторовому уявленню: $x = f(h)$.

Автокодувальник, змінюючи f і g , прагне вивчити тотожну функцію $x = f(g(x))$, мінімізуючи похибку (функція витрат). При цьому сімейства функцій кодувальника g та декодувальника f якимось обмежені, щоб автокодувальник був змушений відбирати найбільш важливі властивості сигналу.

Автокодувальники можна використовувати для переднавчання, наприклад, коли стоїть завдання класифікації, а розмічених пар занадто мало. Або для зниження розмірності в даних для подальшої візуалізації. Або в якості складової частини архітектур більш складних нейронних мереж [1]. Або коли просто треба навчитися розрізняти корисні властивості вхідного сигналу.

Сама по собі здатність автокодувальників стискати дані використовується рідко, так як зазвичай вони працюють гірше, ніж вручну написані алгоритми для конкретних типів даних на зразок звуків або зображень. Однак автокодувальники широко використовуються у сферах, де надзвичайно складно або майже неможливо створити спеціалізований алгоритм стискання даних.

Також добре навчений автокодувальник здатний перевершити метод головних компонент (РСА) у стисканні структурованих та неструктурованих даних [2] та зменшення кількості мультиколінеарних факторів.

Отже, автокодувальники можна використовувати як допоміжний інструмент для підвищення точності алгоритмів навчання з учителем шляхом впровадження векторів просторового уявлення даних додатково до навчальної вибірки. Особливість використання даного алгоритму, в контексті цієї задачі, потребує детального розуміння представленої до рішення проблеми. Наприклад, при роботі з часовими рядами, потрібно формувати навчальну вибірку та будувати архітектуру автокодувальника таким чином, щоб змусити нейронну мережу шукати найбільш важливі властивості сигналу в контексті змін у часі. Тобто використовувати рекурентні шари або механізми уваги [3]. Також можна сформуванати для алгоритму додаткову задачу прогнозування наступного значення часового ряду, щоб похибка від прогнозного та реального значення впливала на мінімізацію загальної функції витрат.

Особливості використання автокодувальників чітко залежать від поставленої задачі. Тому застосування даного алгоритму може значно допомогти у рішенні задач, де неможливо або недоцільно використовувати класичні методи стискання даних.

ЛІТЕРАТУРА

1. Ian Goodfellow, Yoshua Bengio, Aaron Courville. DeepLearninBoook – P. 499 – 523.
2. G. E. Hinton, R. R. Salakhutdinov. Reducing the Dimensionality of Data with Neural Networks (англ.)// Science. — 2006-07-28. — Vol. 313, iss. 5786. — P. 504-507. — ISSN 1095-9203 0036-8075, 1095-9203. — doi:10.1126/science.1127647.
3. Vaswani, Ashish; Shazeer, Noam; Parmar, Niki; Uszkoreit, Jakob; Llion, Gomez, Aidan N.; Kaiser, Lukasz; Polosukhin, Illia (2017-12-05). "Attention Is All You Need". [arXiv:1706.03762](https://arxiv.org/abs/1706.03762) [cs.CL]

РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В КОНЦЕПЦІЇ ДИСТАНЦІЙНОГО НАВЧАННЯ

*Андрієнко Олеся Григорівна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Інформаційні технології відкрили для людей нові горизонти - не лише в роботі, але й в освіті. Швидкий розвиток інформаційно-телекомунікаційних технологій поступово визначає перехід від постіндустріального суспільства до інформаційного. Інформаційне суспільство визначає елементи виробництва та розповсюдження інформації як основу економічного розвитку, а не як виробництво товарів та послуг.

З розвитком інформаційно-комунікаційних технологій взаємодія людини вимагає все менше спілкування в режимі реального часу. Виділяються комунікації, послуги зв'язку та відео-конференції в соціальних мережах. За допомогою сучасних інформаційно-комунікаційних технологій дистанційне

навчання може забезпечити низку освітніх послуг для широких мас, незалежно від того, де вони знаходиться.

Інформаційно-комунікаційні технології (ІКТ) є важливою складовою сучасного освітнього процесу. ІКТ - це різноманітне обладнання та методи обробки інформації, насамперед комп'ютери з необхідним програмним забезпеченням та засоби зв'язку з інформацією. Вони дозволяють віддалену взаємодію між викладачами та студентами, іншими словами, дистанційну освіту.

Дистанційні технології в освіті значно розширили її можливості. У сучасному світі ми можемо отримати освіту з будь-якої точки планети. Хоча традиційна форма навчання не втрачена, останнім часом технологія дистанційного навчання стає все більш популярною.

В Україні дистанційне навчання успішно застосовується у вищих навчальних закладах. Але в зв'язку з останніми подіями така форма навчання застосовується не лише у ВНЗ, а й у школах.

Дистанційне навчання є більш широким поняттям, ніж електронне навчання, це поєднання інтерактивного самонавчання та інтенсивних консультацій. Тому електронне навчання можна розглядати як інструмент дистанційної освіти. Дистанційне навчання - це сукупність технологій, які можуть забезпечити студентів великою кількістю навчальних матеріалів та дозволити студентам взаємодіяти з викладачами під час навчального процесу. У цьому випадку посібник може бути доставлений без участі комп'ютерів та Інтернету.

Розглянемо переваги дистанційного навчання:

- можливість навчання за місцем проживання;
- можливості органічно поєднати роботу та навчання;
- доступ до високоякісних технологій та освітнього контенту;
- об'єктивність атестаційного процесу;
- персоналізовані методи навчання, гнучкі графіки, поєднані з можливістю вчитися та працювати.

Дистанційна освіта вважається ефективною, завдяки її інтерактивності, особливостям задіяних інформаційних технологій, персонального планування навчального процесу.

Останні розробки в галузі ІКТ можуть і повинні використовуватися для організації дистанційного навчання. Для того, щоб зрозуміти, яка технологія використовується, необхідно визначити основний спосіб і форму постачання матеріалу.

Існує кілька традиційних форм подачі та контролю матеріалів, яким потрібно знайти еквівалентні форми:

- навчальний посібник;
- лекція;
- семінар;
- модульний контроль;
- екзамен.

Необхідно розглянути технології, що дозволяють віддалено представляти кожен з цих форм по черзі. Звичайно, у дистанційній освіті ще є місце для класичних підручників. Очевидно, що вони повинні подавати їх в електронній формі, оскільки це збільшує доступність для всіх студентів. Електронні підручники можна розмішувати на веб-сайті школи або на FTP-сервері.

Застосування дистанційного навчання широко використовується у всьому світі і зарекомендувало себе найкращими способами. Ефективність дистанційного навчання підтверджена неодноразовим використанням студентами університетів та працівниками комерційних підприємств. І наразі є доволі вагомі причини застосування даної форми навчання.

Інформаційно-комунікаційні технології досить швидко розвиваються і відіграють важливу роль у ефективності сучасних методів дистанційного навчання. Наявність глобальної мережі Інтернет та всюдидоступність мобільних пристроїв в Інтернеті дозволяють організовувати дистанційне навчання практично в будь-якій точці світу. Розвиток інформаційних технологій також вплинув на технології дистанційного навчання, зробивши їх інтерактивними та покращивши їх ефективність.

Дистанційні технології сприяють створенню одного освітнього простору в рамках індивідуалізації освіти з масою вищої освіти. Розвиток інформаційних технологій у сучасному світі призвів до перегляду традиційних підходів до виявлення перспективних форм організації навчального процесу.

Список використаних джерел:

1. Гурін Р.С. *Методика впровадження нових інформаційних технологій у навчальний процес. Навч. посібник / Р.С. Гурін // – Одеса: ПДПУ імені К.Д.Ушинського, – 2002 р. – 57 с.*
2. Дичківська І. М. *Інноваційні педагогічні технології / І. М. Дичківська // – К.: Академвидав, 2004. – 352 с.*
3. Кухаренко В.М. *Дистанційне навчання та умови застосування / В.М.Кухаренко, О.В. Рибалко, Н.Г. Сиротенко // Харків, 2002. – 320 с.*

ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ІР-ТЕЛЕФОНІЇ НА БАЗІ ДИФЕРЕНЦІЙНОГО ОБСЛУГОВУВАННЯ

Кулик М.С.

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Технологія забезпечення QOS розроблена робочою групою IETF по диференційованому обслуговуванню (Differentiated Services, DiffServ). Ця група виділилася з робочої групи по інтегрованому обслуговуванню (Integrated Services, IntServ), завдання якої полягає в розробці стандартів для підтримки трафіку Internet реального часу.

Робота, що проводиться в рамках IntServ відображає деякі з особливостей концепції RSVP. Інтегроване обслуговування передбачає сигналізацію з кінця в кінець і насправді використовує RSVP між відправниками і одержувачами.

IntServ визначає три класи обслуговування для IP-мереж: в міру можливості - те, що зараз пропонує Internet; з контрольованою завантаженістю - додаток отримує той рівень обслуговування, який він мав би у слабо завантаженої мережі; з гарантованим обслуговуванням - необхідна пропускна спроможність протягом всього сеансу надається з гарантією на параметри якості обслуговування.

Як і RSVP, інтегроване обслуговування має проблеми з масштабуванням, тому дана технологія навряд чи проб'ється за межі корпоративних мереж. І, як було відмічено, RSVP передбачає значні накладні витрати, оскільки кожен вузол впродовж шляху слідування пакетів повинен погодитися надати запрошену якість послуг [1,с.231].

Диференційоване обслуговування пропонує більш простий і масштабований метод QOS для додатків реального часу. Одним з ключових моментів в роботі над DiffServ є перевизначення 8-бітового поля «Тип сервісу» в заголовку IPv4. Назване «Диференційованим обслуговуванням» (DS), це поле може містити інформацію, на підставі якої вузли вздовж маршруту визначають, як їм слід обробляти пакети і передавати їх наступному маршрутизатору.

В даний час лише 6 з 8 біт в полі DS були визначені, і лише одне призначення було стандартизовано. Це призначення відоме як прийняте за замовчуванням - Default (DE) - і воно визначає клас обслуговування в міру можливості. Інше передбачуване призначення, термінова відправка (Expedited Forwarding, EF), повинні забезпечити скорочення затримок і втрат пакетів.

Під час вступу трафіку в мережу краєвий маршрутизатор класифікує графік відповідно до інформації, що міститься в полі DS. Він передає наступним за ним маршрутизаторам цю інформацію, на підставі якої вони дізнаються, яким чином обробляти даний конкретний потік.

DiffServ, крім того, скорочує службовий трафік в порівнянні з RSVP і IntServ, що спираються на сигналізацію з кінця в кінець. DiffServ класифікує потоки відповідно до зумовлених правил і потім об'єднує однотипні потоки. Подібний механізм робить DiffServ набагато більш масштабованим, ніж його попередника IntServ. Весь трафік з однаковими мітками розглядається однаковим чином, тому реалізація DiffServ в мережі крупного підприємства або по каналах глобальної мережі виявляється реальнішим завданням [2,с.142].

Як можна здогадатися, переваги DiffServ не можна отримати автоматично. Маршрутизатори повинні розуміти «мічені потоки» і вміти відповідним чином реагувати на них. Це вимагатиме модернізації мікропрограмного забезпечення маршрутизаторів.

Список використаних джерел;

1. Оліфер В.Г. Комп'ютерні мережі. Принципи, технології, протоколи, четверте видання. Підручник для ВНЗ / В.Г.Оліфер, Н.А.Оліфер – СПб: Пітер, 2015. – 944 с.
2. Полканов Є.І. Інтелектуальні мережі і комп'ютерна телефонія / Є.І.Полканов, М.А.Шнепс-Шнеппе, С.В.Крестьяников – М.: Радіо і зв'язок, 2018 – 240 с.

ДОСЛІДЖЕННЯ ПРИНЦИПІВ РОБОТИ SSH-ТУНЕЛЮ

Аніщенко Крістіна Ярославівна
Навчально-науковий інститут телекомунікацій
Державний університет телекомунікацій

SSH є технологією, яка призначена для віддаленого виконання команд, а також для входу через мережу на інший комп'ютер. Використовуючи SSH можна завантажувати і копіювати файли між комп'ютерами, але частіше за все вона використовується для безпечної передачі файлів сайту між вашим комп'ютером і сервером хостинг-провайдера. Secure Shell - так розшифровується аббревіатура SSH. Завдяки використанню цієї технології досягається надійна авторизація та безпечна передача інформації по відкритих каналах зв'язку [1,с.211].

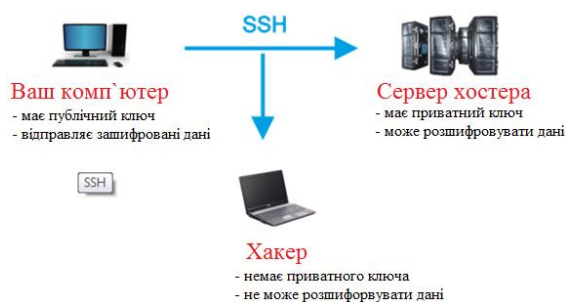


Рис. 1. Схема організації передачі даних з використанням технології SSH

SSH-тунелі створюються для вирішення 2-х незалежних завдань:

1. Забезпечення конфіденційності даних, що передаються по захищеному каналу
2. Створення сполучного мосту (або декількох мостів) між клієнтом і сервером через проміжні комп'ютери, так як клієнт може не мати прямого доступу до сервера. В цьому випадку конфіденційність є другорядною або зовсім не потрібно.

SSH-тунелі можуть бути організовані як в режимі перенаправлення окремих TCP-портів (Port forwarding), так і в режимі справжніх VPN-тунелів через віртуальні інтерфейси, коли передаватися може трафік будь-яких протоколів і з будь-яких портів. У даному розділі мною було розглянуто перший режим [2,с. 47-49].

При роботі в режимі Port Forwarding пакет, що надходить на вхідний порт тунелю, повинен бути переданий в незмінному вигляді на його вихідний порт. Така схема застосовується в роботі інтернет-шлюзів: пакети з одного інтерфейсу передаються на інший без зміни і аналізу.

Таким чином, SSH-канал в цьому режимі з усією його інфраструктурою нагадує віртуальний шлюз з вхідним і вихідним інтерфейсами, але тільки за конкретною парі TCP-портів:

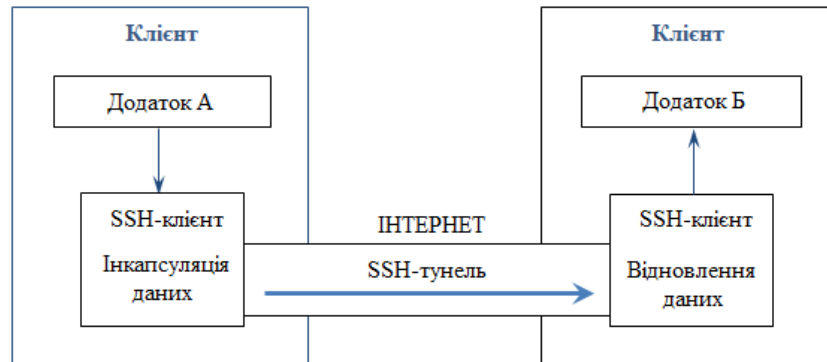


Рис.2. Схема організації з'єднання клієнт/сервер

Стрілкою зазначений напрямок ініціювання SSH-сесії. В даному випадку ініціатором з'єднання виступає Клієнт з встановленим на ньому PuTTY. Наведена вище схема є базовою, в якій взаємодіють лише 2 учасника клієнт і сервер. На практиці ж між клієнтом і сервером може бути кілька проміжних хостів. І до потрапляння на вхід конкретного тунелю і після виходу з нього пакети можуть передаватися по незахищених каналах. Для встановлення зв'язку з SSH-протоколу буде потрібен обліковий запис на SSH-сервері, яка може бути будь-який, в тому числі без яких би то не було прав і навіть без шелла, якщо ви відкриваєте на прослуховування порти від 1024 і вище. В іншому випадку необхідний рутовий доступ і значення директиви PermitRootLogin рівне yes або without-password.

Перелік використаної літератури:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – 2011. – 668 с.
2. Никитин А.В., Пяттаев В.О., Никульский И.Е., Филиппов А. А. Концепция построения мультисервисной сети оператора связи. //Вестник связи. 2015 №5. - с. 47-49.

МЕХАНІЗМИ ПЕРЕХОДУ НА IPV6

Коновал А.С.

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Механізм переходу являє собою технологію, яка забезпечує міграцію з IPv4 на IPv6. Оскільки IPv4 та IPv6 не можуть напряму взаємодіяти, технологія переходу призначена вирішити цю проблему і дозволити хостам взаємодіяти один з одним. Деякі основні механізми тунелювання визначенні в RFC 4213.

Розглянемо наступні методи:

- Stateless IP/ICMP Translation
 - Тунельний брокер
 - NAT64
 - DNS64
 - 6PE/6VPE
 - 6to4
 - Ipv6 rapid deployment
- Stateless IP / ICMP Translation

здійснює перетворення між форматами заголовка пакета в IPv6 і IPv4. Метод SIIT визначає клас адрес IPv6 називається IPv4, перекладені адреси. Вони мають префікс `::FFFF::0/96`, і може бути записана у вигляді `:: FFFF:0: ABCD`, в якому IPv4 - адреса, відформатований ABCD відноситься до IPv6 з підтримкою вузла. Префікс був обраний для отримання нульового значення контрольної суми змін, щоб уникнути контрольної сумі заголовка транспортного протоколу. Алгоритм може бути використаний в розчині, що дозволяє господарям IPv6, які не мають постійно призначений адресу IPv4 для зв'язку з IPv4-тільки хостів. Призначення адрес і деталь маршрутизації не розглядаються в специфікації. SIIT можна розглядати як окремий випадок особи без трансляції мережевих адрес.

Специфікація є продуктом робочої групи NGTRANS IETF, і був спочатку розроблений в лютому 2000 року E. Nordmark з Sun Microsystems. Він був переглянутий в 2011 році, а в 2016 році була опублікована його нинішня редакція.

Тунельний брокер

Тунельний брокер забезпечує підключення по протоколу IPv6 шляхом інкапсуляції трафіку IPv6 в транзитних Інтернет посилення IPv4, як правило, з використанням бін4. Це встановлює тунелі IPv6 в IPv4 інтернет. Тунелі можуть управлятися за допомогою протоколу настройки тунелю (TSP) або AYIYA.

NAT64

NAT64 являє собою механізм, щоб вузли IPv6 взаємодіяли з серверами IPv4. Сервер NAT64 є кінцевою точкою, щонайменше, одну адресу IPv4 і IPv6 - сегмент мережі з 32 бітів, наприклад, `64: ff9b :: / 96` (RFC 6052 , RFC 6146). Клієнт IPv6 вбудовує адресу IPv4, з яким він хоче спілкуватися за допомогою цих біт, і посилає свої пакети до отриманого адресу. Потім сервер NAT64 створює NAT - відображення між IPv6 і IPv4 - адреса, що дозволяє їм спілкуватися.

DNS64

DNS64 описує DNS сервер , що при запиті домену AAAA записи , але знаходить лише A записи , синтезує AAAA записи із записів A. Перша частина синтезованих точок IPv6 - адреси з перекладачем IPv6 / IPv4 і другою частиною вбудовує адресу IPv4 із запису A. Перекладач в питанні , як правило, сервер NAT64. Специфікація стандартної доріжки DNS64 в RFC 6147.

Є два помітні проблеми з цим механізмом переходу:

Він працює тільки в тих випадках, коли DNS використовується, щоб знайти адресу віддаленого хоста, якщо IPv4 літералов використовується сервер DNS64 ніколи не братиме участі.

Оскільки сервер DNS64 повинен повертати записи, які не вказані власником домену, DNSSEC перевірка проти кореня зазнає невдачі в тих випадках, коли DNS - сервер робить переказ не сервер власника домену.

6PE / 6VPE

Технологія використовується тими провайдерами, які вже використовують MPLS на своїй IPv4-мережі, для того, щоб здійснити зв'язність між IPv6-хостами. На мережі провайдера, крім звичайних IPv4-MPLS-PE-

маршрутизаторів, заводяться 6PE / 6VPE-маршрутизатори. Основне їхнє завдання - здійснювати пропуск трафіку через існуючі IPv4 MPLS LSP. Кожен такий маршрутизатор встановлює відповідність IPv6-адресами IPv4-напрямки, і здійснює маршрутизацію пакетів. Таким чином, не виникає необхідності впроваджувати складні технології MPLS, використовуючи IPv6-механізми, для надання сервісу клієнтам, які вже працюють по IPv6. Це дозволить витримати конкуренцію на ринку, маючи мінімальні витрати на модернізацію мережі. Ця технологія не вирішує проблему переходу до IPv6-адресації, а дозволяє IPv6-хостів спілкуватися через IPv4 mpls-мережу.

6to4

Технологія пропуску IPv6-трафіку через IPv4-мережа дозволяє IPv6-клієнтським пристроїв і додатків отримувати послуги доступу до IPv6-хостів, через IPv4-мережу провайдера послуг.

Мабуть, найпростіший спосіб отримання зв'язності між IPv6-хостами через IPv4-мережу. Для цього від провайдера послуг не потрібно робити нічого додаткового на мережі. Єдиною умовою для роботи технології є наявність у клієнта статичного публічного IPv4-адреси.

Технологія використовує спеціальні пристрої, які називаються 6to4 relay. Ці пристрої деінкапсулюють клієнтські IPv6-пакети з IPv4, і передають їх далі по мережі до необхідного IPv6-призначення. Вони можуть розташовуватися де завгодно на просторах Інтернет. Даний функціонал може використовуватися як окремим пристроєм, так і відразу в підмережі з декількох пристроїв.

Технологія не дозволяє здійснювати комунікації між "чистим" IPv4 і IPv6-пристроєм, як це робить NAT64, а також не вирішує проблеми закінчення IPv4-адресного простору. Це просто механізм спілкування IPv6-пристроїв через IPv4-мережу. (2)

IPv6 rapid deployment

Дана технологія необхідна тим, хто хоче надавати послуги IPv6 через мережу, засновану на IPv4. Технологія 6rd використовує принцип тунелювання IPv6-пакетів через IPv4, а також дозволяє обійти деякі обмеження 6to4.

Основна відмінність від технології 6to4 полягає в тому, що IPv6-адреси виділяються з підмережі, яка закріплена за провайдером інтернет-послуг, а також всі 6to4 relay-пристрої, знаходяться під управлінням провайдера інтернет-послуг. Таким чином, вирішується проблема технології 6to4 – недосяжність деяких 6to4-хостів, в силу відсутності маршрутної інформації до цих хостів у звичайних IPv6-пристроїв. Необхідно відзначити, що дана технологія не вирішує проблему нестачі IPv4-адрес, а тільки дозволяє використовувати послуги IPv6 через IPv4-мережу.

Література:

1. А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. Комп'ютерні мережі. Львів : Магнолія, 2006.
2. Bagnulo, M. RFC 6146. RFC. April 2011 p. <https://tools.ietf.org/html/rfc6146>.
3. Bao, C. RFC 6052. RFC. October 2010 p. <https://tools.ietf.org/html/rfc6052>.
4. Bagnulo, M. RFC 6147. RFC. April 2011 p. <https://tools.ietf.org/html/rfc6147>
5. Nordmark, E. RFC 4213. RFC. October 2005 p. <https://tools.ietf.org/html/rfc4213>

ОСОБЛИВОСТІ ВЗАЄМОДІЇ ДЕКІЛЬКОХ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ

Виговський Олександр Сергійович

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

За замовчуванням кожен протокол маршрутизації, що працює на певному маршрутизаторі, поширює лише "власну" інформацію, тобто інформацію, яку маршрутизатор отримує від цього протоколу. Наприклад, якщо маршрутизатор дізнається маршрут мережі через RIP, він буде використовувати RIP для реклами маршруту в мережі.

Однак такий спосіб роботи маршрутизатора встановлює невидимий бар'єр для поширення інформації про маршрутизацію і є взаємно недосяжний. Область мережі. Якщо маршрутизатори можуть обмінюватися інформацією про маршрутизацію, отриманою за допомогою різних протоколів маршрутизації, завдання маршрутизації буде більш ефективним. Ця функція реалізована в спеціальному режимі роботи маршрутизатора, який називається перерозподілом. Цей режим дозволяє протоколу маршрутизації використовувати не тільки "свою" маршрутизацію, але і "зовнішні" записи таблиці маршрутизації, отримані за допомогою іншого протоколу маршрутизації, зазначеного в конфігурації.

Маршрутизатори можуть перерозподіляти статичні та безпосередньо пов'язані маршрути та маршрути з інших протоколів маршрутизації. Перерозподіл завжди здійснюється зовні. Перерозподілений маршрутизатор ніколи не змінює таблицю маршрутизації. При перерозподілі між OSPF та EIGRP, процес OSPF на крайовому маршрутизаторі витягує маршрути EIGRP із таблиці маршрутизації та розподіляє їх сусідам OSPF. Подібним чином процес EIGRP на прикордонному маршрутизаторі отримує маршрути OSPF з таблиці маршрутизації та розподіляє їх сусідам EIGRP. Тоді обидві автономні системи знають маршрут іншої системи, і кожна автономна система може визначити маршрут у цій мережі. Крім того, найбільша складність полягає в координації використання різних метрик для різних протоколів в його алгоритмі маршрутизації.

Коли маршрутизатор рекламує підключення до одного зі своїх інтерфейсів, початкова метрика називається метрикою за замовчуванням, і це залежить від характеристик інтерфейсу: для OSPF метрика за замовчуванням базується на пропускній здатності інтерфейсу, для EIGRP, пропускній здатності та затримці. Для RIP показник за замовчуванням починається з лічильника перехоплення 0 і збільшується з маршрутизаторами. Потрібно використовувати інші протоколи для вивчення перерозподілених маршрутів, які фізично не підключені до маршрутизатора. Тому важко перетворити з одного показника на інший: з числа прийомів на пропускну здатність. Якщо прикордонний маршрутизатор перерозподіляє інформацію між протоколами маршрутизації, він повинен мати можливість перетворити метрики одного протоколу в метрики іншого протоколу.

Команда `default-metric`, що використовується в режимі конфігурації протоколу маршрутизації, встановлює метрику за замовчуванням для всіх перерозподілених маршрутів. Маршрутизатори Cisco дозволяють встановити метрику за замовчуванням у команді перерозподілу або в параметрі карти метричної маршруту. Але тут повинна бути виконана важлива умова: незалежно від того, який метод ми вибрали для встановлення метрики за замовчуванням, її значення повинно бути більшим за максимальне значення метрики в незалежній системі, щоб запобігти неоптимальним циклам маршрутизації та маршрутизації.

Якщо маршрутизатор отримує інформацію про одного і того ж одержувача або мережу одержувачів з різних джерел, він повинен якимось чином обрати маршрут для розміщення в таблиці. Для цього використовується адміністративна дистанція.

Administrative distance (AD) - це номер, присвоєний кожному можливому джерелу шляху, що є ступенем довіри до джерела. Таблиця маршрутизації буде містити маршрути з джерела з найменшим значенням AD. Адміністративна відстань має лише місцеве значення і не впливатиме на прийняття рішень іншими маршрутизаторами.

Вивчати роботу та налаштування функцій маршрутизаторів, які можуть одночасно працювати на декількох протоколах маршрутизації, можна за допомогою практичної програми CiscoPacketTracer. PacketTracer - це інтегроване, сумісне та візуальне середовище для початківців мережевих адміністраторів, які призначені для вивчення навичок проектування, налаштування та налагодження комп'ютерних мереж.

Отже, за допомогою цієї програми ми можемо збирати різні схеми та налаштовувати різні протоколи маршрутизації на маршрутизаторі.

Література:

4. Мазур А.С., Овчинников А. Л. Исследование Методов Маршрутизации. [Електронний ресурс]. – Режим доступу: <http://ea.donntu.edu.ua>.
5. Остерлох Х. Маршрутизация в IP-сетях. Принципы, протоколы, настройка; пер. с англ. СПб: ООО "ДиаСофтЮП", 2002. – 512 с.
6. Полукаров Д. Ю. Методы IP-маршрутизации на основе алгоритмов с использованием нечетких множеств. – Самара, 2007. [Електронний ресурс].

ПОБУДОВА ZIGBEE МЕРЕЖІ НА ОСНОВІ ZIGBEE ШЛЮЗУ

Каграманова Юлія Костянтинівна

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

Zigbee – це технологія, яка заснована на радіо стандарті IEEE 802.15.4 і призначена для стандартизації малопотужних M2M пристроїв різних виробників. З особливостей мережі можна виділити високу відмовостійкість, тривалий термін служби кінцевих пристроїв від однієї батареї, підтримку великої кількості підключень і спільну роботу пристроїв різних виробників.

Шлюз призначений для роботи з пристроями ZigBee. В основі лежить контролер ESP32 від Espressif . Зв'язуюча ланка протоколу Zigbee виступає тандем чіпів від Texas Instruments Zigbee CC2538 і підсилювача cc2592.

Шлюз виконує роль координатора Zigbee і дозволяє:

1) Використовувати більшість доступного Zigbee обладнання. Є можливість додати нове обладнання через спілкування з розробниками.

2) Відмовитися від необхідності використання хмар виробників пристроїв. В якості альтернативи, пропонується використовувати хмарний сервіс Smart Logic System , або нативні додатки для Android і Apple iPhone (в розробці).

3) Використовувати поширені локальні системи автоматизації, такі як MajorDomo , ioBroker Smarthome , HomeAssistant , Node-Red і ін. Для інтеграції з цими системами використовується протокол MQTT. Структура топиків протоколу MQTT ідентична проекту zigbee2mqtt , тому для використання та інтеграції шлюзу немає необхідності вивчати скриптові мови зазначених вище систем, так як протокол в основному вже доступний за допомогою модулів розширення.

Додаткові можливості шлюзу через Web інтерфейс

Управління та перегляд відомостей пристроїв через Web інтерфейс шлюзу за адресою [http:// ipaddress \(80 порт\)](http://ipaddress(80 порт)). Можливість відображення джерела живлення, рівня заряду батареї, доступних EndPoint пристроїв в web-інтерфейсі.

Створення локальних автоматизацій всередині шлюзу SimpleBind.

Можливість написання сценаріїв на мові Lua.

Можливість створення груп для управління декількома пристроями одночасно (в розробці).

Можливість задавати ім'я пристрою. Якщо ви плануєте використовувати шлюз з локальними системами автоматизації, рекомендується встановити галочку відправки адреси замість пристроїв.

Можливість видалення пристрою.

Можливість відображення маршрутів в web-інтерфейсі (в розробці).

Можливість встановити прямі зв'язки Bind між пристроями ZigBee без участі координатора для управління кінцевими пристроями.

Можливість управляти апаратними світлодіодами (адресними або RGB) .

Можливість управляти звуком (при наявності розпаяного підсилювача) (в розробці)

Можливість змінити PanId і номер каналу.

Можливість задати ім'я шлюзу в мережі.

Можливість переходу шлюзу в режим AP при натисканні апаратної кнопки протягом 2-5 секунд після подачі живлення.

Протоколи з'єднання Zigbee пристроїв

SimpleBind дозволяє налаштувати локальні автоматизації всередині шлюзу.

Для установки необхідно зайти в властивість пристрою (пульта, кнопки, датчика) і на вкладці "States" навпроти "SB rule" прописати необхідний код.

Протоколом zigbee передбачено управління пристроями без координатора. Технологія TouchLink дозволяє створити окрему мережу zigbee між двома пристроями. Для зв'язку підтримують технологію пристроїв, необхідно ознайомитися з документацією. У магазинах Ікеа продаються комплекти ламп і пультів Tradfri, які підтримують таке сполучення. Зазвичай для сполучення лампи і пульта, необхідно піднести пульт до включеної лампочки і натиснути кнопку сполучення. Через якийсь час лампа почне моргати з наростаючою частотою. Через якийсь час моргання зупиниться, пристрої повинні будуть створити свою мережу.

Протокол Zigbee підтримує безпосередній прив'язку Endpoint пристроїв, яка дозволяє безпосередньо управляти один одним без втручання координатора або будь-якого програмного забезпечення для домашньої автоматизації.

Налаштування через Web

Необхідно через Web інтерфейс на вкладці zigbee зайти в керований пристрій (пульт) і вказати адресу і кінцевий Endpoint керованого пристрою.

Порядок дії наступний: 1) Заходимо на сторінку пульта або датчика, який буде прив'язуватися до пристрою 2) Вибираємо доступні кластери пристрої

Список використаних джерел

1. Zigbee 101: руководство для начинающих//<https://habr.com/ru/post/535658/>
2. Zigbee шлюз // https://slsys.github.io/Gateway/README_rus.html

ПОБУДОВА ZIGBEE МЕРЕЖІ НА ОСНОВІ ZIGBEE ШЛЮЗУ

Свердлюк Богдан Ігорович

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

Чи багато пристроїв Zigbee? Приблизно 2600 пристроїв (список сертифікованих пристроїв). Варто уточнити, що в більшості випадків кожен виробник має своє додатки для підключення тільки своїх пристроїв, але, використовуючи додаткове програмне забезпечення, їх можна подружити. Про це нижче.

Середня ціна одного кінцевого пристрою 10 \$.

Ось приклад кінцевих пристроїв декількох популярних виробників:

- Xiaomi Aqara - близько 50 пристроїв різного призначення.
- Philips Hue - близько 100 пристроїв, (більшість світильники),
- Ikea trådfri - близько 40 пристроїв (більшість світильники),
- Tuya - близько 30 пристроїв,
- SONOFF - близько 10 недорогих реле.

Zigbee USB пристрої (стики). Якщо ви використовуєте стороннє рішення, стик зручно використовувати як координатор мережі, підключивши до комп'ютера як роутер, щоб досягти віддалених від координатора місць.

Ось приклад декількох популярних пристроїв:

- cc2530 / 2531 - дешевий і популярний стик. Непоганий вибір для початківців. З мінусів: невеликий радіус покриття (10-15 м без антени) і обмеження по кількості пристроїв, що підключаються.
- cc2538 стик розроблений ентузіастами проекту modkam.ru. У порівнянні з 2531, має більший радіус дії і не має обмежень по кількості підключень (тести показали більше 200 пристроїв).
- deCONZ Conbeeстик також підтримує велику кількість систем розумного будинку. З мінусів рідної прошивки - іноді відвалюються кінцеві пристрої.
- Sprut.stick (в бета тестуванні) координатор від проекту Sprut.AI на основі модулів EFR32MG12 або MGM12P32F1024. Володіє відмінними характеристиками потужності, підтримує велику кількість пристроїв, також поступово додаються нові.

Також приклади менш популярних:

- nRF52840 Dongle - універсальний стик з підтримкою Bluetooth 5, Bluetooth mesh, Thread, ZigBee, 802.15.4 і ANT і зручним середовищем розробки.

Zigbee шлюзи. Xiaomi / Aqara три найпопулярніших пристрої - Xiaomi Gateway 2 і 3 версії і Aqara Hub. Gateway 2 несумісний з homekit і має 3 версію протоколу Zigbee. Третя версія має на борту Zigbee 3.0 і Bluetooth Mesh 5.0. З додатковими відмінностями допоможе розібратися короткий ролик .

SLS шлюз- Пристрій на основі CC2538 + CC2592 і ESP32-Wrover-B, а також прошивка. Підтримує Zigbee 3.0 і на відміну від Xiaomi він не обмежений однією екосистемою. А на відміну від стиків CC2531, CC2538 і Deconz - він є готовим пристроєм і може працювати як самостійно, так і в системі домашньої автоматизації Home Assistant. На даний момент підтримується 113 пристроїв . Відео огляд

ZESP32 - це прошивка для шлюзу Xiaomi Gateway. Точно так само як і SLS він розрахований на підключення Zigbee пристроїв різних виробників. Основна концепція - спрощення додавання нового пристрою в мережу за допомогою змінних шаблонів.

cc25xx + комп'ютер зручний варіант якщо у вас вже є raspberry pi, або старенький ПК, який буде виступати в ролі сервера. В цьому випадку ви можете вибрати будь-яку зручну систему домашньої автоматизації, про які нижче.

Що по екосистемах?

Apple home - програмне рішення від Apple. Кількість підтримуваних пристроїв невелика, але функціонал можна розширити за допомогою homebridge і aqara hub. Ви можете використовувати Apple home в домашній мережі використовуючи тільки iPhone і хаб (Zigbee), але для віддаленого управління потрібен домашній центр в ролі якого можуть виступати iPad (iOS 10 або вище), HomePod, або Apple TV.

Google home - також не працює з Zigbee пристроями безпосередньо, але має сумісність з Alexa.

Amazon асистенти Echo Show, Spot та Plus вміють працювати безпосередньо оскільки мають вбудований zigbee координатор. Проте

проблемою є обмежена кількість сумісних пристроїв і непопулярність рішення в країнах СНД.

Xiaomi / Aqara- шлюзи компаній Xiaomi і Aqara підтримують тільки свої zigbee пристрою. На відміну від Xiaomi Gateway у Aqara Hub не передбачена можливість інтеграції з альтернативними системами домашньої автоматизації.

Samsung SmartThings позиціонується як універсальний хаб. Працює з великою кількістю пристроїв Z-Wave і Zigbee. Користувачі часто скаржаться на падіння хмари (відсутність підключення до сервера) і відсутність інтересу в розвитку проекту з боку розробників.

Яндекс будинок. Діалоги Яндекс Станції і для телефону це різні речі. Для колонки діалогів менше, вони примітивні. Заявлена підтримка ZigBee і Bluetooth пристроїв, але не працює з ними безпосередньо. Багато сценаріїв залежать від наявності інтернет з'єднання, але рішенням може бути підключення сторонніх контролерів розумного будинку, наприклад за допомогою yandex2mqtt.

Як там з програмною підтримкою?

Для зручності розділю програмні рішення на категорії

Домашня автоматизація

- Homebridge сервер NodeJS, для інтеграції пристроїв без підтримки HomeKit.
- ioBroker відкрита система автоматизації, розроблена на платформі NodeJS
- HomeAssistant система з відкритим кодом з акцентом на конфіденційність.
- OpenHAB opensource проект з акцентом на зручність настройки
- MajorDoMo система інтеграції з відкритим кодом.

Dashboard

RoboDomo фреймворк, на MQTT з привабливим графічним інтерфейсом.

node-red-dashboard модуль node-red для створення панелі управління, інтегрується в

Інтеграція

Zigbee2mqtt це програма-міст, що дозволяє використовувати разом пристрої різних постачальників, транслюючи команди zigbee в mqtt.

MQTT Explorer зручний mqtt клієнт

Розробка

IAR Embedded Workbench середовище з дружнім інтерфейсом і підтримкою великої кількості мікроконтролерів

Simplicity Studio IDE і набір інструментів для розробки додатків на базі процесорів Silicon Labs

SimpleLink SDK середовище розробки для чіпів розробки Texas Instruments, що включає API, TI-RTOS та інше .

Red-node блокувальний інструмент програмування для з'єднання апаратних пристроїв, API і онлайн-сервісів.

Тестування і аудит

KillerBee - інструмент для тестування Zigbee мереж.

SecBee - тестування реалізацій ZigBee на проблеми безпеки.

Z3sec - основна мета фреймворку тестування сертифікованих пристроїв, що реалізують ZigBee Light Link (ZLL), або стандарт ZigBee 3.0.

pwnrf - інструмент для тестування безпеки в мережах Wi-Fi, Bluetooth і Zigbee.

Список використаних джерел

1. Thread-vs-zigbee-what-s-the-difference https://e2e.ti.com/blogs_/b/process/archive/2018/05/16/
2. Thread та Zigbee для дому та будівництва // <http://www.ti.com/lit/wp/sway012/sway012.pdf>
3. Специфікації // <https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf>
4. Що нового в zigbee 3.0 // <https://www.ti.com/lit/an/swra615a/swra615a.pdf>.

АНАЛІЗ ТОПОЛОГІЙ МЕРЕЖІ ZIGBEE

Волощакевич В.І.

*Навчально-науковий інститут телекомунікацій
Державний університет телекомунікацій*

Безпроводові сенсорні мережі (БСМ) є одним з найбільш перспективних напрямків розвитку сучасних телекомунікаційних технологій. Перспективи їх використання пов'язані як із заміною кабельних систем на радіоэфір, так і з новими функціональними можливостями. Завдяки таким характеристикам БСМ, як мініатюрність вузлів, низьке енергоспоживання, порівняно невисока вартість, стало можливим їх широке використання в багатьох сферах людської діяльності

При побудові різних технічних систем потрібні бездротові мережі зв'язку, що не володіють високою швидкістю передачі, але надійні, живучі, здатні до самовідновлення, прості в розгортанні і експлуатації. Для виконання даних вимог були створені стандарт Zigbee, що описує стійкі масштабовані багатокрокові бездротові мережі, простий в розгортанні і підтримує самі різні програми.

Найкращим рішенням для інтеграції стандарту ZigBee, є застосування mesh топології. Існує кілька можливих форм топологій: точка-точка, кластерне дерево, але частіше за все використовують топології зірка і P2P (peer to peer) рис.1., або їх комбінацію. Залежно від вимог, може бути застосована та чи інша топологія. В одній великій мережі фрагментарно можуть використовуватися їх комбінації [1,с.66-81].

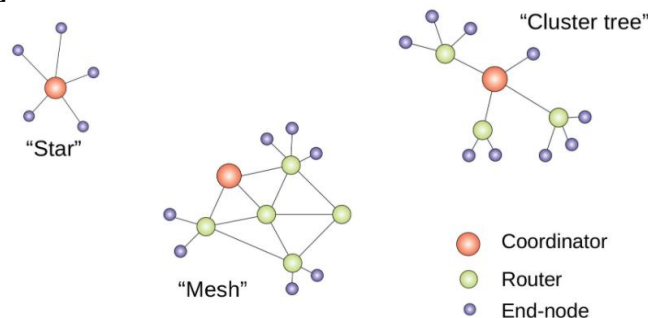


Рис.1. Топології мережі

Розглянемо комунікацію між пристроями в разі зіркоподібній топології. Зв'язок встановлюються між окремими кінцевими вузлами і центральним контролером, який іменується координатором PAN (Personal Area Network). Кінцевий вузол звичайно асоціюється з якимось додатком, що працює в мережі, сенсор вловлює потрібні зміни і буде намагатися надіслати ці дані координатору, або безпосередньо, або через інші вузли. Координатор PAN може виконувати різні функції, він може використовуватися для ініціації деяких додатків, завершення комунікації, або маршрутизації даних в мережі.

Топологія мережі може бути однією з наступних: зірка; кластерне дерево; стильний-модний-молодіжний варіант - mesh.

Топологія peer-to-peer (P2P -меш), аналогічно працює з координатором PAN, але вона відрізняється від зірки тим, що будь-які мережеві пристрої мають можливість комунікувати один з одним. Даний тип топології використовується в моніторингу, промисловому управлінні, інтелектуальному сільському господарстві.

Топологія типу P2P має самоорганізаційну і самовідновлюючу функцію. Дана топологія має можливість організувати багатохопові маршрути для доставки повідомлень. Якщо, наприклад, створювати додаткові канали і залишати резервні контролери, то мережа стає набагато більш стійка до змін в топології. Функції самоорганізації можуть бути додані на більш високому рівні.

Наведені вище рисунки показують, що при необхідності можна реалізувати практично будь-яку топологічну схему.

Одним з ключових переваг Zigbee мереж є їх структура. Вона побудована із застосуванням пористої топології, в той час як Wi-Fi використовує структуру зірки, коли всі з'єднання йдуть через центральний роутер [2,с. 49–54].

У цій структурі, якщо відбувається втрата з'єднання між одним з пристроїв і роутером, воно вже не зможе передати дані до інших вузлів мережі, оскільки між ними немає прямого сполучення. Якщо ж з ладу вийде роутер, то передача даних повністю буде заблокована, що викличе повну непрацездатність системи.

Отже, можна з впевненістю сказати що Zigbee є однією з перспективних технологій, яка має свої переваги і недоліки, та зможе доповнити телекомунікаційний ринок нашої країни.

Перелік використаної літератури:

1. Пахомов С. Технологии беспроводных сетей семейства 802.15.4 // Компьютер Пресс.-2017.- N5.С.66-81.

2. 802.15.4 IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements. The Institute of Electrical and Electronics Engineers, Inc., New York. – 2016.- 49 - 54 с.

АНАЛІЗ ОСНОВНИХ ТЕХНІЧНИХ АСПЕКТІВ МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ П'ЯТОГО ПОКОЛІННЯ

*Ярош Віталій Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Стрімкий розвиток сучасних інформаційних технологій в усіх сферах життя, сприяє до появи нових підходів та методів організації мобільного зв'язку. Вже сьогодні створюються та впроваджуються стандарти мереж мобільного зв'язку п'ятого покоління, які створюють базу для створення істотно нової архітектури в сфері надання інформаційних послуг, але це в свою чергу вимагає створення нових технічних аспектів

Сьогодні перед операторами виникли задачі щодо впровадження нового покоління мобільного зв'язку, які повинно орієнтуватися на надання послуг з високою швидкістю передачі та наднизькою затримкою. Для того, щоб відповідати наведеним вимогам, було розроблено нові технології, об'єднані під загальною назвою 5G NR (нове радіо п'ятого покоління). Розробка даного радіо інтерфейсу велася з урахуванням вимог до характеристик та послуг, що будуть надаватися мережами нового покоління.

5G NR містить важливі покращення до існуючих мобільних мереж та містить в собі наступні технології та принципи організації мобільного зв'язку.

Однією з головних задач при розгортанні мереж 5G є раціональний поділ та використання спектру. Було виділено два головних частотних діапазони FR1 (до 6 ГГц або sub6G) та FR2 (частоти вищі 6 ГГц або mmWave). Такий поділ діапазонів обумовлений тим, що п'яте покоління мобільного зв'язку поєднує в собі різні послуги, що мають різні вимоги до швидкостей, надійності та ступені проникності радіохвилі.

Для збільшення ємності мережі, при збереженні швидкості та якості передачі, використовуються технології MIMO (MassiveMIMO) та beamforming.

Multiple Input Multiple Output (MIMO) – організація передачі даних, коли встановлюють кілька антен на передачу і прийом. Дана схема прийому/передачі дозволяє боротися з багатопроменевим поширенням сигналу за допомогою рознесеного прийому та збільшити полосу пропускання каналу

Технологія beamforming базується на тому, що базова станція обирає найбільш вигідний шлях випромінювання сигналу, в залежності від місця знаходження абонента. Формування діаграми спрямованості дозволяє мінімізувати вплив на інших абонентів, що знаходяться в зоні дії БС.

Однією з головних тенденцій розвитку мобільних мереж п'ятого покоління є напрямок на ефективне використання спектру частот. Таким чином, було прийнято рішення на використання технології OFDM у мережах п'ятого покоління. Основною ідеєю OFDM є використання великої кількості ортогональних піднесучих. Кожна з піднесучих модулюється за звичайною схемою (наприклад QAM). Таким чином, ми маємо наступні переваги використання даного мультиплексування:

- Стійкість до міжсимвольної інтерференції та вузькополосних перешкод.
- Спектральна ефективність .
- Адаптивність методу, тобто використання різного роду модуляцій для кожної з піднесучих.

Для ефективного використання спектру операторами зв'язку використовується технологія поділу спектру, в тому числі динамічний розподіл спектру (DSS). DSS дає можливість операторам використовувати одні і ті ж частотні ресурси та полоси, для різних радіо технологій. Таким чином, вирішується проблема зайнятості частотного ресурсу, що особливо важливо для діапазону низьких та середніх частот, оскільки даний діапазон використовується більшістю радіо технологій.

Технологія 5G принесе з собою високу швидкість передачі даних і малий час затримки, завдяки яким суспільство стрімко увійде в нову еру "розумних" міст та Інтернет речей (IoT).

Таким чином, вище перелічені технології можуть бути застосованими для швидшої цифровізації та інформатизації населення

Список використаних джерел

1. 5G Пятое поколение мобильной связи [Електронний ресурс] // – Режим доступу: <http://www.tadviser.ru/index.php/>.

2. Ярош В.О. Тенденції розгортання мобільних мереж п'ятого покоління / В.О. Ярош // IX Міжнародна науково-технічна конференція студентства та молоді "Світ інформації та телекомунікацій", Київ, 10 жовтня 2019р. Збірник матеріалів. – 2019. – С. 100-102.

РОЛЬ МЕРЕЖЕВОЇ МОДЕЛІ OSI В ПОБУДОВІ ПРОМИСЛОВИХ МЕРЕЖ

Осипець Олексій Анатолійович

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

Міжнародна організація зі стандартизації (ISO) розробила модель мережі OSI (OpenSystemInterconnectionReferenceModel), яка вирішує проблему стандартизації з'єднань різних пристроїв. Мережева модель OSI - це абстрактна модель, яка використовується для розробки мережевих протоколів та мережевих комунікацій. Це уніфіковане представлення даних у мережі за допомогою різних пристроїв та програмного забезпечення. Ця модель реалізує пошаровий метод мережі та визначає процес та правила передачі даних у різних мережевих середовищах. Це семирівнева ієрархія мережі, що виконує певні завдання в процесі передачі інформації через мережу та надає послуги для різних частин процесу взаємодії відкритої системи.

Модель ISO визначає мету еталонної моделі наступним чином: "Забезпечити загальну основу для розробки узгоджених стандартів оперативної сумісності системи, враховуючи, що існуючі стандарти будуть описані в рамках загальної еталонної моделі в майбутньому". По суті, OSI є своєрідною структурою управління, яка може спростити передачу даних у семирівневій ієрархічній системі. Кожен рівень має певне призначення і взаємодіє з

сусідніми верхнім і нижнім рівнями. Визначте стандарти для кожного рівня таким чином, щоб забезпечити певну гнучкість, дозволяючи розробникам систем розробляти незалежні рівні протоколів. Будь-які два або більше шарів разом утворюють так званий стек протоколів.

Модель OSI може бути використана для забезпечення загальної основи для всіх систем зв'язку. Однак вона не визначає фактичний протокол, який буде використовуватися на кожному рівні. Передбачається, що групи виробників у різних галузях будуть співпрацювати для розробки програмних та апаратних стандартів, які найбільш підходять для їх галузей. Ті, хто бажає надати загальну основу для своїх конкретних вимог до обміну даними, із ентузіазмом використовували модель OSI та використовували її як основу для розробки своїх галузевих стандартів, таких як Fieldbus та HART.

Важливо розуміти, що еталонна модель OSI - це не протокол або набір правил протоколу, а загальна структура визначення протоколів. Побудова моделі OSI чітко і детально визначає функції або послуги, які повинні надаватися кожним із семи рівнів.

Взаємодію на рівні моделі мережі OSI можна розділити на дві моделі взаємодії:

- горизонтальна модель взаємодії, що забезпечує зв'язок між програмами та процесами на різних пристроях;
- вертикальна модель взаємодії, яка забезпечує роботу між мережевими рівнями на одному пристрої.

Під час передачі даних відбувається взаємодія між пристроєм, що відправляє, і пристроєм, що приймає, на мережевому рівні. Цей тип зв'язку називається логічним або віртуальним, хоча взаємодія насправді відбувається між сусідніми рівнями пристрою.

Відправляючий пристрій отримує запит, з якого формується повідомлення стандартного формату, що має заголовок певного рівня та поле даних. Повідомлення виконується на міжрівневому стеку, де виконуються певні функції на основі інформації, отриманої від заголовка верхнього рівня, і додається заголовок поточного рівня, що містить інформацію для того самого рівня приймального пристрою. Передане повідомлення "заростає" заголовками всіх рівнів і приймається у фізичному середовищі приймаючим пристроєм. Знову ж таки, повідомлення послідовно переміщується на той самий рівень, з якого воно було надіслане відправником.

Роль кожного рівня в цій мережевій моделі полягає в аналізі та обробці заголовків, які містять інформацію з їх рівня, на якому виконуються функції, що відповідають шару, потім заголовок видаляється і повідомлення надсилається на наступний рівень.

Горизонтальна модель взаємодії між двома пристроями вимагає загального протоколу, який реалізує обмін даними між ними. У вертикальній моделі сусідні рівні обмінюються інформацією за допомогою API (Application Programming Interface) - інтерфейсу програми.

Прикладний рівень - це верхній рівень OSI / RM. Відповідає за надання додаткам доступу до мережі. Прикладами завдань на рівні програми є передача

файлів, електронна пошта та управління мережею. Для виконання цих завдань прикладний рівень надсилає програму та запити даних на рівень перегляду, який відповідає за кодування даних прикладного рівня та переведення їх у відповідну форму.

Представницький рівень перетворює дані у форму, придатну для транспортного рівня. Перетворює формат та синтаксис даних, наданих програмами, а також кодує та стискає дані. Сесійний рівень контролює взаємодію між пристроями. Визначає використання програмного забезпечення, яке дозволяє отримати доступ до іншого пристрою за іменем, а не за двійковою адресою (логічна адресація). Це також забезпечує відновлення перерваних сеансів спілкування.

Через специфічний напрямок промислової мережі використовуються лише два із семи рівнів моделі мережі OSI: фізичний та канальний. Фізичний рівень - це перший рівень мережевої моделі OSI. Він призначений для інтеграції з поєднанням фізичного середовища, обладнання та програмного забезпечення, що забезпечує передачу сигналу між системами. Перший рівень моделі OSI визначає спосіб переміщення двійкових даних з одного пристрою на інший. Одиницею виміру, що використовується на цьому рівні, є біт, який є фізичним рівнем і передає бітовий потік через фізичне середовище через відповідний інтерфейс.

Канальний рівень є другим рівнем мережевої моделі OSI. Він визначає правила доступу до середовища передачі даних, топологію логічної мережі, вирішує проблеми, пов'язані з адресацією фізичних пристроїв усередині логічної мережі та управлінням потоком інформації (синхронізація передачі та послуга з'єднання) між мережевими пристроями.

Канальний рівень визначає доступ до середовища та контроль передачі даних по каналу. При отриманні з них кадрів створюються передані блоки даних, розмір яких залежить від якості каналу та способу передачі. При великих розмірах блоки даних діляться на кадри і передаються послідовно.

Література:

7. Парк Дж., Маккей С., Райт Э. Передача данных в системах контроля и управления. / Парк Дж., Маккей С., Райт Э; [перевод с англ. В. В. Савельева]. — М.: ООО «Группа ИДТ», 2007. — 480 с.
8. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. / Олифер В. Г., Олифер Н. А. — СПб.: Питер, 2010—944 с.

ЗАСТОСУВАННЯ ІННОВАЦІЙНИХ ПЕДАГОГІЧНИХ ТЕХНОЛОГІЙ У ВНЗ

Дурман Володимир

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

Одним із методів модернізації системи освіти є впровадження інноваційних прийомів і методів навчання у навчальний процес вищої школи.

Інновації – це нові форми організації та управління, що охоплюють нові типи технологій у всіх сферах людського життя.

Інноваційна технологія викладання розглядається як особлива організація діяльності та ідей, спрямована на організацію інновацій у галузі освіти, або як процес засвоєння, впровадження та поширення нової освіти.

Інновація навчального процесу означає введення нової мети, змісту, форми та методу навчання та виховання у спільну діяльність учасників організаційного освітнього процесу.

Інноваційна технологія, що використовується в системі вищої освіти, вважається зразком для викладачів для моделювання змісту, форми та методу навчального процесу відповідно до встановлених цілей та прийняття новизни. У практиці освітньої діяльності в сучасних університетах ця технологія навчання використовується для: диференціації, проблемного, контекстного навчання, технології ігрового навчання, інформаційних технологій, технології кредитних модулів, особистісно орієнтованого навчання тощо.

Характеристика навчальних досліджень сучасних технологій контекстного навчання полягає у зосередженні уваги на тісному зв'язку між навчанням та безпосередніми життєвими потребами, інтересами та досвідом студентів коледжів. Кожен студент є носієм особистого досвіду, який слід враховувати та покладатися на нього під час навчального процесу.

Представлена інформація різноманітна і надзвичайно чітка, що забезпечує ефективність сучасних інформаційних технологій у формуванні навичок викладання майбутніх учителів. Можливість організації колективної та індивідуальної дослідницької роботи.

Впровадження інноваційних технологій у професійну підготовку майбутніх учителів може допомогти їм сприймати інформацію зручно, а отже, самостійно засвоювати навчальні матеріали у своєму власному темпі, що змушує їх генерувати позитивні емоції та формувати позитивну мотивацію до навчання.

Активізувати професійну підготовку студентів університетів шляхом впровадження комп'ютерних презентацій, електронних словників, підручників та підручників; тестові програми, підручники, тренажери, словники, довідники, енциклопедії, відеоуроки, бібліотеки електронних наочних посібників, тематичні комп'ютерні ігри створюють професійно орієнтоване інформаційне середовище, сприятливе для розвитку основ педагогічної майстерності майбутніх учителів.

Зміст інформаційно-розвивальних технологій, метою яких є розвиток основ педагогічної майстерності майбутнього вчителя, маючи необхідну систему знань та великий обсяг інформації, включає лекції, семінари, практичні заняття, самостійне вивчення літератури. Підвищення ефективності лекцій досягається використанням системи мультимедійних лекцій, яка повинна враховувати індивідуальний, оригінальний метод викладача, специфіку дисципліни та рівень підготовки аудиторії.

Наявність програмного забезпечення дозволить студентам проводити рефлексивні заходи та в реальному часі усвідомлювати рівень свого

професійного прогресу у формуванні основ педагогічної майстерності. Це допомагає диференціювати навчальний матеріал за рівнями складності, створюючи позитивний емоційний фон для роботи студента з інформаційними засобами навчання.

Важливою складовою педагогічної майстерності є інформаційна культура майбутнього вчителя, тобто здатність продуктивно читати книги, знаходити необхідну інформацію, розуміти та повідомляти її користувачам.

Використання інформаційних технологій у цьому контексті сприятиме не лише розвитку більш високого рівня мотивації майбутнього вчителя, його критичного мислення, а й формуванню телекомунікаційного співтовариства, реалізації активних форм конструктивної комунікативної взаємодії.

Розвитку інформаційної культури сприяє самостійна та наукова робота студентів, яка вимагає індивідуального підходу та відображається у сформованому індивідуальному стилі їхньої професійної діяльності. Продуктивними методами такої роботи є виконання окремих дослідницьких завдань, таких як науковий звіт, який є публічною передачею, детальне викладення конкретної наукової проблеми.

Одним з найважливіших елементів навчального процесу у вищій школі є науково-дослідна діяльність студентів, яка включає підготовку наукових звітів, статей, тез, написання рефератів, курсових, дисертаційних та інших робіт. Поява онлайн-спілкування та Інтернету сприяє впровадженню проблемних методів комп'ютерного навчання для підготовки майбутніх учителів.

Отже, наукова робота студентів є невід'ємною частиною застосування інформаційних технологій та сприяє розвитку інформаційних компетентностей та основи педагогічної майстерності майбутнього вчителя. У процесі наукової діяльності майбутній вчитель отримує знання, що становлять інформаційну основу евристичної діяльності, освоює педагогічні методи та заходи, що визначають оперативні основи когнітивно-дослідницької діяльності, та набуває досвіду в інформаційній діяльності в галузі програмного забезпечення.

Література:

9. Кошечко Н.В. Методика викладання у вищій школі: Навч. посібник / Н.В. Кошечко. – Ніжин: НДУ ім. М. Гоголя, 2013. – 115 с.
10. Гуревич Р.С. Інформаційно-телекомунікаційні технології в підготовці майбутнього фахівця / Р.С. Гуревич // Неперервна професійна освіта: теорія і практика. – К., 2002. –№ 4. – С. 61–68.
11. Буга Н.Ю. Становлення наукової та інноваційної діяльності у вищих навчальних закладах / Н.Ю. Буга // Економіст. – 2006. –№ 9. – С. 60–64.
12. Галиця І.О. Інноваційні механізми активізації педагогічного і наукового процесів / І.О. Галиця // Вища школа. – 2011. – № 7/8. – С. 31–37.

PLC В ЯКОСТІ ТЕХНОЛОГІЇ ОСТАННЬОЇ МИЛІ

Яковець Всеволод Петрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Зв'язок по лініях електропередач (PLC – Power Line Communication), являє собою технологію зв'язку, в якій для передачі сигналів використовуються існуючі

загальнодоступні і приватні кабелі електропостачання. Завдяки цьому найбільшою перевагою PLC є низька вартість і висока швидкість розгортання [1, с. 2]. За допомогою сигналів зв'язку PLC по низьковольтних лініях електропередачі можна передавати високошвидкісні дані, голос і відео.

PLC – це технологія, яка використовується уже протягом багатьох років, але зараз вона стала більш затребуваною після запуску нових телекомунікаційних технологій, які підтримуються PLC, і тому PLC може стати надійним середовищем зв'язку для таких додатків, як Інтернет речей (IoT – Internet of Things) і Розумні мережі електропостачання (Smart Grids) [2].

Під «останньою милею» розуміється відрізок телекомунікаційної мережі, що з'єднує кінцевого абонента з транспортною мережею передачі та, власне, оператором мережі. Поширеними технологіями останньої милі можна вважати xDSL, Wi-Fi, а також високошвидкісні оптоволоконні FTTx та PON, і хоча PLC використовує електричний сигнал для передачі інформації, який має деякі недоліки в порівнянні з оптоволоконним, головною особливістю PLC все ще можна вважати її доступність: це дешево і не потребує побудови нової мережі.

До недавнього часу найбільшими проблемами PLC були мала відстань покриття і низька швидкість передачі даних, які були усунені з введенням нових стандартів [1, с. 2]. Однак навіть незважаючи на те, що нові стандарти гарантують високі швидкості передачі даних, практична реалізація цих технологій для використання в якості рішення останньої милі відсутня [1, с. 2]. Технологія PLC може замінити локальну мережу як рішення «останньої милі», однак у неї є деякі недоліки, перш за все – загальне середовище (лінія електропередачі). Це призводить до втрат пакетів UDP і збільшення затримки TCP, коли мережею користується велика кількість клієнтів [1, с. 2].

Технологія PLC поділяється на два види [3, с. 1-2]:

- Вузькосмуговий PLC (Narrowband PLC). Технологія, що працює в діапазоні частот 3-500 кГц. Відповідно до швидкості передавання даних, ця технологія може бути далі поділена на два підтипи:
 - Низька швидкість передавання даних (LDR – Low Data Rate). Технології з однією несучою і швидкістю передавання даних в декілька кбіт/с.
 - Висока швидкість передавання даних (HDR – High Data Rate). Технології з багатьма несучими та швидкістю передавання даних від десятків до 500 кбіт/с.
- Широкопсмуговий PLC (Broadband PLC). Широкопсмугова технологія працює в діапазоні частот 1.8-500 МГц та може надавати швидкість передавання даних від декількох Мбіт/с до Гбіт/с.

Відповідно до даних, що були отримані в ході незалежних досліджень, приведених в [3, с. 4], теоретична швидкість передавання даних з допомогою PLC стандарту NR AV складає 200 Мбіт/с. Дослідження Horvat, et al. показали, що практична швидкість цього стандарту в реальних умовах із-за загального середовища складає 30-35 Мбіт/с. Стандарт ITU-T G.hn, який зазвичай використовується в домашніх додатках, по результатам дослідження Hallak, et al. може надавати практичну швидкість 95.5 Мбіт/с. Пропускна здатність на

рівні програми становила щонайменше 70 Мбіт/с для ідеального сценарію шуму та щонайменше 30 Мбіт/с для звичайного сценарію шуму; пропускна здатність для гіршого сценарію шуму становила лише 18 Мбіт/с і лише на відстані 55 м [3, с. 14]. Стандарт НР AV2, відповідно до результатів досліджень Fujdiak et al., дозволяє досягати швидкостей передавання інформації в 800-900 Мбіт/с на малих відстанях.

Використання широкосмугового PLC дає можливість надавати користувачам високошвидкісні послуги Інтернет за прийнятну вартість, і крім того, дозволяє реалізовувати додатки Smart Home и Internet of Things. З введенням нових стандартів технологія постійно оновлюється і вже зараз вона знайшла застосування в вигляді клієнтського обладнання, наприклад PLC-адаптерів.

Література:

1. Goran Horvat, et al., "Power Line Communication Throughput Analysis for Use in Last Mile Rural Broadband", Research Gate, 2012, pp. 2-5.
2. Abhiemanyu Pandit, "What is Power Line Communication (PLC) and How it works" [Електронний ресурс] / CircuitDigest.com. – 2019.
3. Mlýnek, P.; Ruzs, M.; Beneš, L.; Sláček, J.; Musil, P. "Possibilities of Broadband Power Line Communications for Smart Home and Smart Building Applications". Sensors 2021, 21, 240., pp. 1-4.

ЕФЕКТИВНІСТЬ СИСТЕМИ УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ

Китаєв Олексій

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

Поняття ефективності може застосовуватися як до системи управління телекомунікаційною мережею, так і до телекомунікаційної мережі. Спершу розглянемо основні поняття ефективності загалом. Ефективністю системи управління телекомунікаційною мережею є створення сприятливих умов для досягнення посадовцями цілей у найкоротші терміни з найвищими якісними та кількісними показниками та найменшими витратами ресурсів. Оскільки завдання управління - це цілеспрямований вплив на об'єкт, що управляється, з метою забезпечення досягнення цілей, ефективність управління може бути оцінена за ступенем досягнення цих цілей: кінцеві результати (забезпечення зв'язку з необхідною якістю), якість планування (розробка планових документів), функціонування системи управління (затримки обробки даних, обсяг інформації, що надсилається за одиницю часу), надійність системи управління (рівень відмов, рівень доступності, простота використання і тд).

На практиці для оцінки ефективності системи управління використовується кілька підходів.

Цільовий підхід - оцінка ступеня досягнення цілей - реалізація програми залежно від вирішення конкретних завдань, досягнення запланованих технологічних показників, прогнозних умов.

Ресурсний підхід - оцінка ефективності управління залежно від ступеня використання ресурсів, як пов'язаних із самим управлінням, так і всіх ресурсів, пов'язаних із забезпеченням комунікації. Для цього необхідно порівняти результат із витратами, за яких він отриманий, порівняти одне абсолютне значення - ефект, з іншим абсолютним значенням - вартість, що дає відносне значення - ефективність. Тобто ефективність - отримання бажаного максимального результату при найменших витратах.

Оцінка досягнутого стану зв'язку військ, їх місця в системі управління - оцінка динаміки основних показників за порівнянний проміжок часу, порівняння їх з нормативними значеннями.

Комплексний підхід поєднує в собі всі попередні.

Ефективність системи управління – це конкретна категорія, що відображає рівень і динаміку управління, якісну та кількісну сторону цього процесу.

За змістом ми розрізняємо військову та економічну ефективність управління, ефективність на етапах управління (планування, розгортання, оперативне управління), ефективність на тактичному (підрозділі), оперативно-тактичному, стратегічному рівні, метод управління Розрахунок ефективності - абсолютний (конкретна система управління) та відносна (порівняно з іншими подібними системами управління) тощо.

Оцінка ефективності управління поділяється на такі типи:

1. З метою оцінки: визначити стан та напрямок розвитку системи управління; визначити ефективність та результативність системи управління та шляхи їх подальшого вдосконалення.

2. Характер оцінки: військові, методичні, функціональні, економічні, соціальні, організаційні, технічні та правові аспекти.

3. Взаємозв'язок між системою управління та керованим об'єктом: з точки зору всієї системи та з точки зору системи управління як частини цілого.

4. Про об'єкт оцінки: комплексна оцінка всієї системи управління та її компонентів.

5. За напрямом оцінки: динамічні (технологічні) та статичні (структурні) характеристики системи управління.

6. За критеріями оцінки: кількісні та якісні.

7. За допомогою методів оцінки: експерти, бали, коефіцієнти, екстраполяція, евристика, порівняння, системи тощо.

Для того, щоб виразити ефективність управління, використовуються деякі часткові поняття:

1. Ефективність системи управління чиновниками.

2. Ефективність системи управління або управлінської діяльності окремих її установ та підрозділів.

3. Ефективність процесу управління (при формулюванні та реалізації конкретних управлінських рішень).

4. Ефективність системи управління (з урахуванням рівня управління).

5. Ефективність механізмів контролю (методів, важелів, стимулів).

6. Ефективність удосконалення управління.

Як правило, ефективність управління розглядається як сукупність трьох частин:

1. Ефективність службових осіб системи управління.
2. Ефективність підрозділів (установ, офісів).
3. Ефективність усієї системи управління.

Показники ефективності управління відповідають вимогам системи управління. Ці вимоги: економічна ефективність (впливає на здатність об'єктів, що управляються, з найменшими витратами), ефективність (своєчасність отримання та обробки інформації, підготовка, прийняття та виконання рішень), надійність системи управління з метою уникнення втрати інформації, різні помилки, і розумний стиль, що характеризує організацію системи управління), ефективність (кількісні аспекти).

На сьогоднішній день не існує стійкого методу визначення ефективності. Тому є особливість, тобто проблема визначення та кількісної оцінки ефективності управління. Система управління телекомунікаційною мережею складається з безлічі підсистем управління, які є частиною підсистеми підтримки прийняття рішень. Це підсистеми, що визначають зміст системи управління: управління маршрутизацією (метод управління маршрутизацією), управління топологією, управління навантаженням, управління якістю послуг, управління ресурсами тощо.

Література:

1. Карганов В.В. Показатель оценки эффективности систем связи и их элементов/ В.В. Карганов, А.Г. Расчесова, Кудряшов В.А. Научнотехнические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2016. – № 1 (236). – С. 7 – 13.
2. Минович А.И. Маршрутизация в мобильных радиосетях – проблема и пути решения / А.И. Минович, В.А. Романюк. – Київ: Зв'язок. – 2006. – № 7. – С. 49 – 55
3. Цыбизов А.А. Оценка эффективности сетей связи/ А.А. Цыбизов. – Рязань: Вестник РГРТУ. – 2009. – № 3 (выпуск 29).

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ІМІТАЦІЙНИХ ПОВЕДІНКОВИХ МОДЕЛЕЙ СИСТЕМ І МЕРЕЖ ЗОВНІШНЬОГО ЗБЕРІГАННЯ І ОБРОБКИ ДАНИХ

*Міненко Єгор Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Імітаційне моделювання вважають одним з напрямків комп'ютерного моделювання. Доречно проаналізувати поведінковий аспект імітаційного моделювання, при якому на комп'ютері відтворюється процес функціонування системи зі збереженням його логічної структури і часовій послідовності подій.

Зазвичай при побудові і використанні імітаційних моделей дослідники роблять акцент на багаторазовому повторенні комп'ютерної реалізації імітаційної моделі з метою збору статистичних даних про об'єкт моделювання, що використовуються для вибору оптимального поведінки і аналізу альтернативних варіантів поведінки системи. При створенні імітаційної моделі

зазвичай використовується і інтерпретується формалізована і неформалізована інформація, а також різні форми представлення даних і знань.

Моделі можна структурувати за ознаками функціонального і ієрархічного порядків. Доцільно розрізняти моделі за цільовим призначенням: архітектурні, функціональні, структурні, організаційні, керуючі та ін.

На архітектурних моделях засновані такі підходи, сформовані в архітектурній практиці автоматизованих систем: об'єктно-орієнтована архітектура (Object-oriented architecture); архітектура, що базується на компонентах (Component-based architecture); сервісно-орієнтована архітектура (Service-oriented architecture); архітектура, що базується на подіях (eventbased architecture); архітектура, керована моделями (model-driven architecture); архітектура, центрована на даних (data-centered architecture). Додамо до цього переліку архітектурні моделі, базуються на знаннях (knowledge-based architecture) і правилах (rulebased architecture).

У своєму розвитку імітаційна модель зазвичай проходить різні стадії - від вельми абстрактних концептуальних моделей до імітаційних моделей з серйозним опрацюванням обчислювальних аспектів.

Архітектурне опис поведінкової імітаційної моделі на базі логіко-алгебраїчного формалізму мереж абстрактних машин, що реалізуються мережами віртуальних машин, відноситься до категорії виконуваних артефактів, подаються у формі, яку можна відтранслювати в виконуваний код програми, а потім вибрати модулі, які доцільно реалізувати мікропрограми або апаратно (наприклад, на основі модулів асоціативної пам'яті).

Додатковим позитивним результатом використання механізму виконуваних формальних специфікацій є спрощення процесу перевірки адекватності моделі реальній системі, так як їх реалізація може базуватися практично на одних і тих же програмах. Це пояснюється тим, що на кінцевому етапі проектування внаслідок вибору одного і того ж формалізму логічна структура імітаційної моделі може практично повністю збігатися з логічною структурою проектованої системи.

Література:

1. Молчанов В. П. Засоби систем обробки даних : навч. Посібник / В. П. Молчанов. – Х.: Вид. ХНЕУ, 2013. – 100 с.
2. Соснин, П. И. Архитектурное моделирование автоматизированных систем: учеб. пособие / П. И. Соснин. - Ульяновск: УлГТУ, 2007. - 146 с.
3. Поспелов, Г. С. Искусственный интеллект — основа новой информационной технологии / Г. С. Поспелов. - М.: Наука, 1988. - 280 с.

DIGITAL COMMUNICATION SYSTEMS OF 5G STANDART

Stanislav Volohovych

State University of Telecommunications

Scientific and Training Institute of Telecommunications

In the modern ICT industry, physical network elements are constantly developing and merging with each other. The more complete accounting for user experience is a step forward to smart terminals and network technologies in the ICT

mobile industry. 5G will provide a much better user experience and will make further rapprochement with innovations in terms of terminals, wireless networks and services. 5G will revolutionize perceptions, acquisition, participation and information control. 5G services will expand to attract more corporate users. The 5G network will use excellent features of the local network and cellular network; It will become smarter and more friendly, and will serve for a wider range of purposes. It will penetrate all aspects of life and coexist with other successful technologies.

5G implies not only an increase in bandwidth and meeting the needs of personal users; It also implies a higher emphasis on user experience and satisfying the needs of the social programs connected to the Internet. In order to achieve these goals, there are three big problems: provision of widespread services, processing data of mass connections, as well as ensuring energy efficiency. Mass data connections. The 5G network sets a high-speed connection between a man and man, a man and a car, and a car-machine. With information as a connection between physical and digital worlds, a ubiquitous general purpose network must be built and high-speedly combined. 5G provides effective compounds with social and corporate applications. These compounds are massive and will be a big problem in terms of network bandwidth and its reliability.

Therefore, 5G should include in the mobile Internet industry all relevant references and production elements associated with an office, shops, medical service, education, entertainment, transport and public life. Physical map, thus, is created on the Internet, and the physical world integrates with the digital world. Energy efficiency. Energy efficiency is important for 5G. In the M-ICT era, large, dense 5G networks with ubiquitous services and mass connections for data transmission will consume a huge amount of energy if they are built on existing technologies. Terminals connect a person and a car to a general network and directly affect what is called user experience. There will be many problems associated with the development of 5G terminals, which include all types of sensing and new media technologies, materials and entertainment devices. Therefore, it is necessary to change the network architecture and restructure NOT and related functions in order to save energy both from the network and the term.

Technological expectations. 5G R & D will focus on enhancing the user experience, targeting applications on the information society, as well as creating an integrated smart network. Technologies for heavy data traffic. Intelligent Mobile Terminals and Cloud Appendices will provide explosive growth of data traffic. To support heavy data traffic, more research must be carried out on a wireless radio line, using a spectrum and network creation.

With the introduction of 5G for the first time, the determining factor will not be a speed but reliability, zero delay, the ability to adjust to certain needs and objectives of applications. And indeed, even high-quality movies thanks to the fifth generation network will load in seconds. This will be possible due to the combination of a number of factors. Yes, an advanced radio winding with increased bandwidth will be used. You should take into account the use of broadband frequencies.

One of the main requirements for the implementation of new services in the network of mobile communication networks 5G is a significant increase in bandwidth

compared to networks of previous generations. If in generations of 3G and 4G it was achieved mainly due to the introduction of new signal-code structures, optimal distribution of frequency resources and expansion of the frequency spectrum, then there is currently an acute shortage of the frequency resource, and the capabilities of its expansion are limited. The development of mobile communication technologies in such conditions makes it possible to look for new ways and solve complex technical tasks in order to ensure the implementation of requirements for increasing the bandwidth of networks 5G.

One of the effective ways to increase the bandwidth is the MASSIVE MIMO technology. These systems have a potential for significant improvement of such indicators as the reliability of the communication channel, spectral and energy efficiency. Another way in future development 5G will increase spectral efficiency by using a millimeter wave frequency range. The advantage of a millimeter range is close to the optical form of radiation distribution, which excludes interference and a violation of communication stability through a multi-beam reception.

References:

1. Portal about modern mobile and wireless technologies. Electronic resource. <http://1234g.ru/1g/chto-takoe-pokolenie-setej-sotovoj-svyazi>
2. Article "What is a mobile communication? How does cellular connection work?" Electronic resource. <https://bumotors.ru/uk/chto-takoe-sotovaya-svyaz-kak-rabotaet-sotovaya-svyaz-sputnikovaya-svyaz-za-i-protiv.html>
3. Tikhvinski V. O. Network 5G prospects and requirements for the quality of their maintenance / Tikhvinski V. O., G. S. Bochechka // Telecommunication, 2014, N N 11.-p.40-43.

ШТУЧНИЙ ІНТЕЛЕКТ ДЛЯ 5G: НАПРЯМКИ ДОСЛІДЖЕННЯ ТА ПАРАДИГМИ

Березнюк А.В., Лазебний С.Г., Макаренко А.О.

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

У цій роботі ми розглядаємо проблеми які виникають 5G та узагальнюємо можливі напрямки застосування для штучного інтелекту у 5G у чотирьох основних категоріях:

1. Проблеми, які важко моделювати;
2. Проблеми, які важко вирішити;
3. Рівномірне впровадження;
4. Спільна оптимізація та виявлення.

У роботі представлені приклади застосування методів штучного інтелекту в 5G, які охоплюють чотири різні проблеми (1), включаючи: розподіл мережевих ресурсів, SON, рівномірний прискорювач 5G та оптимізацію наскрізного зв'язку фізичного рівня.

При використанні штучного інтелекту наймовірно важливо натренувати модель для подальшого аналізу даних. В дослідженні ми використовуємо та

аналізуємо наступні алгоритми (2) для тренування моделей штучного інтелекту базуючись на вхідних даних:

Контрольоване навчання: Зразки пар даних входів та бажаних виходів подаються в комп'ютер, і мета полягає в тому, щоб вивчити загальну функцію, яка пов'язує входи з виходами та додатково виявляє невідомі виходи майбутніх входів

Навчання без нагляду: Під час нагляду без нагляду не наводяться мітки на алгоритм навчання, а структура в його вході повинна знаходитись сама по собі

Підкріплення навчання: Ця методика заснована на альтернативній взаємодії між «агентом» та «навколишнім середовищем»

Зворотне розповсюдження (BP): зворотне розмноження - це метод, що використовується в ANN, який відноситься до категорії градієнтного спуску

- Q-навчання: У цьому алгоритмі визначена функція (функція Q) для оцінки дій «Агента» на основі поточного «Середовища» та виведення результату у вигляді винагороди або штрафу. На певному кроці всі можливі дії «Агента» будуть оцінені функцією Q, а дія з максимальною нагородою в поточному «Навколишньому середовищі» буде обрана наступним кроком і буде фактично виконана

Для застосування штучного інтелекту в 5G вже проведено багато досліджень (3). У цій роботі замість того, щоб намагались переглянути всі існуючі підходи, ми зосереджуємось на поясненні перспективних напрямків досліджень з найбільшим потенціалом. В майбутньому можна очікувати, що 5G досягне значно кращої продуктивності та зручніших реалізацій порівняно з традиційними системами зв'язку. Завдяки надихаючим дослідницьким парадигмам, представленим у цій роботі, ми з нетерпінням чекаємо чудових досягнень штучного інтелекту в 5G найближчим часом.

Список використаної літератури

1. You X H, Pan Z W, Gao X Q, et al. The 5G mobile communication: The development trends and its emerging key techniques. Sci Sin Inform, 2014, 44 (5): 551-563 [5G. 2014, 44 (5):551-563]
2. 3GPP. RP-170741, Way Forward on the Overall 5G-NR eMBB. Workplan[s]. 2017
3. 3GPP. Release-15: LTE Enhancements and 5G Normative Work. 2018

ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ В СИСТЕМІ АНАЛІЗУ І МОНІТОРИНГУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Петрунько Ростислав Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

В останні роки спостерігається значне зростання дослідницького інтересу до розробки та впровадження прикладних інтелектуальних технологій у промисловій та непромисловій галузях. Сьогодні ми можемо обговорити

формування нового наукового напрямку - інтелектуальної теорії управління складними розподіленими інформаційно-комунікаційними мережами. В даний час фундаментальна та прикладна робота зі створення інтелектуальних систем управління активно проводиться у багатьох технічних галузях. Багаторічні теоретичні дослідження в галузі теорії штучного інтелекту, управління контекстом та моделювання забезпечують для цього зручність. У наш час управління, засноване на аналізі зовнішньої ситуації (події), як і раніше залишається однією з головних ідей управління знаннями. Інтелектуальні системи останнім часом стали досить поширеними комерційними продуктами і користуються великим попитом серед користувачів у різних галузях техніки та науки та техніки.

За останні роки науковий інтерес до розробки та впровадження інтелектуальних технологій для промислових та непромислових застосувань значно зріс. Сьогодні ми можемо обговорити питання формування нового наукового напрямку - інтелектуальної теорії управління складною розподіленою інформаційно-комунікаційною мережею. В даний час у багатьох технічних галузях активно проводиться фундаментальна та прикладна робота для створення інтелектуальних систем управління. Багаторічні теоретичні дослідження в галузі теорії штучного інтелекту, управління контекстом та моделювання забезпечують зручність. У наш час управління, засноване на аналізі зовнішніх умов (подій), як і раніше залишається однією з головних ідей управління знаннями. Інтелектуальні системи останнім часом стали досить поширеними комерційними продуктами, і серед користувачів у різних галузях техніки та науки та техніки існує великий попит на інтелектуальні системи.

Нейронні мережі є одним із найпоширеніших методів побудови правил класифікації та прогнозування. Однак їх головним недоліком є те, що процес налаштування архітектури мережі та оцінка її параметрів є досить складним, забезпечуючи тим самим прийнятну якість прогнозування (класифікацію).

Статистична система аналізу телекомунікаційних мереж використовує мережу з декількома впорядкованими шарами нейронів. У цьому випадку не відбувається взаємодії між нейронами, що належать до одного шару. Нейрони кожного шару отримують дані (сигнали) від нейронів попереднього шару, обробляють їх, а потім передають результати обробки на наступний шар. Нейрони у вхідному шарі є винятком. Кількість нейронів у вхідному шарі дорівнює кількості змінних, вибраних для вирішення проблеми передбачення або класифікації, тому кожен нейрон відповідає змінній. Отже, сигнал, що надходить на вхідний рівень, є значенням цих змінних. Сигнал на виході останнього (вихідного) шару нейрона є результатом нейронної мережі. Отже, якщо для класифікації об'єкта до однієї з M -груп використовується нейронна мережа, кількість нейронів у вихідному шарі має бути рівною M .

Створити нейронну мережу, яка може бути використана для класифікації багатовимірних об'єктів або прогнозування значення незалежних змінних (у разі регресійного аналізу або прогнозування часових рядів). Це особливо важливо у випадку статистичного аналізу телекомунікаційних мереж.

необхідно: - вказати архітектуру мережі, тобто вказати кількість шарів та кількість нейронів у кожному шарі; - оцінити вагу всіх нейронів у мережі.

Нейронна мережа повинна містити принаймні два шари: вхідний і вихідний. Кількість нейронів у вхідному шарі визначається кількістю використовуваних змінних. Якщо всі змінні безперервно кількісні, то кількість нейронів дорівнює кількості змінних. Якщо у змінних є номінальні змінні, то $(l-1)$ вхідні нейрони присвоюються кожній такій змінній (наприклад, змінній u), де l - кількість рівнів (категорій) i -ї змінної у ці $(l-1)$, якщо змінною є значення, їй присвоюється значення 1 ; в іншому випадку їй присвоюється 0 . Отже, після вибору змінної активності для вирішення проблеми класифікації, регресії або прогнозування кількість нейронів у вхідному шарі може бути визначена однозначно. Кількість нейронів у вихідному шарі визначається типом вирішуваної проблеми. Коли вирішується проблема класифікації об'єкта в одну з M груп, вихідний шар містить M нейронів. При вирішенні прогностичних (регресійних) проблем кількість нейронів дорівнює кількості залежних змінних. Дослідники встановлюють кількість проміжних шарів та кількість кожного нейрона перед етапом оцінки ваги.

Література:

4. Усков, А. А. Интеллектуальные технологии управления. Искусственные нейронные сети и нечеткая логика [Текст] / А. А. Усков, А. В. Кузьмин. — М.: Горячая линия — Телеком, 2004. — 124 с.
5. Артеменко, М. Ю. Нейронні мережі та їх застосування в телекомунікаційних системах [Текст] / М. Ю. Артеменко, Л. Н. Беркман, С. В. Толюпа // Радіотехніка. — 2007. — Вип. 134. — С. 45–53.
6. Енюков, И. С. Статистический анализ и мониторинг научнообразовательных интернет-сетей [Текст] / И. С. Енюков, И. В. Ретинская; под. ред. А. Н. Тихонова. — М.: Финансы и статистика, 2004. — 320 с.

SDN - РІШЕННЯ ДЛЯ ОПТИМІЗАЦІЇ ТРАНСПОРТНИХ МЕРЕЖ

Олійник Тимофій

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

Концепція, що називалася налаштованим програмним забезпеченням і мережами або програмним забезпеченням мережі (SDN) - поділ мережного управління і управління даними шляхом передачі функцій управління на окремий сервер (контролер). Залежно від мережевої шкали контролер представляє сервер або групу серверів, на якому встановлено спеціалізоване програмне забезпечення. В цьому випадку мережеві елементи, що мають функції управління мережею, виконують суто основні завдання - робота з просування пакетів. Така архітектура дозволяє виділити рівень управління від мережевого устаткування і зробити його програмованим (налаштований на програмне забезпечення). У цьому випадку основна інфраструктура даних також відділяється від мережевих служб і додатків. Цей підхід дозволяє нам розбити мережу управління на окремі централізовані комп'ютерні ресурси (контролери SDN), які обслуговують всю інфраструктуру в цілому. Як

результат, програми, які використовують мережеві функції, можуть відображатися як "логічний" комутатор /маршрутизатор.

Ідея таких мереж була сформульована фахівцями університетів Стенфорда і Берклі ще в 2006 р, а ініційовані ними дослідження знайшли підтримку не тільки в академічних колах, але і були активно сприйняті провідними виробниками мережевого устаткування, що утворили в березні 2011 р консорціум Open Networking Foundation (ONF).

Основна ідея збільшення ефективності функціонування SDN-мережі - використання динамічного розподілу ресурсів мережі для створення своєї мережевої інфраструктури, здатної підтримувати більш широкий спектр вимог з можливістю створення виділених мереж. Такі мережі можуть контролюватися користувачами, наприклад, через корпоративні портали самообслуговування. Реалізація такого рішення дає можливість гнучкої адаптації до різних вимогам прикладного характеру. Для цього була сформована логічна структуру програмно-конфігурується мережі, з відділенням процесу управління системою від самих пристроїв.

Централізована площину управління працює під управлінням програмного комплексу, відомого як SDN-контролер і за характеристиками нагадує проміжне програмне забезпечення. Воно діє на базі алгоритмів, які обчислюють маршрут пересилання пакетів, і відправляє інформацію про даному маршруті в базу даних передачі (FIB) мережевих пристроїв. Вона одночасно підтримує роботу додатків поверх API-протоколів таким чином, що додатки можуть виявляти мережеві ресурси і запитувати їх - до того ж як під управлінням живих мережевих адміністраторів, так і в повністю автоматичному режимі. У той час як така концепція централізованого протоколу вже була відома і випробувана раніше, на цей раз є деякі зміни - вже доступні практичні невичерпні віртуалізовані обчислювальні потужності, які можуть обробляти запити в рамках централізованого управління великими операторськими мережами, в поєднанні з простими принципами програмування на базі Web 2.0 і API-інтерфейсами, за допомогою яких можна просто і швидко розробляти необхідні додатки.

Наступним етапом для SDN стали ЦОДи. Поява віртуальних машин (VM) призвело до зростання ефективності серверів, але при цьому збільшило складність архітектури, в рамках якої на одному сервері працювали десятки VM, які потребують мережевих з'єднань, кількість яких передбачувано зросла. VM з'єднуються з іншими VM або користувачами, тому їх число постійно зростало, або ж у міру старіння вони виводилися з експлуатації, мігрували з сервера на сервер. Відповідно, постійно мінливі конфігурації комутаторів на маршруті, по якому віддавалися дані, ставали все менш керованими. Централізовані SDN-контролери продемонстрували свою цінність: вони «бачили» всю мережу Цодов як абстрактну віртуальне середовище, заздалегідь емулюючи будь-які зміни конфігурації мережі і потім автоматично конфігуруємо безліч комутаторів, як тільки зміни набрали чинності. Не так давно фахівці з архітектури мережі почали експериментувати з SDN в рамках мереж WAN. Самим знаменитим експериментом стало впровадження

централізованого управління на базі SDN в глобальній мережі Google поряд зі спеціалізованими OpenFlow-комутаторами, що з'єднав 12 хмарних Цодов в різних країнах світу.

У той час як SDN, очевидно, має потенціал для спрощення мереж на рівнях IP та Ethernet, оператори проводять капітальні інвестиції і в транспортні мережі. Завдання ускладнюється тим, що потрібно ефективно експлуатувати багаторівневі і Мультидоменні мережі, іноді також працюють на обладнанні різних виробників. Так що немає впровадженого в реальних операторських мережах єдиного рішення, яке б координувало і оптимізував роботу всієї інфраструктури між даними рівнями. Таким чином, в багаторівневої мережі відбувається наступне: весь трафік повинен пройти через маршрутизатор, а якщо йому потрібно більше ємності на транспортному рівні, доводиться вдаватися до ряду ручних процесів, що здійснюються між рівнем даних і транспортним рівнем - а це затратно з точки зору засобів і часу і, в загальному, неефективно. Розширення функціональності SDN з метою здійснювати дані операції на всіх рівнях на обладнанні будь-якого вендора може відбуватися в автоматичному порядку: всі рівні можуть розглядатися в контексті загальних мережевих ресурсів, доступних додатків, виконуваним з SDN-контролера. SDN може служити способом представлення багаторівневої мережі як єдиної виртуалізованої абстракції, іноді званої накладеної мережею. Це дозволяє співробітникам компанії-оператора (або ж додатків в автоматичному режимі) просто «запросити» з'єднання точки А до точки Б при пропускну здатності X Гбіт / с і якість сервісу (QoS) Y без потреби розбиратися в принципах роботи рівнів мережі. Всі мережеві ресурси на будь-якому рівні при такому підході об'єднуються в єдиний пул, доступний будь-якого сервісу або додатком.

SDN-контролер, маючи в своєму розпорядженні пул віртуалізованих ресурсів в рамках всіх рівнів мережі, обчислює самі ефективний маршрут для обходу всіх обмежень або труднощів, емулює його перед підключенням, а потім підключає сервіс на безлічі пристроїв з мінімальним втручанням людини. Наприклад, найефективнішим підходом до виконання запиту від певного сервісу є комутація трафіку на транспортному рівні, уникаючи його маршрутизації через маршрутизатор опорної мережі. В іншому випадку оптимальний підхід може полягати в перенаправленні трафіку через опорний маршрутизатор, а потім його передача в транспортну мережу. Можливий і сценарій, при якому додатку потрібно пропускну здатність маршрутизатора, а останнім, в свою чергу, необхідно більше оптичної пропускну здатності, щоб забезпечити роботу сервісу, і при цьому SDN-контролер автоматично надає необхідну оптичну ємність. Крім того, сьогодні існує можливість забезпечувати більш високу відмовостійкість багаторівневої мережі, наприклад, при використанні рішення shared mesh protection (SMP), яке реалізується на транспортному рівні, дозволяючи забезпечити надійність мережевих ресурсів і оптимізацію їх використання. Таким чином, дана технологія допомагає реалізувати резервні маршрути, що підключаються з низькою затримкою, а також знизити ступінь резервування ресурсів маршрутизатора при непередбачуваних сценаріях відновлення після збою. Архітектура

інтелектуальної транспортної мережі, доповнена функціональністю SDN операторського класу, забезпечує високу ступінь автоматизації, конвергенції і масштабованості мереж операторів, підвищуючи при цьому експлуатаційну ефективність.

Література:

1. Марціленко С.В. Застосування програмно-визначуваних мереж (SDN) в технології 5G / Марціленко С.В., Глоба Л.С. // Десята міжнародна науково-технічна конференція “ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙ” – Київ, Україна, 2016. – с. 191 – 194.
2. Р.Л. Смелянский Технологии SDN и NFV: новые возможности для телекоммуникаций [Электронный ресурс]. – Режим доступа: <http://arccn.ru/media/1132>
3. Роговой В.П. Центры обработки данных на базе технологии SDN / Роговой В.П. // Десята міжнародна науково-технічна конференція “ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙ” – Київ, Україна, 2016. – с. 182 – 185.

ОСОБЛИВОСТІ ЗАПРОВАДЖЕННЯ 5G МЕРЕЖ

*Марковський Сергій Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

5G-стандарти мобільних мереж працюють у певному діапазоні частот – радіохвиль. Їхня частота сягає від 3 кілогерц (кГц) до 300 гігагерц (ГГц). Із кожним новим поколінням діапазон використовуваних радіохвиль зростає. 5G розшифровується як п’яте покоління («5th Generation») мобільних мереж. Це наступна після попередніх поколінь (1G, 2G, 3G, 4G) технологія бездротового зв’язку, яка є ефективнішою й більш досконалою.

Логіка тут проста: чим більше частот — тим більше можливостей доставити сигнал, а отже, тим більше покриття мережі. Чим вища частота хвилі — тим більше можна нею передати за той самий проміжок часу. А інформації й пристроїв стає так багато, що нинішня еволюція до 5G видається логічною. Якщо швидкість 4G сягає в середньому 10 Мб/с, а максимум — до 1 Гб/с, то 5G має середню швидкість від 50 Мб/с, а максимальну — в межах 1-10 Гб/с, і це не межа. Повнометражний фільм із роздільною здатністю HD завантажуватиметься за лічені секунди, а не за хвилини, як зараз.

Активна розробка 5G почалася в 2008 році, але запуск першої 5G-мережі відбувся наприкінці 2018-го — на початку 2019 року в Південній Кореї, а згодом — і у США. Нова технологія доступна в 37 країнах світу, але загальнонаціональної мережі немає в жодній із них. Лідерами у впровадженні 5G, крім згаданих Південної Кореї та США, також є Китай.

Чому ж розширити частоти швидко не вдається? Хоча б тому, що для прийому сигналу певної частоти потрібне відповідне обладнання. А швидко створити багато пристроїв із підтримкою певних радіочастот складно (смартфони з підтримкою 5G уже є).

Але головна причина — конфлікт частот. Річ у тім, що вкрай високі частоти (30-300 ГГц), які пропонують використати для 5G, вже застосовуються для низки інших технологій — це і супутники, і військова техніка, і навіть

радари фіксації швидкості авто та мікрохвильовки. Одночасно використовувати ті самі частоти для завантаження відео й, наприклад, прогнозу погоди неможливо.

Тому уряди країн узгоджують із мобільними операторами конкретні частоти, в межах яких ті будуватимуть свою мережу 5G. А тому очікувати на появу більш-менш широкої мережі п'ятого покоління варто принаймні через кілька років — і це лише в тих країнах, де частоти вже розподілили серед операторів, наприклад США.

Міністерство цифрової трансформації планує забезпечити 95% населення України швидкісним Інтернетом впродовж наступних трьох років. Зокрема, і для цього уряд планує запровадити мережу 5G. Новий стандарт зв'язку використовує хвилі вищих частот, ніж вже діючі мобільні мережі. З одного боку, це дозволяє передавати дані значно швидше. З іншого, через те, що такі радіохвилі дуже короткі, і сигнал гасне на відстані до кілометра, нова технологія потребує більшої кількості передавачів.

При запровадженні технології 5G швидкість Інтернету збільшується в 10-20 разів і з'являється можливість підключати більшу кількість девайсів для користування Інтернетом на одній площі. Наприклад, маючи зв'язок 5G, можна буде завантажити повнометражний фільм у високій якості менш ніж за хвилину.

18 листопада відомство затвердило план вивільнення смуг радіочастот для 5G. Зараз у цьому діапазоні працює телебачення, яке планують перевести на нижчі частоти. А вже за рік планують оголосити тендер на частоти для 5G серед операторів мобільного зв'язку.

Український уряд акцентує увагу на тому, що нова технологія дозволить пришвидшити інтернет для користувачів мобільного зв'язку. Проте 5G – не лише про це. Зв'язок нового покоління, зокрема, допоможе розвивати й інші технології.

Наприклад, швидший інтернет дозволить краще працювати технологіям штучного інтелекту. Таким чином, запровадження 5G зробить реальністю діагностику захворювань на відстані завдяки сенсорним рукавицям, а також проводити хірургічні операції на відстані. Технологія особливо важлива, коли немає можливості транспортувати пацієнта, якому необхідна термінова операція, до лікаря, який може її провести.

Автомобілі-безпілотники вже існують. Проте 5G допоможе ввести їх у масову експлуатацію. Завдяки кращій роботі штучного інтелекту такі автомобілі зможуть краще реагувати на зовнішні обставини – це знизить кількість аварій.

Мобільні оператори: Запуску 5G в Україні варто очікувати не раніше 2022 року

Велика трійка мобільних операторів - "Lifecell", "Vodafone Україна" і "Київстар" - заявили, що всі інвестиції та зусилля спрямовані на розвиток 4G, а запуску 5G варто очікувати не раніше 2022 року.

Про це повідомляє AIN.UA з посиланням на представників операторів мобільного зв'язку.

Зокрема, у "Vodafone Україна" планують запуск 5G у 2022 році.

5G буде давати новий досвід там, де ці дві характеристики є вкрай важливими. Наприклад, для безпілотних автомобілів 5G допоможе ліквідувати небезпечну затримку сигналу на великій швидкості. Швидкодія роботів і уніфікація інфраструктури будуть важливими для промисловості. З рештою завдань успішно справляється і 4G.

Vodafone у найближчому майбутньому зосередить інвестиції на розгортанні мереж 4 покоління на всій території України, а не на точковому впровадженні 5G.

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

*Теренковський Максим Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Штучний інтелект – це атрибути розумних систем, які виконують інноваційні функції, традиційно вважаються прерогативою людини; наука і технологія створення інтелектуальних машин, особливо інтелектуальних комп'ютерних програм. Штучний інтелект пов'язаний із завданням використання комп'ютерів для розуміння людського інтелекту, але він не обов'язково обмежується біологічно здійсненими методами. Поля застосування сучасних інтелектуальних систем дуже вузькі. Наприклад, програма, яка може перемогти людей у шахи і не може відповідати на запитання тощо.

Комп'ютерна техніка проникла у всі рівні суспільства, щоб допомогти людському розвитку, але також принесла багато загроз. Очевидним прикладом є розвиток нової форми мислення, а саме штучного інтелекту. Штучний інтелект (ШІ) - це здатність автоматизованих систем формалізувати та виявляти атрибути, пов'язані з поведінкою людини. Розвиток штучного інтелекту пов'язаний з науками психології, нейрофізіології, математики та інформаційних технологій. Штучний інтелект - це дуже молода наукова сфера, заснована американськими нейрофізіологами. Вони розробили першу, засновану на теорії людської мозкової діяльності "Нейтронні" моделі.

Сьогодні штучний інтелект як і раніше є однією з найбільш перспективних і нерозкритих напрямків розвитку систем та технологій управління інформацією. Сьогодні в поняття штучного інтелекту входять нейронні мережі, нечітка логіка, експертні системи, комп'ютери п'ятого покоління та системи моделювання мислення. Багато компаній, включаючи автономні транспортні засоби Google, Mercedes-Benz та Honda, розробили дивовижні приклади ШІ.

Автомобіль оснащений системами без управління водіями, GPS навігаторами, високомобільними камерами та датчиками, які можуть:

перемикатися в автономному режимі, розпізнавати дороги, визначати його розташування, прокласти дорогу, знаходити вільне місце та припаркувати його.

Штучний інтелект носить складний характер. Тут використовується дуже складна суміш інформатики, математики та інших складних наук. Комплексне програмування допомагає цим машинам відтворювати пізнавальні здібності людини.

Використання штучного інтелекту в телекомунікаціях стає все більш популярним, і легко зрозуміти, чому. В епоху Інтернету речей (IoT) телекомунікаційна індустрія вже не обмежується наданням основних телефонних та Інтернет-послуг, а стала центром технологічного розвитку під керівництвом мобільних та широкосмугових послуг. Штучний інтелект додає цінності телекомунікаційним компаніям. Сучасні постачальники послуг зв'язку (CSP) стикаються зі зростаючим попитом на кращі послуги та краще обслуговування клієнтів (CX). Телекомунікаційні компанії користуються цими можливостями, скориставшись величезною кількістю даних, зібраних з їх величезної клієнтської бази протягом багатьох років. Ці дані надходять із пристроїв, мереж, мобільних додатків, географічного розташування, детальної інформації про клієнтів, використання послуги та даних про виставлення рахунків. Телекомунікаційні компанії також використовують функції ШІ для обробки та аналізу великої кількості масивних даних для отримання ефективних ідей та покращення якості обслуговування клієнтів, поліпшення операцій та збільшення доходу за рахунок нових продуктів та послуг.

Чотири випадки використання ШІ в галузі телекомунікацій
Інвестиції в штучний інтелект у чотирьох основних сферах:

- Оптимізація мережі
- Профілактичне обслуговування
- Віртуальний помічник
- Автоматизація роботизованих процесів (RPA)

У цих сферах штучний інтелект почав давати відчутні результати бізнесу. Телекомунікації - одна з найбільш швидко зростаючих галузей, яка використовує штучний інтелект та безліч бізнес-операцій для покращення обслуговування клієнтів, підвищення надійності мережі та прогнозування послуг. Крім того, телекомунікаційні компанії застосовують рішення щодо штучного інтелекту для вилучення відповідних бізнес-даних із великого обсягу даних, зібраних з багатьох джерел даних. Ці ідеї дозволяють їм покращити якість обслуговування клієнтів, розширити сферу діяльності та вплинути на загальний стан доходів організації. Телекомунікаційні компанії використовують ШІ, машинне навчання та інтелект для збору та аналізу великої кількості даних. Проаналізувавши зібрані дані, він автоматично виявить збій передачі, щоб швидко вжити коригуючих заходів. Автоматизовані служби підтримки допомагають підвищити прозорість та порадувати клієнтів. Програми штучного інтелекту доповнюють хмарні обчислювальні операції, такі як Інтернет речей, електронна пошта та сховище бази даних.

Штучний інтелект набирає популярності швидшими темпами; впливаючи на те, як ми живемо, взаємодіємо та покращуємо досвід клієнтів. У найближчі роки в майбутньому буде набагато більше вдосконалень, розвитку та управління. ЗМІ, Інтернет, сучасні електронні пристрої активно впроваджують в будинок програмне забезпечення штучного інтелекту. У той же час пристрої, оснащені штучним інтелектом та покликані покращити комфорт життя, стали ознакою повсякденного життя. Це має великий вплив на напрямок науково-технічних досліджень, пов'язаних із використанням комп'ютерів, та забезпечує практичні результати для суспільства.

Потенційні переваги ШІ, очевидно, більше, ніж потенційні недоліки. Для безпечного закріплення технологічного розвитку та звільнення суспільства від упереджень та ризиків необхідно сформулювати та посилити чинне законодавство у цій галузі. Це створить етично правове середовище для розвитку інновацій. На сьогодні можна бачити, що ШІ вже заповнив всі кутки людського сприймання та аналізу. Навіть, якщо взявши смартфон до рук та сфотографувати свого друга, ми зустрічаємося з роботою ШІ. А саме автоматичне фокусування людського обличчя (контур фокусування зображення на істотах при фотозйомці).

Література:

1. Стюарт, Р., Норвіг, П. Искусственный интеллект: современный подход (АИМА) / Artificial Intelligence: A Modern Approach (АИМА). – 2-е изд. Стюарт Р, П. Норвіг. – М.: «Вильямс», 2007 – 1424 с.

2. Turing, A. M. Computing Machinery and Intelligence.// <https://www.intellias.com/ai-in-telecommunications/> (дата звернення 18.04.2021)

ТЕХНОЛОГІЯ МІМО В МЕРЕЖІ LTE

Резніченко Сергій Сергійович

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

У сучасних системах стільникового зв'язку постійно зростають вимоги до їх пропускнув спроможності і ємності, що може бути досягнуто за рахунок збільшення числа базових станцій, ширини смуги частот радіоканалів, або числа радіоканалів, а також підвищення спектральної ефективності. Економічно виправданим є шлях підвищення ефективності використання радіочастотного спектру, тобто збільшення пропускнув здатності системи в одній соті мережі, що припадає на одиницю радіочастотного спектру.

Одним із способів підвищення спектральної ефективності є застосування методу просторового кодування сигналу МІМО, що дозволяє збільшити смугу пропускання каналу, в якому передача даних і отримання даних здійснюються системами з декількох антен. Передальні і приймальні антени розносять так, щоб кореляція між сусідніми антенами була малою.

Мобільна передача даних LTE відноситься до покоління 4G. За допомогою неї підвищується швидкість приблизно в 10 разів і ефективність передачі даних, в порівнянні з 3G мережею. Однак, не рідко буває, що швидкість прийому і передачі, навіть нового покоління, залишає бажати кращого. Це безпосередньо залежить від якості сигналу, який надходить від базової станції. Для вирішення даної проблеми використовують зовнішні антени.

За своєю конструкцією, LTE антени можуть бути: звичайні і MIMO. За допомогою звичайної системи можна добитися швидкості до 50 Мбіт / сек. MIMO ж, може збільшити цю швидкість в два рази. Це здійснюється за рахунок установки в одній системі (коробі) двох антен, розташованих на невеликій відстані один від одної. Вони одночасно приймають і передають сигнал через два окремих кабелю до приймача. За рахунок цього відбувається таке збільшення швидкості.

MIMO (Multiple Input Multiple Output - множинний вхід множинний вихід) - це технологія, яка використовується в бездротових системах зв'язку (WIFI, WI-MAX, стільникові мережі зв'язку), що дозволяє значно поліпшити спектральну ефективність системи, максимальну швидкість передачі даних і ємність мережі. Головним способом досягнення зазначених вище переваг є передача даних від джерела до одержувача через декілька радіо з'єднань, звідки ця технологія і отримала свою назву.

В умовах щільної міської забудови, через велику кількість перешкод, таких як будівлі, дерева, автомобілі та ін., Дуже часто виникає ситуація коли між абонентським обладнанням (MS) і антенами базової станції (BTS) відсутня пряма видимість. В цьому випадку, єдиним варіантом досягнення сигналу приймача є відбиті хвилі. Однак, багаторазово відбитий сигнал уже не володіє вихідної енергією і може прийти із запізненням. Особливу складність також створює той факт, що об'єкти не завжди залишаються нерухомими і обстановка може значно змінитися з плином часу. У зв'язку з цим виникає проблема багатопроменевого поширення сигналу - одна з найбільш істотних проблем в бездротових системах зв'язку.

Для боротьби з багатопроменевим поширенням сигналів застосовується Receive Diversity - рознесений прийом.

Суть його полягає в тому, що для прийому сигналу використовується не одна, а зазвичай дві антени, розташовані на відстані один від одного. Таким чином, одержувач має не одну, а відразу дві копії переданого сигналу, що прийшов різними шляхами. Це дає можливість зібрати більше енергії вихідного сигналу, тому що хвилі, прийняті однією антеною, можуть не бути прийнятими іншою і навпаки. Цю схему організації радіо інтерфейсу можна назвати Single

Input Multiple Output (SIMO). Також може бути застосований зворотний підхід: коли використовується кілька антен на передачу і одна на прийом, ця схема називається Multiple Input Single Output (MISO).

В результаті ми приходимо до схеми Multiple Input Multiple Output (MIMO). У цьому випадку встановлюються кілька антен на передачу і прийом. Однак на відміну від зазначених вище схем ця схема рознесення дозволяє не тільки боротися з багатопроменевим поширенням сигналу, але і за рахунок використання декількох антен на передачу і прийом кожній парі передавальної/приймальної антени можна зіставити окремий тракт для передачі інформації. В результаті, теоретично, можна збільшити швидкість передачі даних в стільки разів, скільки додаткових антен буде використовуватися.

На сьогоднішній день можна відзначити бурхливе зростання обсягу трафіку в мережах рухомого зв'язку 4 покоління, і щоб забезпечити необхідну швидкість всім своїм абонентам, операторам доводиться шукати різні методи щодо підвищення швидкості передачі даних або щодо підвищення ефективності використання частотного ресурсу. MIMO ж дозволяє в наявній смузі частот передавати майже в 2 рази більше даних за той же часовий проміжок при варіанті 2x2. Якщо ж використовувати антенну реалізацію 4x4, то, на жаль, максимальна швидкість інформації складе 326 Мбіт / с, а не 400 Мбіт / с, як передбачає теоретичний розрахунок. Це пов'язано з особливістю передачі через 4 антени. Кожній антені виділені певні ресурсні елементи для передачі опорних символів. Вони необхідні для організації когерентної демодуляції і оцінки каналів. На закінчення можна зробити висновок, що MIMO виправдала себе як перспективна технологія для побудови мобільних систем широкосмугового радіодоступу зі швидкостями в сотні Мб / с.

Список використаних джерел

1. Степутин А.Н. Мобильная связь на пути к 6G // А.Н.Степутин. – СПб, 2017. – 416 с.

ПРОЕКТ ТИПІЗОВАНОЇ МОДЕЛІ МУЛЬТИПЛЕКСОРНОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

*Батушев Антон Борисович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Предмет дослідження – моделі та алгоритми оцінки пропускної здатності ланок мультисервісної мережі

Мета роботи – підвищення показників якості мультисервісної мережі.

Методи дослідження – методи натурального моделювання, теорії обчислювальних систем і масового обслуговування; методи теорії інформації та алгоритми складних систем, методи теорії системного аналізу, рекомендації та стандарти міжнародних організацій.

В роботі проведено огляд особливостей розвитку і планування мультисервісних мереж зв'язку, який показав, що при спільному обслуговуванні неоднорідного трафіку комунікаційних додатків реального часу спостерігається неконтрольований оператором перерозподіл каналного ресурсу на користь потоків заявок з малими потребами в ресурсі передачі інформації [1]. Для усунення негативних наслідків цього явища пропонується застосовувати або резервування, або роздільне використання ресурсу ланок мережі. Виконаний аналіз особливостей розвитку і планування мультисервісних мереж зв'язку показав, що при спільному обслуговуванні неоднорідного трафіку комунікаційних додатків реального часу спостерігається неконтрольований оператором перерозподіл каналного ресурсу на користь потоків заявок з малими потребами в ресурсі передачі інформації. Для усунення негативних наслідків цього явища пропонується застосовувати або резервування, або роздільне використання ресурсу ланок мережі. Для обґрунтування процедури вибору конкретного сценарію необхідна розробка моделей, що реалізують ці сценарії, а також алгоритми.

Отже, виконаний аналіз особливостей розвитку і планування мультисервісних мереж зв'язку показав, що при спільному обслуговуванні неоднорідного трафіку комунікаційних додатків реального часу спостерігається неконтрольований оператором перерозподіл каналного ресурсу на користь потоків заявок з малими потребами в ресурсі передачі інформації. Для усунення негативних наслідків цього явища пропонується застосовувати або резервування, або роздільне використання ресурсу ланок мережі. Для обґрунтування процедури вибору конкретного сценарію необхідна розробка моделей, що реалізують ці сценарії, а також алгоритмів розрахунку їх характеристик в розрахунку їх характеристик.

Література:

1. Вишневикий В.М. Теоретические основы проектирования компьютерных сетей. – М.: Техносфера, 2003. – 512с.

ПОБУДОВА БЕЗПРОВІДНОЇ МЕРЕЖІ З ВИСОКОЮ ІНТЕНСИВНІСТЮ ПЕРЕДАЧІ ІНФОРМАЦІЇ

*Білокриницький Олег Васильович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

На базі використання сучасного обладнання та програмного забезпечення в даний час цілком можливо побудувати на базі стандарту 802.11ac [1] надійну, ефективну, захищену і стійку безпроводну мережу.

В роботі проаналізовано та досліджено процес розробки, налаштування та оцінки пропускної здатності безпроводної мережі з високою щільністю, який складається з наступних етапів:

- вибору необхідної кількості каналів;
- визначення пропускної здатності кожного каналу;
- визначення кількості користувачів на канал та необхідної кількості точок

доступу у кожному каналі;

-вибору просторового фактору повторного використання частотних каналів;

-обчислення загальної пропускної здатності системи.

Отже, з розвитком безпроводних технологій та появою точок доступу нового покоління з'явилася можливість створення складних високопродуктивних безпроводних мереж, які дозволять підвищити швидкість передачі, забезпечити високу щільність абонентів та задану надійність.

Література:

1. HP Ethernet Virtual Interconnect and Multitenant Device Context Enable Cloud Computing with multi-tenancy and simple Data Cent Interconnection. [Електронний ресурс] – Режим доступу. – URL:<http://h17007.www1.hp.com/docs/814/factsheet.pdf>

ТЕХНОЛОГІЯ FTTx ЯК ОСНОВА ПОБУДОВИ МЕРЕЖІ ДОСТУПУ

Голда Марина Анатоліївна

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

За час, що пройшов з моменту появи перших локальних мереж, було розроблено декілька сотень самих різних мережевих технологій, проте помітне поширення отримали небагато. Це пов'язано, передусім, з високим рівнем стандартизації принципів організації мереж і з підтримкою їх відомими компаніями. Проте, не завжди стандартні мережі мають рекордні характеристики, забезпечують найбільш оптимальні режими обміну. Але великі обсяги випуску їх апаратури і, отже, її невисока вартість дають їм величезні переваги. Важливо і те, що виробники програмних засобів також в першу чергу орієнтуються на найпоширеніші мережі. Тому користувач, що вибирає стандартні мережі, має повну гарантію сумісності апаратури і програм.

Нині зменшення кількості типів використовуваних мереж стало тенденцією. Річ у тому, що збільшення швидкості передачі в локальних мережах до 100 і навіть до 1000 Мбіт/с вимагає застосування передових технологій, проведення дорогих наукових досліджень. Природно, це можуть дозволити собі тільки найбільші фірми, які підтримують свої стандартні мережі і їх досконаліші різновиди. До того ж більшість споживачів вже встановили у себе якісь мережі і не бажає відразу і повністю замінювати мережеве устаткування. В найближчому майбутньому навряд чи варто чекати того, що будуть прийняті принципово нові стандарти [1].

На ринку пропонуються стандартні мережі усіх можливих топологій, так що вибір у користувачів є. Стандартні мережі забезпечують широкий діапазон допустимих розмірів мережі, кількості абонентів і, що не менш важливо, цін на апаратуру. Але зробити вибір все одно непросто. Адже на відміну від програмних засобів, замінити які неважко, апаратура зазвичай служить багато років, її заміна веде не лише до значних витрат, до необхідності перекладання кабелів, але і до перегляду системи комп'ютерних засобів організації. У зв'язку

з цим помилки у виборі апаратури зазвичай обходяться набагато дорожче за помилки при вибиранні програмних засобів.

Схожі програми розвитку широкосмугових мереж існують і в ряді інших країн. Головну роль в побудові таких мереж буде грати оптичне волокно. Оптичне волокно може прокладатися до приватних будинків або квартир (FTTH), будівель (FTTB) або будь-яких інших вузлів, розташованих в безпосередній близькості від житлових будинків і приміщень. Термін FTTx вказує на загальний принцип організації кабельної інфраструктури мережі доступу.

Отже, в межах дослідження проведено порівняння технологій FTTx та PON, проведено порівняння конструкцій оптичного волокна, підібране обладнання для організації мережі за обраною технологією. У даній роботі спроектована, оптична кабельна інфраструктура за допомогою технології FTTH у вже побудованому житловому комплексі.

Технологія FTTH є дорожчою від інших технологій при побудові мережі, але при експлуатації і обслуговуванні даної мережі вона є на багато економічно вигідною від інших технологій конкурентів.

Провівши розрахунки, було виявлено, що загальна вартість такої мережі складає 4 319 799 грн., а ціна для замовника 5 183 758 грн, що робить спроектовану інфраструктуру прибутково вигідною.

Література:

1. FTTx. Принципы построения, технологии и решения для монтажа. Бонч-Бруевич М.А., Былина М.С. Под редакцией Глаголева С.Ф. Санкт-Петербург, 2012.

РОЗРОБКА ПРОЕКТУ БАГАТОКАНАЛЬНОЇ СИСТЕМИ ПЕРЕДАЧІ НА ОСНОВІ PDH ТА SDH

*Горбач Валерій Валерійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Дана робота присвячена темі синхронізації в мережі SDH. Сучасна первинна мережа орієнтована на використання технології SDH. На відміну від технології PDH, де передбачався режим, плезиохронної ("майже синхронної") роботи різних пристроїв систем передачі, технологія SDH передбачає синхронну роботу всієї мережі і всіх пристроїв, що входять в мережу [1]. Тому сучасною тенденцією в розвитку первинної мережі є підвищення ролі СС і ця тенденція збережеться в найближчому майбутньому.

Всі елементи мережі в SDH мережі працюють, використовуючи одну частоту синхронізації, що поставляється джерелом синхросигналу. Джерелом СС може бути зовнішній еталон або лінійний сигнал. Розподіл синхросигналу здійснюється за системою передачі SDH. Рівень якості СС, використовуваного при виробництві STM-N лінійного сигналу вказується байтом SI SOH. (STM -

синхронний транспортний модуль, інформаційна структура, що складається з інформаційного навантаження і секційного заголовка SOH).

Основне завдання синхронізації цифрової мережі полягає в тому, щоб гарантувати отримання однієї і тієї ж швидкості передачі і прийому інформації в цифрових мережах зв'язку і уникнути появи "прослизанні". Всі генератори, встановлені в цифровій мережі зв'язку, повинні бути синхронізовані від одного або декількох провідних генераторів з близькими значеннями частот вихідних коливань.

Отже, в процесі виконання роботи потрібно спроектувати дві системи: на основі PDH і на основі SDH.

Для мережі PDH довелося розраховувати безліч параметрів, таких як захищеність сигналу, кількість розрядів в кодової комбінації і ін. Так само потрібно було перевести вихідну двійкову кодову комбінацію 111011000011 в послідовність кодових імпульсів. І для цієї послідовності розрахувати і побудувати графік після накладення перешкод і при межсимвольної інтерференції. Далі пропонувалося вибрати коаксіальний кабель найбільш вигідний для конкретного випадку. Все це говорить про те, що при використанні PDH можуть з'явитися різні складності в передачі, прийомі і розшифровці сигналів. Пропонується для вихідної топології мережі вибрати і налаштувати обладнання транспортної мережі. Оснастити обладнання тільки необхідними модулями для економії коштів.

Література:

1. Гордієнко В. Н., Тверецкая М.С. "Багатоканальні телекомунікаційні системи. Підручник для вузів" Москва: Горяча лінія-Телеком, 2007.

РОЗРОБКА ПРОЕКТУ СИСТЕМИ РЕЗЕРВУВАННЯ ДАНИХ ДЛЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

*Григоренко Мирослав Михайлович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Об'єкт дослідження – резервування даних інформаційної системи.

Предмет дослідження – методи різних типів захисту даних.

Мета роботи – визначити кращі рішення для збереження даних і надання захисту обчислювальних ресурсів систем резервування даних різних підприємств.

Методи дослідження – метод експертних оцінок, аналітичний аналіз, теоретичні відомості, детальне вивчення та комплексне порівняння надійності захисту даних.

В роботі приведено основні відомості про засоби і технології резервування даних для інформаційних систем та виявлено потреби їх встановленню та подальший розвиток. Сформульовані вимоги до підсистеми автоматичного резервування даних користувачів. Описано склад, призначення комплексу програм і його компонентів. Визначено постановка задачі, склад і

функції підсистеми. Розглянуто існуючі системи резервування даних, а так само проаналізовані: Технології резервного копіювання [1], технології зберігання резервних копій і даних, зберігання, технології відновлення даних з резервних копій, способи перевірки актуальності резервних копій, технології стиснення даних. Сформульовано нові задачі підвищення їх ефективності як на етапі аналізу окремих підприємств так і систем збереження інформації великих корпорацій за їх технічними вимогами. Проаналізовано різні типи резервування та розроблено рекомендації з їх вибору в залежності від заданих технічних вимог обчислювальних ресурсів підприємства з врахуванням їх коректної та надійної роботи. Представлені програмні інтерфейси і алгоритми роботи підсистеми автоматичного резервування даних користувачів і їх відновлення після інциденту втрати даних.

Отже, проведені аналізи технології резервного копіювання, технології зберігання резервних копій і даних, зберігання, технології відновлення даних з резервних копій, способи перевірки актуальності резервних копій, і технології стиснення даних. Описано архітектура, загальна схема функціонування і принцип роботи "Підсистема автоматичного резервування даних користувачів і їх відновлення після інцидентів в ІКС СП". Були визначені основні функції і функціонування підсистем ПК «Створення та контроль версій ПЗ, також дано опис інтерфейсу користувача».

Література:

1. Russell D., DiCenzo C, Аналітика корпоративних систем резервування \ відновлення даних. Унікальний код пошуку Gartner RAS Core Research Note G00142739.

СИСТЕМА ЗАХИСТУ ТА КОНТРОЛЮ ДОСТУПА В ПРИМІЩЕННЯХ

Ковальчук Євгеній Анатолійович

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

Досвід впровадження та експлуатації систем GPS-моніторингу транспорту на підприємствах різних галузей показує, що використання GPS трекерів дозволяє максимально ефективно запобігати нецільовому використанню автотранспорту працівниками організації [1]. Таким чином, доцільно дослідити та реалізувати методику застосування GPS трекерів для автотранспортного підприємства. Виконуючі поставлені завдання в дипломній роботі проаналізовано особливості функціонування системи глобального позиціонування та системи GPS-моніторингу транспорту. Виконано дослідження системи супутникових навігаційних систем та дослідження ринку GPS трекерів. У практичній частині обґрунтовано фінансову ефективність застосування GPS трекерів для автотранспортного підприємства

Отже, в результаті досліджень сформована оптимальна структура периферійного обладнання для запобігання проникнення сторонніх осіб в приміщення. Запропонований спосіб є ефективним для захисту приміщень від сторонніх осіб та може бути використаним на практиці.

Список використаних джерел:

1. Системи захисту та контролю // <https://www.videorus.ru/articles/35/>

ЗАСТОСУВАННЯ GPS-ТРЕКЕРІВ ДЛЯ КОНТРОЛЮ АВТОТРАНСПОРТУ «УКРПОШТА»

*Корчемська Наталія Олександрівна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Досвід впровадження та експлуатації систем GPS-моніторингу транспорту на підприємствах різних галузей показує, що використання GPS – трекерів дозволяє максимально ефективно запобігати нецільовому використанню автотранспорту працівниками організації. Таким чином, доцільно дослідити та реалізувати методику застосування GPS – трекерів для автотранспортного підприємства.

Отже, проаналізувавши актуальність питання впровадження GPS – трекерів на сьогоднішній день стає зрозуміло що питання контролю є напрочуд гострим питанням для кожної організації, яка хоча б мінімально пов'язана з використанням автотранспорту. Тим паче дане питання є особливо актуальним і можна навіть сказати критичним для автотранспортних підприємств. Стан дослідження питання на сьогоднішній день, можна сказати залишає підґрунтя для розвитку перспективного напрямку, як з наукової так і з практичної точки зору.

В роботі за допомогою аналізу [1], порівняння та класифікації досліджено ринку GPS – трекерів, принципи їх функціонування та розглянута класифікація, актуальних на сьогоднішній день моделей, які є найбільш ефективними та популярними у використанні, як апаратних так і програмних трекерів. За допомогою структурно-функціонального методу досліджено систему глобального позиціонування та супутникові навігаційні системи, що дає теоретичні можливості для практичної реалізації нових продуктів, які зможуть бути більш ефективними та встигати за розвитком науково-технічного прогресу. За допомогою методів аналізу та прогнозування оцінена та розроблена методика застосування GPS – трекерів для автотранспортного підприємства та обґрунтована економічна ефективність її впровадження.

Дослідивши в комплексі всі завдання поставлені на початку роботи, стає зрозумілим той факт, що питання впровадження та експлуатації GPS трекерів фактично не вимагає значних капіталовкладень на початковому етапі їх закупки та монтажу, враховуючи ту кількість різноманітних варіантів, які доступні на сьогоднішній день на ринку [2].

В результаті дослідження становлено, що всі витрати підприємства будуть компенсовані вже після першого або максимум другого місяця використання GPS – трекерів. В подальшому ми отримуємо прибутки для підприємства, фактично бб без додаткових витрат фінансового чи людського ресурсів. Дане питання постає особливо актуальним враховуючи світові тенденції до мінімізації витрат та оптимізації розподілення коштів в середині бізнес-середовища на період пандемії.

Література:

1. Серапинас Б.Б. Глобальные системы позиционирования. — М. : ИКФ "Каталог", 2012. — 106 с.
2. Соловьев Ю.А. Системы спутниковой навигации.-М. Эко-Трендз, 2009.с

ASTERISK ЯК РІШЕННЯ ДЛЯ ПОБУДОВИ МЕРЕЖІ ІР-ТЕЛЕФОНІЇ

*Макаренко Артем Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Asterisk в комплексі з необхідним обладнанням має всі можливості класичної АТС, підтримує безліч VoIP-протоколів і надає багаті функції управління дзвінками, серед них: голосова пошта; конференц зв'язок; IVR (інтерактивне голосове меню); постановка дзвінків в чергу і розподіл їх по абонентам; Call Detail Record (докладний запис про виклик) [1].

Для створення додаткової функціональності можна скористатися власною мовою Asterisk для написання плану нумерації, створивши модуль на мові Сі, або скориставшись Asterisk Gateway Interface - гнучким і універсальним інтерфейсом для інтеграції з зовнішніми системами обробки даних. Модулі, що виконуються через AGI, можуть бути написані на будь-якій мові програмування.

Додаток Asterisk [2] може працювати як з аналоговими лініями FXS-модулі), так і цифровими (ISDN, BRI і PRI - потоки T1 / E1). За допомогою певних комп'ютерних плат (найбільш відомими виробниками яких є Digium, Sangoma, OpenVox, Rhino, AudioCodes) Asterisk можна підключити до високопропускних ліній T1 / E1, які дозволяють працювати паралельно з десятками телефонних з'єднань. Повний список обладнання для з'єднання з телефонною мережею загального користування визначається підтримкою обладнання в модулях ядра, наприклад DUNDi.

Додатком Asterisk підтримуються наступні протоколи:

– SIP;	– IAX2;
H.323;	– SIMPLE;
– MGCP;	– Skinny / SCCP;
– XMPP;	– Unistim.

Додаток дає можливість транслювати текст і відеосигнали (наприклад, використовувати відеофон). Крім того, реалізована робота з іншими комп'ютерними протоколами: DUNDi; OSP; T.38 (підтримка передачі факсів).

Налагодження та програмування додатку проводиться за допомогою декількох механізмів: використання спеціальних мов програмування (AEL; Lua), а також AGI та AMI.

Розширення виконуваних функцій також можливо шляхом написання на мові Сі нового модуля, що можливо завдяки докладній Doxygen-документації.

Література:

1. Огляд вільно доступних і безкоштовних IP АТС [Електронний ресурс] // – Режим доступу: <https://habr.com/ru/post/122215/>
2. Asterisk [Електронний ресурс] // – Режим доступу: <https://www.asterisk.org>

МІКРОПРОЦЕСОРНА ОХОРОННА СИСТЕМА АВТОМОБІЛЯ

*Максименко Максим Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Для охорони автомобілів в наш час використовується складний комплекс, в якому присутні найсучасніші механічні, електронні та електронно-механічні пристрої.

Класифікувати ці пристрої можна наступним чином:

- механічні засоби (Mult-lock, Beer-lock, Construct та інші);
- електронні (автосигналізації, протиугінні пристрої, блокатори ланцюгів керування відповідними пристроями та агрегатами та інше);
- електронно механічні (Hood-lock, Construct та інше).

В даній статті розглянуті тільки електронні пристрої. Їх перелік включає: автосигналізації (односторонні, двохсторонні, супутникові та GSM-сигналізації), іммобілайзери та блокіратори ланцюгів керування (живленням, запаленням, стартера, палива, педалі щеплення та інше).

Розроблений пристрій має ряд переваг над існуючими, наприклад VlagBug або SkyBrake. По-перше низьку ціну за рахунок використання доступних матеріалів (мікросхем, конденсаторів, транзисторів, опорів, перемикачів та інше), по-друге простота в використанні, по- третє проста процедура налагодження.

Розробка пристрою включала наступні процедури:

- розробка функціональної схеми;
- розробка принципової схеми;
- розробка монтажною плати;
- розробка зовнішньої упаковки;
- розробка інструкції з встановлення системи;
- розробка інструкції користувача.

Розроблений пристрій призначений для захисту автомобіля від викрадення. Перехід від чергового режиму в режим блокування здійснюється програмно з часовим інтервалом 15с, 30с, 60с. принцип роботи пристрою побудовано на вмиканні (вимиканні) чергового режиму (режиму охорони), за рахунок чого забезпечується блокування (розблокування) ланцюга управління двигуном автомобіля.

Особливістю функціонування пристрою є те, що його активація здійснюється відкриттям дверей водія. Часові інтервали спрацювання реле блокування програмуються при встановленні пристрою (заводське встановлення-15 с). Індикація режимів роботи пристрою здійснюється за допомогою багатофункціонального світло діода, звукових та світлових сигналів [1].

Якщо пристрій знаходиться в активному режимі, а підтвердження (натиснення потайної кнопки) відсутнє, спрацьовує реле блокування (двигун автомобіля блокується) та вмикаються світлові (як правило габаритні вогні) та звукові (сирена) індикатори.

Технічні характеристики пристрою:

- напруга живлення блоку управління (10-15В)
- струм живлення у черговому режимі (30 мА)
- максимальний струм навантаження, який комутує по виходу блокування запалення (40 А)
- кількість програмованих часових інтервалів (3)

Особливості користування пристроєм:

- увімкнення чергового режиму пристрою здійснюється по відкриттю двері водія, а також за допомогою потайної кнопки або брелока автосигналізації, якщо остання встановлена на автомобілі
- відмінною властивістю пристрою є те, що навіть при зчитуванні коду авто сигналізації, що дозволяє зняти її з режиму охорони, пристрій залишається в черговому режимі та може бути розблокованим тільки за допомогою потайної кнопки
- індикація присутності чергового режиму підтверджується відсутністю світловода; у ввімкненому стані він інформує водія, що черговий режим вимкнений.

Література:

1. Маркировка электронных компонентов. Определитель. Додека XXI, 2016 г.-416 стр.

ТЕХНОЛОГІЯ WiMAX ЯК ОСНОВА ДЛЯ ПОБУДОВИ ШИРОКОСМУГОВОГО ДОСТУПУ ДО ТРАНСПОРТНИХ МЕРЕЖ

*Мелконов Роман Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Системи дротового цифрового зв'язку, які існують сьогодні, вже не можуть повною мірою задовольняти зростаючі потреби високошвидкісного широкосмугового доступу. Найважливішими їх недоліками є тривалі терміни прокладання, складності розширення, високі витрати, проблема «останньої милі». Застосування високошвидкісних цифрових з'єднувальних ліній DSL (Digital Subscriber Line) не знімає цієї проблеми.

WiMax – одна з технологій, покликаних вирішити проблему широкосмугового доступу до транспортних мереж, а до того ж, позбавити користувачів необхідності провідного підключення. WiMax повинен забезпечити високошвидкісний, захищений бездротовий доступ з підтримкою контролю над якістю на периферії мережі. Ця технологія не є втіленням принципово нової концепції, її варто розглядати як еволюційний розвиток існуючих раніше технологій широкосмугового бездротового доступу (ШБД).

Основна перевага WiMax – наявність загальноприйнятого стандарту, який дозволяє виробникам працювати над однією технологією, забезпечуючи взаємну сумісність обладнання.

Мета технології WiMax полягає в тому, щоб надати універсальний бездротовий доступ для широкого спектра пристроїв (робочих станцій, побутової техніки «розумного будинку», портативних пристроїв і мобільних телефонів) та їх логічного об'єднання – локальних мереж. Для постачальників послуг WiMax, а також для проектувальників мереж важливо знати, яку територію покриває зона дії станцій WiMax.

Література:

1. WiMax технологія бездротового зв'язку: теоретичні основи, стандарти, застосування / [В. І. Сюваткін, В. І. Єсиненко, І. П. Ковальов, В. Г. Сухоребра]. – СПб. :БХВ-Петербург, 2005. – 368 с.
2. Форум WiMax. Методологія WiMax. Система оцінки. – 2007. – 2012 с.

РОЗРОБКА ПЕРСПЕКТИВНОЇ СИСТЕМИ РАДІОЗВ'ЯЗКУ В ЦИВІЛЬНІЙ АВІАЦІЇ

*Петришин Владислав Валерійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Постановка задачі. З появою сучасних пілотованих та безпілотних апаратів з'явилася необхідність у вдосконаленні систем радіозв'язку. Це пов'язано з удосконаленням систем протидії.

Мета дослідження. Виявити можливості підвищення завадозахищеності існуючих систем радіозв'язку та запропонувати нові способи підвищення захисту каналів зв'язку в літаках цивільної авіації з відповідним наземним обладнанням.

Результати дослідження. На основі аналізу існуючих систем радіозв'язку в цивільній авіації був запропонований спосіб, який підвищив завадозахищеність вищевказаних систем та може бути впроваджений у розробках нових перспективних систем радіозв'язку.

Висновки і перспективи. Запропонований спосіб дозволить підвищити завадостійкість системи радіозв'язку та безпеку літаків цивільної авіації при виконанні польотів.

Література:

1. Інтернет ресурс - <http://megalib.com.ua/>
2. Інтернет ресурс - <https://dt.ua/>

МЕТОДИКА СТВОРЕННЯ МЕРЕЖ П'ЯТОГО ПОКОЛІННЯ ІЗ ЗАСТОСУВАННЯМ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ

*Рощенко Антон Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Принципові зміни в технологіях телекомунікацій вимагають перегляду принципів побудови мереж зв'язку для забезпечення реалізації вимог цих нових технологій. Саме реалізація SDN, яка являє собою нову концепцію побудови мережевої інфраструктури та методики надання сервісів кінцевим користувачам, дозволяє створити умови для прискореного впровадження нових послуг, впровадження нових мережевих протоколів і функціональності та дає можливість інтеграції з інноваційними програмами сторонніх розробників.

Перспективи використання технологій SDN в мережах операторів зв'язку обумовлені наступним чинниками, як : висока масштабованість мережі, гнучке централізоване управління мережею і мережевими ресурсами; зниження капітальних витрат на закупівлю обладнання COTS; зниження операційних витрат завдяки використанню віртуальних мережевих функцій; поліпшення енергетичної ефективності за рахунок використання високопродуктивних серверів центрів обробки даних; зменшення часу запуску нових мережевих сервісів; використання хмарних платформ в центрах обробки даних на периферії оператора для підвищення якості сервісу.

Для досягнення поставленої мети у магістерській кваліфікаційній роботі вирішуються наступні завдання: аналіз концепції розвитку мереж п'ятого покоління і вимог, що пред'являються цією концепцією до мереж зв'язку; дослідження моделі обслуговування та контролю інформаційних потоків із використанням програмно-конфігурованих мереж; експериментальне дослідження підвищення показників якості та розподілу мережевих ресурсів н базі програмно- конфігурованих мережах

У роботі досліджено модель адаптації системи моніторингу безпроводової мережі, конфігурація якої визначається програмно, а саме частоти опитування стану мережних ресурсів, до завантаження вузлів та каналів. Новизна моделі полягає в тім, що на підставі зміни кроку опитування стану каналу вдається підвищити точність оцінки статистичних характеристик використання мережевих ресурсів та ймовірності блокування певного елемента мережі.

У результаті проведення експериментів доведено, що комплексне застосування розглянутих у роботі наукових та технічних рішень дає змогу зменшити затримку для потоків реального часу на 15% та підвищити рівномірність завантаження мережних ресурсів на 30%.

Література:

1. Н.И. Горлов «Оптические линии связи и пассивные компоненты ВОСП» - Новосибирск 2003.-229 с.

РОЗРОБКА ПРОЕКТУ МАГІСТРАЛЬНОЇ ВОЛЗ МІЖ НАСЕЛЕНИМИ ПУНКТАМИ ВІННИЦЯ-ПОЛТАВА

Савченко Богдан Васильович

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

В роботі приведено основні відомості про системи та мережі дротового зв'язку та виявлено тенденції їх сучасного розвитку. Сформульовано нові задачі підвищення їх ефективності як на етапі аналізу окремих функціональних вузлів так і синтезу системи та дротової мережі в цілому за технічними вимогами. Проведена оцінка пропускної спроможності мережі з високою інтенсивністю передачі інформації [1].

В результаті виконання магістерської кваліфікаційної роботи досліджено параметри оптичного волокна. Можуть бути різні варіанти побудови конкретних систем, що відрізняються ступенем захисту і контролю несанкціонованого доступу до інформації, що передається по ВОЛЗ інформації. Це робить необхідним проведення спеціальних досліджень з метою експертизи реалізованих науково-технічних рішень та їх відповідності вимогам забезпечення захисту інформації. Тому важливою проблемою в області захисту ВОЛЗ є розробка нормативної та методичної бази і документів, що забезпечують і регламентують як розробку захищених ВОЛЗ, так і порядок їх впровадження в мережах зв'язку. Ця проблема вимагає свого прискореного вирішення.

Тут необхідно зазначити, що всі перераховані вище методи захисту і їх комбінації можуть забезпечувати безпеку інформації лише в рамках відомих моделей загроз нападу. При цьому ефективність систем захисту визначається як відкриттям нових, так і вдосконаленням технологій застосування вже відомих фізичних явищ. З плином часу противник може освоїти нові методи перехоплення, буде потрібно доповнювати захист, що не властиво криптографічним методам захисту, які розраховуються на досить тривалий термін. Тому, завжди актуальний захист саме від не санкціонованого доступу до волокон но-оптичних ліній зв'язку, а саме, до місць прокладки кабелів.

Література:

1, Н.И. Горлов «Оптические линии связи и пассивные компоненты ВОСП» - Новосибирск 2003.-229 с.

РОЗРОБКА ПРОЕКТУ ТЕЛЕФОННОЇ МЕРЕЖІ ШЛЯХОМ ВПРОВАДЖЕННЯ ЦИФРОВОЇ АТС

Рінсевич Володимир Миколайович

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

На мережі Укрзалізниці існує дві мережі технологічного зв'язку: транспортний зв'язок загального призначення і зв'язок, призначений для рішення задач оперативного характеру – оперативно-технологічний зв'язок. По

районах своєї дії обидва види зв'язку поділяють на магістральний, дорожній, відділковий і станційний.

Реорганізація системи керування тісно зв'язана з використанням нових інформаційних технологій на основі розвитку зв'язку і засобів обчислювальної техніки [1]. Зв'язок пронизує всю галузь на всіх рівнях, включаючи окремі підприємства; послугами зв'язку користуються всі працівники залізничного транспорту.

Однак існуюча мережа зв'язку Укрзалізниці не відповідає сучасним вимогам галузі, насамперед надання нових видів послуг і використання нових технологій, що забезпечують пропуск великого обсягу інформації, високі швидкості передачі, показники надійності і якості зв'язку, а також широкої функціональної можливості, що дозволяють адаптувати мережу зв'язку до структурних перебудов системи керування. Мережа зв'язку є фундаментом системи інформатизації і всієї системи керування галуззю, тобто є частиною інфраструктури Укрзалізниці, що забезпечує життєдіяльність галузі.

Відомча мережа зв'язку будується на базі відомчої автоматичної телефонної станції (ВАТС) [2]. Еволюція ВАТС за останні роки міняла ту стадію, коли їхнім основним призначенням було збільшення номерної ємності відомчої мережі і надання співробітникам підприємства зручного й ошадливого засобу виходу на телефонну мережу загального користування (ТфЗК). Функціональні можливості сучасних цифрових ВАТС надзвичайно різноманітні - починаючи від використання їх як концентраторів телефонного навантаження (міні АТС).

Впровадження проекрованої сучасної цифрової системи комутації дозволить покращити якість зв'язку на телефонній мережі залізничного вузла, збільшити її надійність та можливості, а також надання додаткових видів послуг: прямий зв'язок, скорочений набір, пріоритетне порушення встановленого з'єднання, повідомлення про вхідний виклик, закрита група абонентів, заборона вхідного зв'язку (вибірковий) і т.п.

Представлені дослідження охоплюють новітні технологічні рішення, дозволяють поліпшити показники якості мережі і доцільні до впровадження на сучасних мережах телекомунікацій.

Література:

1. ITU - T/Recommendation G.703/Network Node Interface for the Synchronous Digital Hierarchy (SDH).
2. Андрушко О.С., Васильєв О.К. Резервирование цифровых систем передачи оперативно - технологической связи. //Автоматика, связь, информатика. 2001, №4, С. 8 - 11.

МЕТОДИКА ПОБУДОВИ МІКРОПРОЦЕСОРНОЇ ОХОРОННОЇ СИСТЕМИ АВТОМОБІЛЯ

*Максименко Максим Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Постановка задачі. На основі використання сучасної елементної бази [1] (PIC контролери) та сучасних принципів організації інформаційного обміну між віддаленими об'єктами, розробити систему передачі сповіщень про проникнення.

Ціль дослідження. Розробка надійної, гнучкої (можливість конфігурування), з розширеними функціональними можливостями і простотою у використанні (автоматична постановка під охорону і зняття з охорони об'єктів) системи охоронної сигналізації.

Результати дослідження. Для налагодження керуючої програми використовувався програмний пакет фірми Microsoft v 3.22. Він дозволяє розробляти програмне забезпечення для широкого спектра мікроконтролерів цієї фірми [2]. В процесі проектування була розроблена радіосистема охоронної сигналізації автомобіля, реалізуюча крім типових функцій контролю доступу на охоронювану автостоянку та можливість використання.

Висновок та перспективи. У подальшій перспективі в розробленій системі можна реалізувати додаткові сервісні функції, поєднати в переносній підсистемі функції кодового брелока і прийому тривожних повідомлень по радіоканалу.

Література:

2. Маркировка электронных компонентов. Определитель. Додека XXI, 2016 г.-416 стр.
3. Зарубежные микросхемы памяти и их аналоги. Справочник-каталог. Том 1. РадиоСофт, 2002 г.,-576 стр.

ОСОБЛИВОСТІ РОЗРОБКИ ПРОЕКТУ ДІЛЬНИЦІ МАГІСТРАЛЬНОЇ ВОЛЗ

*Тертичний Роман Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Поява оптичного волокна спричинила величезний прорив у розвитку сучасних телекомунікацій. Стрімкий розвиток ринку телекомунікацій призвів до доступності інформаційних послуг, а збільшення інформатизації суспільства спричинило значний приріст попиту, який й досі не зменшується, але навпаки, зростає з кожним роком в арифметичній прогресії.

Зважаючи на вищевказані обставини потрібно підвищувати рівень конкуренції шляхом впровадження нових магістральних волоконно-оптичних ліній зв'язку та модернізації старих.

Об'єкт дослідження – розробка проекту магістральної ВОЛЗ між населеними пунктами Мукачєво - Суми.

Предмет дослідження – магістральна ВОЛЗ між населеними пунктами Мукачево - Суми.

Мета роботи– розробити проект магістральної ВОЛЗ між населеними пунктами Мукачево - Суми.

Методи дослідження – розрахункова робота, нормативна документація, аналіз обладнання на ринку телекомунікацій у галузі магістральних мереж.

В роботі приведено основні відомості про волоконно-оптичні магістральні мережі світу та України. Тенденції їх сучасного розвитку. Сформульовано нові задачі підвищення їх ефективності, та запропоновано методи їх вирішення [1]. Проаналізовано різні методи підвищення ефективності магістральних ВОЛЗ, та розроблено один з них на базі магістральних ВОЛЗ між населеними пунктами Мукачево – Суми.

Отже, в процесі виконання роботи був вибраний тип оптичного волокна, а також проведений розрахунок довжини ділянки регенерації.

У магістральних ВОЛЗ витрати на придбання та прокладку кабелю є основною частиною вартості всієї системи. Тому доцільно прокласти кабель з можливо низьким загасанням і широкою смугою частот в розрахунку на можливість його використання при розвитку системи. На основі завдання було розраховано пропускну здатність та обраний необхідний тип оптичного кабелю.

Література:

1, Н.И. Горлов «Оптические линии связи и пассивные компоненты ВОСП» - Новосибирск 2003.-229 с.

УДК 621.391

АНАЛІЗ ПЕРСПЕКТИВ ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ДОСТУПУ

Миронов О. М.

*Державний університет інтелектуальних технологій і зв'язку
oleolemironov@mail.ru*

Науковий керівник – Проф Бондаренко О.В.

У роботі аналізується процес розвитку мереж доступу в Україні, дається аналіз перспектив розвитку різних технологій доступу щодо їхнього застосовуються для розгортання мереж доступу.

Масштабне проникнення інформаційних сервісів та послуг у повсякденне життя людини та економічні процеси призводять до їх інтеграції з традиційними бізнес_процесами та, як наслідок до розвитку нових моделей надання традиційних послуг – телемедицини, електронної комерції, інтернет-банкінгу, електронного уряду, віртуальних турів, дистанційної освіти, тощо. Очевидно, що для того, щоб мати можливість користуватися означеними сервісами потрібно мати стабільний та швидкісний доступ до мережі Інтернет. Виходячи з цього, можна сказати, що питання створення мереж доступу є актуальним для операторів зв'язку. Сучасні мережі доступу створюються з використанням технологій доступу, які поділяються на три групи [1]: – мідні технології доступу ; – безпроводні технології доступу; – оптичні технології

доступу. Мідні технології доступу представлені в Україні сімейством технологій xDSL, технологіями DODSIS (використовують мережі кабельного телебачення), безпроводовий технології – це технології 3G/4G(LTE) та WI-FI, а оптичні технології концепціями AON та PON. Загальна кількість абонентів, що мають швидкісний доступ до мережі Інтернет у першому півріччі 2019 року склала близько 25,4 млн. Найбільшу частку складають абоненти, які отримують доступ до мережі Інтернет через безпроводові канали зв'язку – близько 68% [2], частка абонентів що використовують проводові технології становить 32%. Статистичні дані свідчать, що подальший ріст числа користувачів, які використовують безпроводовий доступ буде обмежений, тоді як потенціал проводового доступу оцінюється у 10-12 мільйонів потенційних абонентів [3]. При виборі технології доступу, оператор приймає до уваги, в першу чергу, наступні фактори: економічний, топографічний та можливість використання вже існуючої інфраструктури. Фактор використання існуючої інфраструктури фактично впливає на економічний фактор, тобто на об'єктивні показники економічного розвитку оператора, які обумовлюють можливість вкладати кошти в оновлення інфраструктури, її модернізацію. Топографічний фактор визначає можливість використання тієї чи іншої технології у районі де планується створення мережі доступу.

Як ми вже зазначали вище, безпроводові технології досягли зони насичення і останнім часом, в Україні стала спостерігатися тенденція скорочення мереж на базі технологій мідних кабелів та збільшення мереж доступу на базі оптичних технологій (рис. 1). Оцінимо перспективи використання різних проводових технологій доступу в Україні. Для цього скористаємося підходом запропонованим в роботі [3]. В якості інтервалу спостереження оберемо інтервал у 3 роки, а в якості стартової точки – 2013 рік. Отже, інтервали спостереження – 2013, 2016 та 2019 роки. У табл. 1 наведено відсоток абонентів, які були підключені за допомогою різних технологій [2].

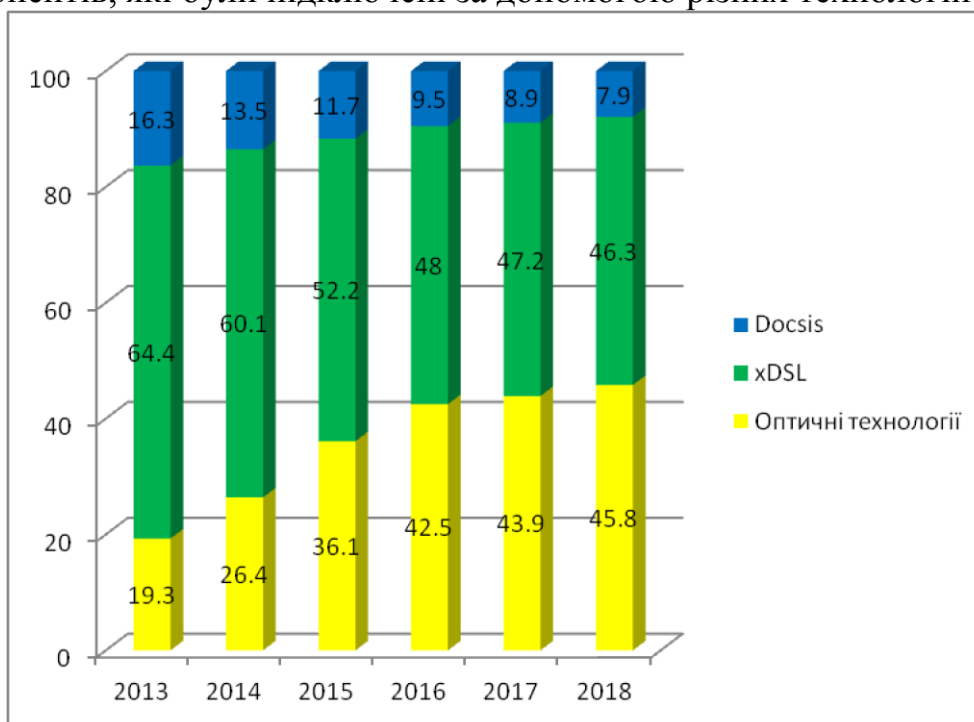


Рисунок 1 – Популярність проводових технологій доступу в Україні

Таблиця 1 – Динаміка зростання числа абонентів підключених провідними технологіями

ік	Оптичні технології (PON, AON) число абонентів, тис.	Мідні технології (xDSL + DOCSIS) число абонентів, тис.	Число потенційно можливих абонентів, тис.	% співвідношення	
				Оптичні технології (PON, AON)	Мідні технології (xDSL + DOCSIS)
013	295	3730	49400	0,6	7,6
016	1072	3350	48500	2,2	6,9
019	2560	2620	45100	5,67	5,8

Відповідно до алгоритму з [3] отримуємо, що період переходу до області насичення для оптичних технологій буде становити $T_p \approx 6,5$ років, тоді сама точка входження до області насичення є $T_\omega = 2016 + 6,5 = 2023$ рік. Для мідних технологій спостерігається негативна динаміка, а отже точка переходу до області стагнації буде становити $T_p \approx 12$ років, тоді сама точка входження до області стагнації є $T_\omega = 2016 + 12 = 2028$ рік.

Отже, можна стверджувати, що при плануванні розвитку мереж доступу найбільш доцільними є використання в якості провідних технологій доступу доцільно застосовувати оптичні технології. Існуючі мідні технології демонструють стабільний спад і за прогнозами у 2028 році повністю перейдуть у зону стагнації.

Список використаної літератури:

1. Маколкіна М.А. Развитие услуг дополненной реальности в рамках концепции тактильного интернета / М.А. Маколкіна // Электросвязь. – 2017. – №2. – С. 34-38.
2. Recommendation J.301 Requirements for augmented reality smart television systems. Telecommunication Standardization Sector of ITU, Geneva, 2014
3. Ganapati, Priya. "How it Works: Augmented Reality." Wired. Aug. 25, 2009. <http://www.wired.com/gadgetlab/2009/08/total-immersion/>

ВИДИ ЗАГРОЗ ДЛЯ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

*Костюк Каріна Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій*

Телекомунікаційні мережі є важливою частиною повсякденного ведення бізнесу та надання основних державних послуг у всьому світі. Однак протягом останнього десятиліття виникали занепокоєння щодо безпеки цих мереж та їх здатності працювати з порушенням роботи. Підприємства, державні установи, охорона здоров'я та соціальна інтерактивність цілих країн покладаються на основні телекомунікаційні послуги, такі як телефони та

Інтернет-послуги, що надаються мережевими провайдерами. Існує ряд природних, ненавмисних та зловмисних загроз, що виникають у різних сферах телекомунікаційної мережі, включаючи фіксовану, мобільну, підводну та супутники.

1. Зловмисні напади на телекомунікаційні мережі включають викрадення мережевого обладнання, вандалізм, шпигунство або тероризм.

- Викрадення кабелів - мідні кабелі часто викрадають із незахищених частин мережі, оскільки це розглядається як цінна і проста мішень для злодіїв. Оскільки кабельні посилення зазвичай не захищені, їх часто легко отримати та видалити. Відповідно до звіту Openreach, викрадення металу з усіх секторів коштує лише британської економіки 770 мільйонів фунтів стерлінгів на рік.

- Пошкодження кабелю - підводна кабельна мережа включає кілька кабелів, які прокладені через одну географічну точку, навмисне націлювання на ці ділянки мережі може призвести до пошкодження кабельних мереж, що може призвести до відключення послуг. Зловмисні атаки на підводні кабелі трапляються рідко, проте підводні човни або кораблі можуть навмисно перетягувати якір уздовж морського дна, намагаючись пошкодити кабельні зв'язки.

- Перешкодження сигналів - можна перешкодити мобільним та супутниковим сигналам за допомогою перешкод, які передають радіосигнали, щоб їм заважати. Пристрої варіюються від ручних глушителів, які можуть досягати десятків метрів, до інструментів промислового масштабу, здатних порушувати сигнали на відстані до 750 метрів.

2. Несвідомі загрози

- Збій у системі - несправності апаратного та програмного забезпечення часто зустрічаються в телекомунікаційних мережах. Погане планування, яке призводить до того, що телекомунікаційні продукти не підтримуються, а запасні частини недоступні, може розглядатися як загроза критичній телекомунікаційній інфраструктурі.

- Збої в живленні - живлення мереж є життєво важливим для безперебійної роботи. Якщо системи електропостачання не резервуються, а сейфові сейфи не встановлюються у разі відключення електроенергії, цілі ділянки мереж можуть випасти.

- Випадкові пошкодження кабелю - Як описано вище, пошкодження кабелю може спричинити значні збої в роботі мереж, але може бути, що заподіяна шкода є випадковою. Операторам важливо переконатися, що навіть коли кабельні мережі надійно захищені, можливість випадкових пошкоджень максимально обмежена.

3. Природні небезпеки

Погана погода, така як повені, вітри та спекотна чи холодна погода, може спричинити порушення роботи телекомунікаційних систем. Операторам потрібно забезпечити, щоб було зроблено все для того, щоб їхня інфраструктура була максимально захищена.

4. Кіберзагрози

Багато персональних даних зберігається в базах даних телекомунікаційних компаній, що зробило їх мішенню для кіберзлочинності, особливо за останнє десятиліття. Існує низка кіберзагроз для телекомунікаційної інфраструктури, які можуть не тільки зробити дані вразливими, але й потенційно спричинити збій у роботі мереж.

- Компрометація пристроїв - пристрої, що використовуються в різних областях телекомунікаційної мережі (наприклад, маршрутизатори), вразливі до кібератак. Хакери можуть здійснювати атаки, часто анонімно, для доступу до служб. Прикладом уразливості пристроїв може бути ланцюг поставок (те, що нещодавно потрапляло у заголовки у всьому світі, коли різні уряди занепокоєні безпекою телекомунікаційних продуктів Huawei).

- Напади людини посередині - спілкування між двома сторонами може бути вразливим для перехоплення третьою стороною. Інформація могла бути записана, зібрана і навіть змінена зловмисником.

- Спадкові протоколи - якщо на продуктах всередині телекомунікаційної мережі все ще працює застаріле програмне забезпечення, яке не було розроблене для того, щоб витримати будь-яке або все вищезазначене, тоді обладнання буде вразливим для більш сучасних, складних технологій.

Електронні ресурси

1. <https://www.carritech.com/news/telecommunication-network-security/> (дата звернення: 17.04.2021)
2. https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-SEC-2015-PDF-E.pdf (дата звернення: 18.04.2021)

ПРОБЛЕМИ РОЗВИТКУ 5G МЕРЕЖ

Ткачук Владислав Ігорович

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

За останні десятиліття бездротові технології досягли значних успіхів. За першим поколінням слідували друге і третє покоління (послуги голосового зв'язку, обміну повідомленнями та доступ до Інтернету), а потім четверте покоління (4G або Long Term Evolution (LTE)) із потоковим передаванням відео. Очікується, що п'яте покоління (5G) стане доступним у всьому світі вже зовсім скоро. Незважаючи на оптимістичні передбачення експертів, є доцільним виокремити деякі проблеми розвитку технологій п'ятого покоління.

5G пропонує значне збільшення швидкості та пропускної здатності, але його більш обмежений діапазон вимагатиме подальшого розвитку інфраструктури. Містам, ймовірно, доведеться встановити додаткові ретранслятори, щоб розповсюдити хвилі на більший діапазон, одночасно підтримуючи незмінну швидкість у більш щільних районах населення. Це означає, що в майбутньому модеми та Wi-Fi маршрутизатори можуть бути замінені на інше обладнання 5G. Щоб забезпечити підключення 5G для свого

дому та бізнесу, потрібно буде покінчити з дротовим Інтернетом, яким ми використовуємо сьогодні. Розширення доступу до сільських районів стане такою ж проблемою, як і впровадження LTE.

5G має доволі складну архітектуру мережу. Для забезпечення успішного розгортання 5G як в основній мережі, так і в мережі RAN, критично важливо розробити архітектуру, пов'язану з IT, а також платформи для її підтримки. Бездротова архітектура 5G не така проста, як може здатись на перший погляд. Багата функціональна структура робить її більш складною, ніж будь-коли, тому для роботи з такою мережею необхідний досвідчений персонал, який добре знає цю технологію.

Враховуючи всі загальновідомі факти, можна зробити логічний висновок, що вартість побудови мереж 5G буде дуже дорогою, адже це не просто побудова шару поверх існуючої мережі - це закладення фундаменту для нових технологій. За даними мобільного оператора Heavy Reading 5G Capex, загальний обсяг глобальних витрат на 5G досягне 88 млрд. доларів до 2023 року.

Не варто виключати загрозу безпеки та конфіденційності. Це може бути проблемою для будь-якої сучасної технології і 5G аж ніяк не стане винятком. Зважаючи на тенденції росту кібератак, можна зроби припустити, що новітня технологія буде боротися як зі стандартними, так і з складними загрозами кібербезпеки. Група дослідників виявила проблеми з протоколом безпеки 5G, відомим як Угода про автентифікацію та ключі (АКА). Він повинен гарантувати, що пристрій і мережа 5G можуть автентифікувати один одного, зберігаючи конфіденційний обмін даними та зберігати особисті дані та місцезнаходження користувача. Однак дослідники кажуть, що в теперішньому стані АКА не спроможний виконати це на даний момент.

Електронні ресурси:

1. http://www.heavyreading.com/details.asp?sku_id=3568&skuitem_itemid=1789
2. <https://www.informationweek.com/strategic-cio/security-and-risk-strategy/the-security-missing-from-5g/d/d-id/1333230>

МЕРЕЖІ ОПЕРАТОРІВ

*Пузирьов Володимир Анатолійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Оператором мережі (Network Operator) називається компанія, яка є власником телекомунікаційної інфраструктури та бере на себе всі витрати щодо забезпечення її працездатності з заданим рівнем якості обслуговування. Її ще називають мережевим оператором, або просто оператором. Кінцевим продуктом діяльності мережевого оператора є надання послуг з транспортування інформації його мережею. Ці послуги називаються телекомунікаційними послугами (Telecommunication Services) та надаються як кінцевим користувачам мережі, так і іншим мережевим операторам, забезпечуючи їх транзитною можливістю з передачі трафіку через свої мережі.

У зв'язку з цим мережі операторів прийнято називати телекомунікаційними мережами («теле-» в перекладі з давньогрецької означає «далеко»). Їх основним завданням є забезпечення можливості віддалено розташованих об'єктів обмінюватися інформаційними повідомленнями.

Створюючи мережу загального користування, оператор зобов'язаний забезпечити в будь-якому місці мережі, до якого під'єднано кінцеві пристрої, стандартний інтерфейс (точку з'єднання).

Розрізняють операторів фіксованого та мобільного (стільникового) зв'язку.

Оператори фіксованого зв'язку (Fixed Communication Operators) організовують стаціонарні мережі, в яких комунікаційне обладнання та пристрої користувачів розміщуються в стаціонарних пунктах мережі.

Оператори мобільного зв'язку (Mobile Communication Operators) створюють мережеве покриття території, розміщуючи свої базові станції за стільниковою схемою в стаціонарних або рухомих пунктах, забезпечуючи тим самим можливість вільного переміщення абонентів у зоні покриття.

Серед основних тенденцій розвитку ринку стільникового зв'язку найприкметнішою є поява так званих віртуальних операторів (Virtual operators). Це компанії, які не мають власних мережевих ресурсів, займаються в основному маркетинговою діяльністю й у вигляді пакетів популярних послуг на основі гнучкої тарифної сітки реалізують їх клієнтам під своєю торговою маркою. Реалізацію ж послуг виконує мережевий оператор, з яким віртуальний оператор вступає у договірні відносини з частковою участю в прибутку від 25 продажу послуг. Оператор, якому належить мережеве обладнання, при цьому повністю зосереджує свою діяльність на підтримці високого рівня його працездатності.

У період лібералізації ринків основні інтереси всіх операторів зосереджуються на пошуку нових ринкових форм комплексних рішень щодо розширення послуг, які надаються користувачам. Для операторів фіксованих мереж таким рішенням є надання мобільного доступу своїм абонентам. Операторові мобільного зв'язку фіксована мережа дозволяє стати постачальником повного набору послуг. Доступність комбінації мобільного та фіксованого доступу, надання широкосмугового доступу, а також послуг передачі даних забезпечують ідеальні умови виживання операторів зв'язку в умовах високої конкуренції на ринку телекомунікацій.

Література:

1. Vorobiyenko P.P. Telekomunikatsijni ta informatsijni merezhi. <https://ktpu.kpi.ua/wpcontent/uploads/2014/02/>

ВПЛИВ COVID-19 НА СФЕРУ ТЕЛЕКОМУНІКАЦІЙ

*Кравченко Ростислав Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій*

Вплив COVID-19 відчуваються у всьому світі та вносить свої корективи в підсектор телекомунікацій. Оскільки все більша кількість країн вводить обмеження на пересування, люди проводять більше часу вдома для роботи та відпочинку та використовують значно більший обсяг даних в мережі.

Телекомунікаційні компанії зосереджені на підвищенні стійкості мережі та вивчають, як COVID-19 впливає на їх заплановані інвестиції, особливо в 5G. Телекомунікаційні компанії також вносять зміни на користь споживачів, котрі в цей час як ніколи потребують мережевих послуг. У деяких країнах дані використовуються як інструмент для відстеження та стримування поширення вірусу.

Використання мережі та стійкість:

- Багато телекомунікаційних компаній повідомляють, що використання мережі стрімко зростає. У деяких країнах обсяг голосових дзвінків також збільшується в геометричній прогресії.

- Надійність мережі є основною метою сьогодення. У мережевій інфраструктурі в Європі спостерігається велика кількість розривів з'єднань, знижена якість звуку та знижений рівень з'єднання. Європейський Союз намагався пом'якшити потенційні відключення, попросивши трансляційні служби обмежити якість зображення.

- COVID-19 також веде до співпраці, яка могла бути немислимою кілька тижнів тому. Наприклад, оператори в США збільшують потужність, позичаючи спектр у конкурентів.

Зміни для замовників телекомунікаційних послуг:

- По всьому світу телекомунікаційні компанії вживають різноманітних заходів для покращення взаємодії з клієнтами та надання людям доступу до мережевих послуг. У Великобританії телекомунікаційні компанії збільшили потужність мережі, пропонують необмежену кількість хвилин та надають анонімізовані дані для допомоги у відстеженні поширення COVID-19.

- Телекомунікаційні компанії також пропонують мережеві інструменти безкоштовно або за меншими витратами, щоб допомогти клієнтам працювати вдома. Подібним чином платформи продуктивності праці запускають рекламні пропозиції, щоб охопити новостворений попит.

- З закритими магазинами по всьому світу телекомунікаційні компанії пристосовуються до нових способів продажу продуктів та надання послуг споживачам, при цьому самообслуговування стає все більш важливим.

- Випуск нових смартфонів може бути відкладений через обмеження поставок.

Як висновок можемо зазначити, що лідери телекомунікаційних служб визначатимуться тим, що вони роблять у трьох напрямках боротьби з кризою: реагують, відновлюються та процвітають.

Ключовими практичними кроками в часи кризи створеної COVID-19 є:

- Перевірити надійність мережі в роботі з великим навантаженням
- Переконатись, що колл-центри обладнані для збільшення обсягу звернень
- Врахувати вплив державних обмежень на телекомунікаційні компанії
- Оцінити можливості для більшої автоматизації надання послуг клієнтам

Електронні ресурси:

1. Understanding COVID-19 - <https://www2.deloitte.com/global/en/pages/about-deloitte/articles/the-heart-of-resilient-leadership.html>

РОЗВИТОК ТЕЛЕКОМУНІКАЦІЙ

Грищенко Ольга Юріївна

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

Телекомунікаційний ринок є одним з найбільш перспективних і швидко зростаючих напрямків галузі зв'язку. В даний час система телекомунікацій знаходиться на шляху швидкого розвитку, в цілому орієнтована на вхід російської системи зв'язку в світову як рівноправного партнера для надання послуг міжнародного, міжміського, міського зв'язку, передачі даних, інтернету, мобільного зв'язку та ін.

Перспективи розвитку нашої цивілізації багато в чому залежать від того, наскільки швидко і адекватно людство проникне в сокровенні таємниці інформації, усвідомлює переваги і небезпеки, пов'язані зі становленням суспільства, заснованого на виробництві, розповсюдженні та споживанні інформації і званого інформаційним. Суть змін, що відбуваються, що охопили сферу діяльності людини, в самому загальному вигляді полягає в тому, що матеріальна складова в структурі життєвих благ поступається місцем інформаційної.

В Україні успішно працюють ряд фірм. Так, наприклад, фірма «АТРАКОМ» побудувала біля 20000 км ліній ВОЛЗ і поставляє користувачам оптичні тракти. Але ряд фірм допускають, як конкуренти, неетичні дії. Вони не мають суттєвого контролю з боку держави за системним розвитком і доходять до пошкоджень ліній ВОЛЗ конкурентів.

Оцінка розвитку різних країн світу за індексом NRI (Networked Readiness Indeks) ведеться з 2002 року. У першому звіті WEF (Всесвітній економічний форум), в якому була застосована методика NRI, за 2002-2003 роки було зібрано і проаналізовано показники розвитку ІКТ-сфери 82-х країн світу. Для України тоді індекс NRI склав 2,98 і вона тоді зайняла 70-те місце у рейтингу за значенням NRI. Перше місце у цьому рейтингу посіла Фінляндія з NRI=5,92. У звіті WEF за 2006-2007 роки ІКТ-сферу України оцінено вже значенням NRI=3,46 і вона зайняла 75 місце з 122-х країн світу. Перше місце діталось

Данії з NRI=5,71. У останньому звіті WEF за 2008-2009 роки Україна отримала оцінку NRI=3,88 і зайняла 62-ге місце у рейтингу серед 134 країни світу. Перше місце зайняла Данія з NRI=5,85.

Проблематика розвитку телекомунікацій в Україні. Наприкінці ХХ ст. – початку ХХІ ст. світ перебуває в стані інформаційної революції, вплив якої можна порівняти з впливом індустріальної революції минулого століття. Є всі підстави вважати, що обробка інформації – одна з найвагоміших складових економічної активності. Тому можна стверджувати, що розвиток телекомунікацій як важлива складова інформатизації суспільства та забезпечення населення високоякісними послугами зв'язку є одним з найважливіших напрямів національного та економічного розвитку будь якої держави, і, зокрема, України. Протягом останніх років сфера телекомунікацій в Україні зберігає позитивну динаміку розвитку, незважаючи на кризові явища в економіці, але в Україні залишається невирішеною проблема телефонізації населення, особливо в сільській, гірській місцевостях та віддалених районах.

Отже, на наших очах відбувається справжнісінький комунікаційний вибух, цілком порівнянний за масштабами і наслідками з тим, що був викликаний появою перших персональних комп'ютерів. Просте і ефективне пристрій - модем, що об'єднує потенціал двох найбільших винаходів людства, телефону та персонального комп'ютера, дає всім бажаючим доступ до неймовірних обсягів інформації і наділяє скромний персональний комп'ютер воістину фантастичними можливостями. Загальна комп'ютерна грамотність, про яку ми мріяли ще зовсім недавно, тепер - більш-менш доконаний факт. Немає ніякого сумніву в тому, що телекомунікаційна грамотність потрібна зараз нітрохи не менше: без неї просто немислимо встигнути за цивілізованим світом ні в бізнесі, ні в науці, ні в освіті, ні в багатьох інших областях. Вже зараз відсутність модему порівняно з відсутністю принтера - і те й інше значною мірою позбавляє комп'ютер сенсу. І не за горами той час, коли від самотнього комп'ютера буде не більше користі, ніж зараз від мікрокалькулятора.

Список використаної літератури:

1. Світові тенденції розвитку засобів телекомунікації. <http://ua-referat.com/>
2. Стан та розвиток телекомунікацій в Україні. <http://shag.com.ua/>

РОЗВИТОК МЕТОДІВ ШИРОКОСМУГОВОГО РАДІОДОСТУПУ У WAN МЕРЕЖАХ

Стрельцов С.А., Макаренко А.О.

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

В цій роботі описано стан технологій широкосмугового бездротового доступу та зусилля, які робляться відомими організаціями зі стандартизації, щоб матеріалізувати бачення і виконати завдання для наступного покоління систем широкосмугового радіодоступу.

Найбільш важливі заходи в цій області проводяться Інститутом інженерів з електротехніки та електроніки і Проектом партнерства третього покоління. Бездротові і мобільні технології пережили експоненціальне зростання за останнє десятиліття. Фактично, стільникові мережі пережили технологічну революцію чотирьох поколінь, а саме від 1G до 4G [1].

Технології бездротового широкосмугового доступу забезпечують повсюдний широкосмуговий доступ для мобільних користувачів, дозволяючи споживачам користуватися широким діапазоном мобільності і різноманітністю бездротових мультимедійних послуг і додатків. Технології широкосмугового бездротового доступу забезпечують широкосмуговий доступ до даних через бездротові носії для споживчих і промислових ринків [2]. Найбільш поширеним прикладом широкосмугового бездротового доступу є бездротова локальна мережа (LAN). Вони в даний час готові доповнити провідні мережі як в більшості розвинених, так і в багатьох країнах, що розвиваються. Основна мета переходу до іншої технології - запропонувати значне поліпшення продуктивності за рахунок надання бездротових пристроїв доступу до Інтернету та мультимедійних додатків ефективним чином, поліпшення послуг безпеки, визначення набору поліпшень якості послуг, серед іншого.

Були продовжені зусилля щодо забезпечення повсюдного широкосмугового бездротового доступу шляхом розробки і впровадження передових технологій радіодоступу, таких як 3GPP UMTS і LTE, а також мобільних систем WiMAX. Широкосмуговий бездротовий доступ також є привабливим варіантом для мережевих операторів в географічно віддалених районах з відсутністю провідної мережі або з обмеженою провідною мережею. Переваги з точки зору економії в швидкості розгортання та витрат на установку є додатковим стимулом для технологій широкосмугового бездротового доступу.

Література:

1. Wireless and mobile technologies and protocols and their performance evaluation / URL: <https://www.sciencedirect.com/science/article/pii/B9780128008874000018> (дата звернення 19.04.21).
2. Broadband wireless network technologies: current performance benchmarks and future potentials / URL: https://www.researchgate.net/publication/331977070_broadband_wireless_network_technologies_current_performance_benchmarks_and_future_potentials (дата звернення 19.04.21).

ПЕРСПЕКТИВИ ТА РОЗПОВСЮДЖЕННЯ ТЕХНОЛОГІЇ FTTH ТА ЇЇ РІЗНОВИДІВ

*Хорошилов І.В., Макаренко А.О.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

«Fiber to the Home» (FTTH) означає використання волоконно-оптичного кабелю для доставки широкосмугового Інтернет-з'єднання з центрального місця безпосередньо до дому. У мережі FTTH оптичне волокно використовується

протягом останньої милі, витісняючи DSL або коаксіальні дроти з меншою пропускною здатністю [1].

«Волокно до дому» - це одна ітерація категорії «FTTx», яка визначає будь-яку конструкцію широкосмугової мережі, яка підключає оптичне волокно безпосередньо до певної точки закінчення. Інші варіанти включають волокно до приміщення (FTTP), волокно до будівлі (FTTB) та волокно до кабінету (FTTC).

Завдяки FTTH власники будинків отримують швидший Інтернет та збільшують пропускну здатність. Вони можуть передавати данні з більшою якістю і мати більше пристроїв, одночасно підключених до Інтернету. Крім того, користувачі можуть отримати Інтернет та телевізійні послуги через одне і те ж широкосмугове з'єднання [2].

FTTH є привабливим рішенням для будівельників мереж, оскільки основна волоконна технологія є «доказом майбутнього», тобто вона зможе задовольнити вимоги до широкосмугового зв'язку в найближчому майбутньому. Волоконні кабелі мають практично необмежену пропускну здатність. Порівняно з іншими типами широкосмугового з'єднання, FTTH є набагато ефективнішим методом доставки цифрових даних на великі відстані.

Через основну волоконно-оптичну кабельну технологію FTTH пропонує більш високу швидкість з'єднання та майже необмежену пропускну здатність приблизно за однакову вартість. Волокно може нести в 10 разів більше даних, ніж мідь, основний матеріал, який використовується в цифрових абонентських лініях (DSL). У майбутньому, коли попит на Інтернет продовжує зростати в геометричній прогресії, нам знадобиться ця спроможність, щоб уникнути великих вузьких місць у широкосмуговій мережі. Волокно також може передавати інформацію в 400 разів далі і в 10 разів швидше, ніж мідні дроти. З цієї причини волокно вже стало інфраструктурою, завдяки якій сьогодні стільки інформації подорожує по всьому світу. У порівнянні з міддю, волокно набагато безпечніше, надійніше та довговічніше. Оскільки волоконні кабелі передають інформацію через електричні імпульси, вони не сприйнятливі до прослуховування. Вони також стійкі до електричних шумів, перешкод та стрибків напруги. Крім того, волоконно-кабельні кабелі розраховані на 30-50 років.

Сьогодні більшість абонентів мають високошвидкісний Інтернет із підтримкою FTTH. Розширення волоконної мережі стане ключем до підтримки технологій наступного покоління вдома. Протягом наступного десятиліття Інтернет речей та додатки III надзвичайно зростатимуть, що змусить мережевих операторів ширше використовувати волокно.

Література:

1. Fiber To The Home. The Ultimate Guide / URL: <https://get.ospinsight.com/the-ultimate-guide/fiber-to-the-home> (дата звернення 19.04.21).
2. Fiber Broadband Association / URL: <https://www.fiberbroadband.org/> (дата звернення 19.04.21).

ОСОБЛИВОСТІ ПРОЕКТУВАННЯ МЕРЕЖ VANET

Домрачева Катерина Олексіївна

Богдан Наталія Володимирівна

Пукало Микола Іванович

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій

В останні роки системи автомобільного зв'язку привертають все більше уваги, в основному зростаючим інтересом до інтелектуальних транспортних систем (ІТС). Інтелектуальні транспортні системи – це розвиток телекомунікаційних та інформаційних технологій в транспортній системі для підвищення безпеки та ефективності транспортних систем. Ці системи спрямовані на вирішення критичних питань, таких як безпека пасажирів та затори на дорогах, шляхом інтеграції впровадження інформаційних та комунікаційних технологій в транспортну інфраструктуру та транспортні засоби [1].

Вони побудовані на основі самоорганізованих мереж, відомих як автомобільні самоорганізовані мережі (VANET), що складаються з мобільних транспортних засобів, з'єднаних бездротовим з'єднанням. На даний момент існують рішення, які базуються на використанні традиційних архітектур багаторівневих систем зв'язку (OSI модель), але вони часто не вирішують фундаментальних проблем, наприклад, динамічної зміни топології мережі. Крім того, багато ІТС додатків висувають суворі вимоги до QoS, які не виконуються.

Для обслуговування широкого класу додатків ІТС підтримує два види бездротового зв'язку: дальнього та ближнього діапазону. Зв'язок на великих відстанях в основному покладається на існуючі інфраструктурні мережі, такі як стільникова мережа. З іншого боку, зв'язок ближнього радіусу заснований на нових технологіях, таких як варіанти 802.11, для формування мобільних спеціальних мереж VANET, що складаються з мобільних автомобілів та стаціонарного придорожнього обладнання.

VANET підтримує два типи зв'язку: зв'язок між транспортними засобами (V2V) та зв'язок між автомобілем та фіксованою інфраструктурою, яка встановлена уздовж дороги (V2I).

Транспортні мережі VANET схожі з MANET (мобільні Ad hoc мережі) з точки зору самоорганізації, самоналаштування та низької пропускну здатності. Тим не менш на відміну від MANET, топологія мережі в автомобільній мережі працює дуже динамічно через швидкий рух автотранспорту, а топологія часто обмежується структурою дороги. Крім того, автомобілі можуть зіткнутися з великою кількістю перешкод, такі як світлофори, будівлі або дерева, в результаті спостерігається погана якість каналу та можливість відключень. Отже, протоколи розроблені для традиційних MANET, не можуть забезпечити надійну, високу пропускну здатність та невелику затримку в мережах VANET.

Таким чином, існує гостра потреба в ефективних протоколах, які враховують специфіку автомобільних мереж.

Ефективне вирішення цих питань вимагає інформації про обмін даними між рівнями OSI, щоб можна було спільно оптимізувати різні рівні для досягнення кращої пропускну здатності та мінімальну затримку передачі. Наприклад, протокол може використовувати інформацію, отриману з фізичного рівня та MAC, такі як рівні шуму та перешкоди для знаходження стабільних та оптимальних маршрутів.

Фізичний рівень пов'язує кілька транспортних засобів всередині радіусу дії бездротового каналу. Рух транспортних засобів та перешкоди навколишнього середовища впливають на стабільність бездротового зв'язку. Таким чином, багато міжрівневих рішень надають можливість фізичному рівню спостерігати за станом каналу та передавати повідомлення, коли поточний стан каналу знаходиться в задовільному стані.

Наприклад, адаптація швидкості передачі - це можливість регулювання швидкості модуляції, з якої пакети передаються в залежності від параметрів каналу, таких як відношення сигнал шум (SNR) та коефіцієнту втрати пакетів. Маючи можливість вибору частоти модуляції можливо впливати на продуктивність зв'язку. Інформація про стан каналу зворотного зв'язку корисна для підвищення продуктивності.

Згідно протоколів заснованих на втраті передавачі визначають швидкість втрати пакетів, просто відстежуючи прийом кадрів пакета передачі на рівні MAC. [2]. Якщо АСК отриманий до закінчення тайм-ауту, то передача вважається успішною. Поява тайм-ауту в протоколі MAC під час передачі вказує що процес доставки пакета не вдался. Ці результати доставки пакетів агрегуються в базі даних, яка розділяється між фізичним рівнем та MAC рівнем. Потім кожен вузол визначає відповідну швидкість модуляції.

В автомобільних мережах мобільність транспортних засобів часто обмежується топологією основної дорожньої мережі, особливо на автомагістралях. Завдяки такому просторовому співвідношенню транспортних засобів на дорогах багато стрибкове пересилання пакетів є одним з перспективних рішень, яке може використовувати автомобіль для спілкування з іншими транспортними засобами та елементами інфраструктури, які поза його діапазоном передачі. Наприклад, автомобіль може пересилати свої пакети на базову станцію, щоб отримати доступ в Інтернет, навіть коли він їде від базової станції. Оскільки WiMax має дальність зв'язку до 50 км та швидкість до 1 Гбіт/с, автомобілі з WiMax потенційно можуть діяти як транспортні засоби-ретранслятори (RV), де вони можуть використовуватись в пересиланні пакетів на великі відстані з невеликою затримкою. Таке рішення дешевше, ніж інші методи, такі як розгортання великої кількості базових станцій по дорозі. Однак проблема з цим підходом полягає в тому, що для використання WiMax має бути великогабаритний автомобіль.

Автомобільна схема швидкої передачі обслуговування (VFHS) пропонує зустрічним бічним транспортним засобам надавати інформацію про канал і

місцезнаходження нових великогабаритних автомобілей з WiMax з відключеними автомобілями.

Оскільки VFHS - це додаток та обладнання, то успіх використання великогабаритний автомобілей для цієї мети в основному залежить від розповсюдження технології WiMax.

Мобільність транспортних засобів впливає на можливість підключення вузлів VANET. У розріджених мережах ця проблема стає набагато серйознішою, може викликати значну втрату пакетів. В таких сценаріях збільшується пропускна здатність передачі пакетів, поки не зустрінеться наступний вузол ретрансляції або пункт призначення. Цей механізм широко відомий як store-and-forward [3]. Він підходить для додатків, в яких затримка не є критичною. Мати можливість обслуговувати додатки в реальному часі в розріджених мережах, розширення діапазону передачі - одна з можливих стратегій. Однак збільшення дальності передачі має багато інших наслідків. Наприклад, збільшення діапазону передачі може потенційно збільшити перешкоди, які можуть призвести до відкидання пакетів. Таким чином, вигідно збільшувати дальність передачі при низькій щільності транспортного засобу коли наявність перешкод буде невеликою. Альтернативно, діапазон передачі можливо зменшувати, коли щільність автомобілей буде дуже високою. Тут MAC рівень відповідає за збір інформації про сусідів на фізичному рівні для передачі регулювання потужності. Автомобілі в такому випадку повинні мати декілька антен, що тягне за собою підвищення вартості.

Література

1. Intelligent transportation systems (its) data [Електронний ресурс] // ITS Joint Program Office – Режим доступу до ресурсу: https://www.its.dot.gov/factsheets/pdf/FactSheet_EnterpriseData.pdf.

2. J. Camp and E. Knightly, "Modulation Rate Adaptation in Urban and Vehicular Environments: Cross-Layer Implementation and Experimental Evaluation," in *IEEE/ACM Transactions on Networking*, vol. 18, no. 6, pp. 1949-1962, Dec. 2010, doi: 10.1109/TNET.2010.2051454.,

3. Rashmi, K.H., Patil, R. Survey on Cross Layer Approach for Robust Communication in VANET. *Wireless Pers Commun* (2021). <https://doi.org/10.1007/s11277-021-08414-2>

ТЕХНІЧНІ ОСОБЛИВОСТІ ПОБУДОВИ БЕЗПРОВОДОВИХ МЕРЕЖ ЗА СТАНДАРТОМ 802.11

Кулик Олексій Сергійович
Державний університет телекомунікацій

Найбільш істотними перевагами безпроводових мереж у порівнянні з кабельними є: швидке розгортання й масштабування, мобільність для користувачів, простота підключення нових пристроїв. Однак безпроводові мережі не позбавлені ряду недоліків: слабкий захист при передачі сигналу, менша швидкість, висока уразливість від різних джерел радіоперешкод і зловмисників. Все це повною мірою стосується мереж, побудованих з використанням стандарту IEEE 802.11 або Wi-Fi (англ. аббревіатура від Wireless Fidelity – безпроводова висока точність) [1].

При розгортанні Wi-Fi доводиться вирішувати два основних завдання: як забезпечити прийнятну швидкість й як гарантувати надійний захист даних. Саме рішення першого завдання стає актуальним коли мова йде про мережі, у яких попередньо не передбачається обмін конфіденційною інформацією.

При побудові традиційних кабельних мереж чітко визначена ємність: мережа розрахована на число користувачів, рівне кількості портів у комутаторі. В Wi-Fi-мережі число підключень може варіюватися досить широко. При цьому частотний діапазон, у якому передаються дані, є єдиним для всіх. Працюючи в ньому, клієнти очікують своєї черги на передачу даних, і, чим більше їхнє число, – тим менше швидкість передачі інформації. Таким чином, основні проблеми мережі зв'язані зі зниженням швидкості передачі інформації й перебоями сервісу взагалі, особливо якщо до мережі підключається відразу велика кількість клієнтських пристроїв. Крім того, у радіо ефірі може працювати різне обладнання, що створює перешкоди для сервісу.

Хоча принцип побудови мережі на базі технології Wi-Fi однаковий для будь-якого обладнання, у цілому такі мережі можна поділити на два типи: звичайні споживчі й професійні корпоративні. Різниця між ними в особливостях архітектури, аутентифікації, роумінгу, у рівні безпеки, надійності й, звичайно ж вартості точок доступу. Крім високої продуктивності й захищеності, корпоративне Wi-Fi обладнання пропонує додаткові можливості для системного адміністратора. Це централізоване керування, що дозволяє контролювати мережу, відслідковувати спроби злому, вторгнення в мережу. Крім того, професійна мережа реагує на виникнення перешкод й у випадку їхнього істотного впливу перебудовується на інші радіоканали й продовжує функціонувати [2].

У корпоративних безпроводових мережах застосовується інший підхід до інформаційної безпеки, ніж у звичайних споживчих. Якщо у звичайній Wi-Fi мережі використовується загальний ключ, який через певний час знають всі сусіди, а, часом, і зловмисники, то в корпоративній мережі для кожного користувача застосовується персональна аутентифікація, яку він може пройти за допомогою власного ключа.

Крім того, у корпоративних мережах обов'язкове використання двосторонньої аутентифікації (клієнтської й серверної сторони) і надійного рівня шифрування з метою захисту даних від перехоплення й підміни. Також, з метою безпеки, клієнтським пристроям заборонено підключатися до сторонніх Wi-Fi мереж, навіть якщо сигнал корпоративної точки доступу занадто слабкий, а публічна мережа має аналогічну назву й більш потужний рівень сигналу. Для цього використовуються додатки, які вимагають від власника терміналу підтвердження щодо переходу в іншу мережу.

Звичайне споживче Wi-Fi обладнання дозволяє побудувати мережу, яка складається всього з декількох точок доступу. У професійних мережах їх може працювати декілька сотень. При переході користувача із зони дії однієї точки до іншої забезпечується плавний, «безшовний» роумінг.

Процес побудови корпоративної Wi-Fi мережі припускає наступні етапи:
- формування вимог і розробка технічного завдання;

- радіо розвідка існуючої або радіо планування нової безпроводової мережі;
- модернізація або впровадження нового рішення;
- фінальне тестування та введення в експлуатацію.

На першому етапі необхідно сформулювати технічне завдання. Тут потрібно визначити функціональне призначення мережі, проаналізувати поточну ситуацію й потенціал її росту, розрахувати можливі пікові навантаження, а також, урахувати особливості середовища, у якому буде розгорнута мережа. Це етап, від результатів якого залежить успішність впровадження рішення.

На другому етапі виконується комплекс дій по визначенню типів, характеристик і місця розташування точок доступу для забезпечення необхідного безпроводового покриття й рівня сигналу. Для цього виконується моделювання радіо оточення за допомогою спеціалізованих програм і подальша перевірка розрахунків за допомогою реальних вимірів на об'єкті. При виконанні вимірів важливо, щоб об'єкт був на фінальній стадії будівельної готовності й отримані результати максимально відображали результуюче безпроводове покриття після впровадження мережі.

Радіо планування складається з наступних стадій:

- вивчення планів приміщень із вказівкою місць, де необхідно провести виміри, і можливих місць розміщення точок доступу;
- розташування в передбачуваних місцях точок доступу й сканування радіо ефіру з метою визначення характеристик безпроводової мережі;
- підготовка звіту за результатами проведених робіт, що містить у собі карту покриття, рівень інтерференції, шуму й наявність сторонніх перешкод.

Наступний етап – розгортання мережі з монтажем і настроюванням устаткування, після чого рекомендується виконання повторної радіо розвідки для підтвердження бажаного результату. Це також потрібно у випадку модернізації існуючої безпроводової мережі для визначення властивостей мережі, таких як рівень сигналу, інтерференція, співвідношення сигнал/шум, наявність сторонніх безпроводових мереж. Ці дані використовуються як базис для подальших розрахунків.

Wi-Fi мережу досить легко масштабувати за рахунок додавання нових точок доступу або заміни існуючих на більш продуктивні, але це можливо лише у випадку правильного проектування мережі з урахуванням можливого розширення.

При побудові безпроводової мережі важливо правильно розуміти завдання, які будуть покладені на мережу й виконати відповідне проектування. Розповсюджена помилка – невірна оцінка максимального ймовірного числа користувачів. У результаті в момент пікових навантажень мережа може виявитися повністю непрацездатною.

Крім того, при побудові корпоративної Wi-Fi мережі потрібно використовувати не такий підхід до безпеки, як у випадку з мережами публічними. У другому випадку не обов'язково шифрувати трафік користувачів, адже за рахунок економії на шифруванні можна забезпечити

більшу пропускну здатність. У випадку внутрішньої корпоративної мережі шифрування є обов'язковим.

Обов'язковим також є моніторинг мережі, що дозволяє визначити, наскільки «чистим» у цей момент є ефір. Адже може бути так, що в даний момент Wi-Fi працює нормально, а через хвилину в сусідньому приміщенні включили власну точку доступу (або джерело радіоперешкод) і мережа відразу почне працювати гірше. Також необхідне виконання якісного радіо планування для визначення властивостей покриття, оскільки існують зони, де сигнал дуже сильно падає, хоча теоретичні розрахунки говорять про зворотне [2].

У деяких випадках проблему ємності мережі допомагає вирішити перехід у діапазон 5 ГГц, що менш завантажений. Цей діапазон відрізняється від стандартного 2,4 ГГц скороченим радіусом передачі радіосигналу, у той же час тут можна використати більше радіоканалів.

Таким чином, при побудови мережі Wi-Fi необхідно здійснити аналіз її основного призначення, а вже після цього переходити до етапів планування, прогнозування можливої максимальної кількості підключень, аналізу радіо ефіру приміщення і якісної інсталяції обладнання.

Література

1. Педжман Р., Джонатан Л. Основы построения беспроводных локальных сетей стандарта 802.11.: Пер. с англ. – М.: Издательский дом "Вильямс", 2004. – 304 с.
2. Ротач А. Wi-Fi-сеть, которая работает [Електронний ресурс]. – Режим доступу: <http://www.pcweek.ua/themes/detail.php?ID=147992>.

ОГЛЯД І ПОРІВННЯ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ ЗАСТОСОВУВАНИХ В ІОТ

Табор Денис

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Головною тенденцією, притаманною IoT, так само, як і його головною проблемою, є досить швидке збільшення числа кінцевих пристроїв, підключених до мережі. Висока конкуренція між виробниками в сфері Інтернету речей робить взаємодію між інтелектуальними пристроями ще більш складним завданням. Такий стан справ призвів до появи на ринку великої кількості різномірних пристроїв, які не можуть взаємодіяти один з одним, що несприятливо позначається на розвитку галузі в цілому. Відсутність єдиного стандарту і напрацьованих практик безперешкодного і стійкої взаємодії різних пристроїв на даний момент є однією з основних проблем.

Для вирішення проблем стандартизації IoT з'явилися нові типи мереж LPWAN (Low Power Wide Area Networks). Найбільш популярними серед таких технологій є LoRa, SIGFOX, NB-IoT, Weightless P і ін. Їх поява зумовлена необхідністю підключення безлічі приладів обліку і телеметрії для централізованого збору даних на хмарних серверах.

Технологія LORA

Розробники LoRa Alliance вважають, що технологія LoRa має значні переваги перед WiFi і стільниковими мережами, завдяки можливості розгортання межмашинного з'єднань (Machine-to-Machine, M2M) на відстань до 20 км при швидкості до 50 Кбіт / с, а також має мінімальне споживання електроенергії, що забезпечує кілька років автономної роботи на одному акумуляторі типу AA. Масштаб застосувань даної технології великий: від домашньої автоматизації та інтернету речей до промисловості і розумних міст.

Відмінною особливістю LoRa мережі є те, що вона передбачає три класи пристроїв для вирішення різних завдань і застосувань в мережі: клас А (для всіх), класу В і клас С, в залежності від функціонального режиму роботи.

Технологія SigFox

SIGFOX є приватною компанією, яка спрямована на створення всесвітної мережі, спеціально розробленої для пристроїв IoT. Технологія дозволяє здійснювати передачу даних на великі відстані при малій потужності передавального пристрою і малої ємності батареї. Мережа відмінно підходить для простих і автономних пристроїв, які посилають невеликі кількості даних в цю мережу.

Стандарт має ряд переваг в порівнянні з іншими базовими технологіями LPWAN мереж. Це велика зона покриття; високапроникаюча здатність; до 20 років роботи сенсора від 2-х батарей AA; низька вартість. Але також має і негативні характеристики: - низька швидкість передачі даних; - залежність від стільникового інфраструктури; - обмежена стійкість;

Технологія NB-IoT

NB-IoT, він же стандарт LTE-Cat.M2, має ряд переваг таких, як широка зона охоплення, швадка модернізація існуючої мережі, низьке енергоспоживання, який гаранте 10- річний термін служби батареї, низьку вартість терміналу, підвищену надійність і високу мережу операторського класу безпеки. Це бездротова узкополосная різновид глобальних мереж з низьким енергоспоживанням, яка в першу чергу призначена для додатків M2M.

В 3GPP були запропоновані 3 сценарії для розгортання LPWAN NB-IoT: Guard Band (захисна смуга), In Band (в смузі частот) і Standalone (автономний).

Мережа може бути розгорнута як автономний носій Standalone з використанням будь-якого доступного спектра більше 180 кГц. Крім того, мережа може бути в розподілі LTE спектра, або в рамках ширшої несучої LTE In- Band, або в LTE Guard Band - захисній смузі.

Технологія Weightless P

Лідером розробки стандарту Weightless стала промислова IoT компанія Ubiik. Weightless - являє собою відкритий стандарт для мереж LPWAN підвищеної потужності, призначеної для продуктивності мережі. У спеціальній групі інтересів Weightless пропонується три різних протоколу - Weightless-N, Weightless-W, і Weightless-P, які підтримують різні форми і варіанти використання.

Weightless-N робить акцент на надзвичайно широку зону покриття замість високих швидкостей передачі даних. Weightless-N підтримує більший

діапазон і низький енергоспоживання. Ідеально підходить для сенсорних мереж по виміру температури, контролю рівня рідини в резервуарі, вимірювань і багато іншого. Weightless-P це вузькосмугова технологія LPWAN для IoT-рішень, потребуючих високу щільність кінцевих пристроїв, довгострокову службу батареї, і двосторонню зв'язок. Особливостями цієї технології є масштабованість, оптимізація висхідній і низхідній лінії зв'язку, широка зона покриття, тривалий термін служби батареї і безпечна мережа. Він використовує вузький діапазон груп модуляцій, пропонуючи можливість двобічної зв'язку для того, щоб забезпечити неперевершену якість обслуговування (Quality of Service, QoS).

Порівняння технологій мереж дальнього радіусу дії LPWAN

Порівняння технологій мереж дальнього радіусу дії представлені в таблиці. Як видно з таблиці, технології мають високу дальність зв'язку, підвищеної помехозащищенностью, низькою швидкістю передачі даних, низьким енергоспоживанням і, як наслідок, високим ступенем автономності кінцевих пристроїв.

Характеристики	LoRa	SIGFOX	NB-IoT	Weightless P
Метод модуляції	CSS	-	OFDMA/DSSS	FDMA / TDMA
Діапазон	ISM	ISM	Ліцензований	ISM
Швидкість	0,3-50 кбит/сек	100 бит/сек	1-144 кбит/сек 1-200 кбит/сек	0,2-100 кбит/сек (адаптивная)
Полоса	до 500 кГц	100 кГц	200 кГц	12,5 кГц
Автономний час	> 10 років	-	До 10 років	3-5 років
Частота, МГц	868,8/915/433/33МГц	868,8/915	700 / 800 / 900	169/433/470 /780/868/915/923
Безпека	AES-64 и 128 бит	AES с HMACs	-	AES-128 / 256
Дальність	До 2,5 км в городе, до 45 км вне города	До 10 км в місті до 50 км за межами	-	До 2 км в місті
Підтримка	LoRa Alliance, IBM, Cisco, Actility, Semtech...	SigFox, Samsung	3GPP, Ericson, Nokia, Huawei, Intel.	Ubiik Weightless SIG

Аналіз виявив, що у кожній технології є безліч переваг і особливостей і жоден вище розглянутий варіант не може бути залишений осторонь і має місце в сучасному світі технологій.

На сьогодні домінуючою технологією являється LoRaWAN, завдяки високій масштабованості і низьким вартості передатчиків.

Література:

1. Киричек Р. В., Парамонов А. И., Прокопьев А. В., Кучерявый А. Е. Эволюция исследований в области беспроводных сенсорных сетей // Информационные технологии и телекоммуникации. 2014. № 4 (8). С. 29–41. URL: <http://www.sut.ru/doci/nauka/review/4-14.pdf>

2. Кучерявый А. Е., Владыко А. Г., Киричек Р. В., Маколкина М. А., Парамонов А. И., Выборнова А. И., Пирмагомедов Р. Я. Перспективы научных исследований в области сетей связи на 2017–2020 годы // Информационные технологии и телекоммуникации. 2016. Т. 4. № 3. С. 1–14. URL: <http://www.sut.ru/doci/nauka/review/20163/1-14.pdf>

3. Кулик В. А., Киричек Р. В., Бондарев А. Н. Методы исследования беспроводных каналов связи Интернета Вещей в условиях совместной работы // Информационные технологии и телекоммуникации. 2015. № 1 (9). С. 106–114

ОСОБЛИВОСТІ МОБІЛЬНОЇ МЕРЕЖІ П'ЯТОГО ПОКОЛІННЯ (5G)

Пригода А.О.

Державний університет телекомунікацій

Навчально-науковий інститут інформаційних технологій

5G (англ. 5th Generation) — п'яте покоління мобільних мереж або п'яте покоління бездротових систем. Назва, яку використовують у деяких наукових працях та проектах для позначення наступних телекомунікаційних стандартів для мобільних мереж після стандартів 4G/IMT-Advanced.

Передбачено, що 5G забезпечуватиме швидшу передачу даних у порівнянні з 4G, зробить можливим щільніше розташування пристроїв, та надасть можливості для прямої взаємодії між різними пристроями.

Також дослідники прагнуть скоротити затримки та зменшити споживання електричної енергії (важливо для мобільних пристроїв та пристроїв типу «Інтернет речей») у порівнянні з 4G.

Серед іншого, стандарт 5G має забезпечити такі характеристики:

- пікова швидкість завантаження даних на одну базову станцію до 20Гб/с
- швидкість завантаження даних до 100 Мб/с та вивантаження до 50 Мб/с для одного абонента
- можливість абонентському пристрою рухатись зі швидкістю до 500 км/год між базовими станціями (наприклад, у швидкісному потязі)
- можливість пристроям перемикатись між режимом заощадження енергії та повністю робочим за 10 мс
- затримки (англ. latency) до 4 мс за сприятливих умов, і до 1 мс для спеціалізованих з'єднань
- поліпшена ефективність використання радіочастотного спектру
- передача даних зі швидкістю 1 Гб/с водночас для багатьох користувачів на одному поверсі будівлі
- можливість роботи до 1 млн пристроїв на 1 км².

Низькі затримки та висока швидкість передачі даних мереж 5G може стати в пригоді не лише «інтернету речей», а й системам управління безпілотними автомобілями.

Очікується, що бездротова технологія блискавичного інтернету наступного покоління зможе забезпечити не тільки живлення самокерованих автомобілів, а й віртуальну реальність, розумні міста та мережевих роботів.

Зв'язок 5G використовує два діапазони електромагнітних хвиль — FR1 (600–6000МГц) та FR2 (24–100ГГц).

Основна технології

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

Передавання даних радіохвилями у міліметровому діапазоні (буде обраний сегмент у 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 неортогонального множинного доступу (NOMA) та різних варіантів неортогональних за частотою (N-OFDM) сигналів, кодування LDPC.

4 березня 2021 року компанія Samsung встановила новий рекорд швидкості щодо передачі даних в мережі 5G: 5,23 Гбіт/с. Телефон Samsung Galaxy S20+ завантажив 4-гігабайтовий фільм із роздільною здатністю в full-HD за шість секунд.

Список літератури:

1. Старт 5G: переваги над попередниками // <https://www.ukrinform.ua/rubric-technology/2550975-start-5gzvazku-aki-perevagi-nad-poperednikami-ta-koli-ocikuvati-v-ukraini.html>
2. Що таке 5G. // <https://root-nation.com/ua/articles-ua/tech-ua/ua-what-is-5g>

ЗАГАЛЬНІ ВІДОМОСТІ ПРО ЛІНІЇ ЗВ'ЯЗКУ

Салюк Руслан

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Лінії зв'язку призначені для створення каналів зв'язку, що використовуються на різних участках комп'ютерних мереж. Вони складаються з передавача, приймача сигналів та середу передачі. Ця структура така ж сама

як і структура каналу зв'язку, але відмінність у тому що в одній лінії зв'язку може бути створено від одного до декількох тисяч каналів, це залежить від типів передавача, приймача та середі передачі. Канали лінії зв'язку створюються шляхом частотного, часового або кодового ущільнення лінії. Частотне ущільнення використовують при передачі аналогової інформації, наприклад, мовної в телефонних мережах зв'язку. Для організації каналів методом частотного ущільнення всю доступну полосу пропускання лінії розділяють на сектора, які виділені для одного каналу. Між секторами залишають захисні роздільні полоси для уникнення викривлень. Для дискретних каналів зв'язку використовують метод часового ущільнення. Для цього кожному каналу по чергово виділяють окремий часовий проміжок, в якому здійснюється передача сигналів від даного каналу. При кодовому розділенні каналів цифрові сигнали від кожного каналу кодуються індивідуальним кодом, який дає можливість розділити канали на приймальному кінці лінії. Для організації двостороннього каналу необхідно використовувати дві лінії зв'язку. В лінії, яка містить один канал, ущільнення не відбувається бо вона є лінією та каналом зв'язку.

В залежності від довжини лінії зв'язку поділяють на магістральні (5 км і більше) та місцеві. Однак, такий розподіл умовний так як практично є потреба в лініях зв'язку (каналах) будь-якої довжини – від десятків метрів до сотен та тисяч кілометрів. Якщо лінії зв'язку необхідної довжини не існує то створюють складові лінії, які містять апаратуру переприйому. Розглянемо класифікацію ліній зв'язку:

Кабельні лінії являють собою доволі складну конструкцію. Кабель складається з переплетених попарно мідних провідників на яких нанесено декілька шарів ізоляції: електричної, електромагнітної, механічної, а також, можливо, кліматичної. Крім того кабель може бути оснащено роз'ємами які забезпечують швидко виконувати підключення до нього різноманітного обладнання. В магістральних лініях передачі використовують спеціальні багатожильні кабелі, які дозволяють забезпечити багатоканальний телефонний зв'язок та передачу даних на великі відстані. В комп'ютерних мережах використовують три основні види кабелю: кабелі на основі сплетених пар мідних дротів, коаксіальні кабелі з мідною жилою та оптоволоконні кабелі.

1) Сплетена пара дротів називається *вітою парою*.

Віта пара існує в екрануючому варіанті, коли пара мідних дротів обмотується в ізоляційний екран, та в неекранованому, коли екрануюча оболонка відсутня. Сплетення дротів дозволяє компенсувати наводки від зовнішніх перешкод на корисні сигнали, які передаються по кабелю

2) Коаксіальний кабель має несиметричну конструкцію та складається з внутрішньої мідної жили та екрануючою мідною обмоткою, відділеною від жили шаром ізоляції. Існує декілька типів коаксіального кабелю, які відрізняються характеристиками та сферами застосування. Нас цікавлять коаксіальні кабелі для локальних мереж, а також кабелі, призначені для зв'язку прийомних та передавальних пристроїв з антенами

3) Оптоволоконний кабель складається з тонких (5-60мікрон) волокон, по яких розповсюджуються світлові сигнали. Це найбільш якісний тип кабелю – він забезпечує передачу даних на дуже великій швидкості (до 10 гБит/с та вище) до того ж краще інших типів передавального середовища забезпечують захист даних від зовнішніх завад.

Радіолінії наземного та супутникового зв'язку створюються за допомогою передавача та приймача радіохвиль розміщених на Землі чи на ШСЗ. Існує велика кількість різноманітних типів радіоканалів, які відрізняються як використовуваним частотним діапазоном так і дальністю дії. Діапазони коротких, середніх та довгих хвиль, які називають також діапазонами амплітудної модуляції по типу використовуваного в них методу модуляції сигналу, забезпечують дальній зв'язок, але не пристосовані для передачі даних. Більш швидкими є канали, які працюють в діапазонах ультракоротких хвиль, для яких найчастіше використовується частотна модуляція а також в діапазонах надвисоких частот. В діапазонах УКХ та НВЧ сигнали не відбиваються іоносферою землі та не огинають земну кулю, тому для стабільного зв'язку потрібна пряма видимість між передавачем та приймачем. Тому такі частоти використовують в супутникових або радіорелейних лініях, де ця умова виконується

ТЕХНОЛОГІЯ BLUETOOTH 5.2: ОСОБЛИВОСТІ ТА ПЕРЕВАГИ СТАНДАРТУ

*Фенченко Дмитро Васильович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій*

З'єднання Bluetooth дуже поширені в наші дні. Є багато пристроїв, які ми можемо використовувати з бездротовим підключенням завдяки цій технології. Згодом в нові версії внесені важливі зміни, поліпшення і функції, які дозволяють виконувати завдання, які раніше були неможливі або з гіршою продуктивністю.

Найбільш масовим застосуванням Bluetooth сьогодні є бездротове відтворення звуку. Однак до сих пір параметри інтерфейсу не забезпечували вирішальної переваги перед провідним з'єднанням. Високе споживання енергії, низька швидкість передачі даних, яка змушує використовувати кодек SBC, що жорстко компресує сигнал - все це робило бездротові навушники долею невимогливих користувачів. Ізохронні канали (ISOC). Тепер можна передавати кілька аудіосигналів синхронно, як на нормальному робочому столі. Більш того, технологія дозволяє приймати сигнали без з'єднання, тобто, розсилки, що відправляються відразу на кілька приймачів, що входять в групу широкомовної передачі. Для користувачів смартфонів це не дуже критично, але ж є ще й пристрої розумного будинку. З іншого боку, ця можливість є двосторонньою.

Для користувача це означає, що можна одночасно приймати звук з декількох джерел, наприклад, смартфона, комп'ютера і ноутбука.

Новий аудіокодек LC3. Здатний використовувати технологію ISOC, в тому числі для роздільного звукопередачі на лівий і правий навушники в рамках одного з'єднання. Забезпечує прийнятну якість звукопередачі навіть при слабкому рівні сигналу. Споживає набагато менше енергії, що робить його неоціненним при використанні в слухових апаратах. Повторні передачі даних. Якщо пристрій-приймач не підтвердило передачу пакета, проводиться повторна передача даних. Для цього вибираються ізохронні канали, відмінні від вихідного, щоб зменшити ризик вторинної втрати пакета. Щоб отримувати інформацію про відстань між приймачем і передавачем, в Bluetooth використовується RSSI - індикатор рівня прийнятого сигналу. Це дає можливість декодувати сигнал виходячи з необхідної для цього оптимальної потужності. Якщо він сильніший, або, навпаки, більш слабкий, якість декодування буде страждати. У Bluetooth 5.2 введена функція під назвою LERC, суть якої зводиться до двостороннього управління потужністю сигналу на основі даних RSSI. Головний блок не може просто буде підлаштовуватися під випромінюється передавачем рівень, але може запросити його зміна.

Це дає ряд важливих переваг: Поліпшення контролю якості сигналу. Менша кількість помилок при декодуванні. Більш вузька смуга в діапазоні 2,4 ГГц, що знижує рівень перешкод, в тому числі для джерел, які не є Bluetooth. Все націлене на досягнення якісної роботи в багатопотоковому режимі. Ну а проблеми з діапазоном 2,4 ГГц, спочатку спричинили необхідність створення Wi-Fi 5, а потім - Wi-Fi 6 і Wi-Fi 6E, загальновідомі.

Література:

1. Mob-Mobile.ru Статті и Лайфхаки Bluetooth 5.2 <https://mob-mobile.ru/statya/13749-bluetooth-52-osobennosti-i-preimuschestva-standarta.html> (дата звернення 16.05.2021)
2. ITIGIC Technical How-Tos Tips and Tricks <https://itigic.com/ru/bluetooth-5-2-why-should-i-buy-devices-with-this-standard/> (дата звернення 16.05.2021)

ТЕХНОЛОГІЯ РУХОМОГО(МОБІЛЬНОГО) ЗВ'ЯЗКУ П'ЯТОГО ПОКОЛІННЯ

Маковійчук Іван Ігорович

Державний університет телекомунікацій

Навчально-науковий інститут інформаційних технологій

На сьогодні, в Україні активно розвивають технологію 4G , або ж LTE. Покриття ще не повне та не стабільне, а влада у 2019 році видала наказ про впровадження мереж 5G. Мережа 5G розшифровується як п'яте покоління («5th Generation») мобільних мереж. Це наступна після попередніх поколінь (1G, 2G, 3G, 4G) технологія бездротового зв'язку, яка є ефективнішою й більш досконалою. 5G буде використовувати радіохвилі в сотні до тисяч МГц.

Цей діапазон вже використовують wi-fi , Bluetooth, GPS , та теперішні мережі мобільного зв'язку, але будуть відмінності. В кодуванні, в розподілі каналів та в довжині хвилі. Нове покоління буде використовувати міліметровий діапазон хвиль з частотою до 40 000 МГц. Що , в свою чергу,

дасть можливість досягти швидкість до 20 Гбіт/с , затримку сигналу до 1 мс та покриття у 1 млн абонентів на 1 км² і зменшить витрати електроенергії.

Для кого , або ж для кого потрібне 5G? У зв'язку з тим, що до мережі сьогодні підключено багато інтернет речей , такі як шлагбауми, велосипеди, кондиціонери, автомати із їжею, термінали для оплати. Для них , як раз, дуже критичним є швидкість передачі даних та затримка сигналу. Також , нове покоління , дає можливість зробити «нарізку мережі». Тобто , відокремити мережу для звичайних абонентів від мережі для інтернет пристроїв. Таким чином зробити мережу в середині мережі, що ще знизить затримки для критичних користувачів мережею. Через використання такого широкого діапазону, мережі п'ятого покоління, зможуть розвивати телемедицину. Настане час, коли лікар та пацієнт будуть знаходитись на відстані у 1 000 км один від одного, і щоб провести аналіз непотрібно буде їхати в інше місто до певного фахівця.

Тож, на сьогодні, ми маємо наступне : 5G з 2019 року вже впроваджено у Південній Кореї, США , а згодом і в інших 37 країнах світу. Тому, щоб в Україні з'явилась мережа п'ятого покоління, чекаємо поки військові та інші силові структури , які використовують критичні для 5G діапазони хвиль звільнили для цивільного користування, що за наказом КабМіну, має відбутись у 2021 році.

Література:

3. What is 5G // <https://root-nation.com/ua/articles-ua/tech-ua/ua-what-is-5g/>
4. Глобальні комп'ютерні мережі https://pidru4niki.com/74236/informatika/globalni_kompyuterni_merezhi.

ПРОБЛЕМИ ФУНКЦІОНУВАННЯ МЕРЕЖ 5G

Стрілець Юрій Анатолійович

Державний університет телекомунікацій

Навчально-науковий інститут інформаційних технологій

Головною особливістю сучасного етапу розвитку систем стільникового зв'язку є перехід на системи п'ятого покоління. В першу чергу це пов'язано з тим, що платформа мережі 5G надає операторам значні переваги, які проявляються головним чином в розширенні функціональних можливостей і характеристик мережі, підвищення задоволеності користувачів (User Experience).

Основні параметри мережі IMT2020 (5G) у порівнянні з показниками IMT-Advanced (4G) [1, с. 18]:

- мережі п'ятого покоління в порівнянні з 4G/LTE забезпечать різке зростання швидкостей передачі даних. Пропускна здатність теоретично може досягати 20 Гбіт/с. для сценаріїв з широкими зонами охоплення, наприклад в міських і приміських районах, очікується, що швидкість передачі даних користувачам складе 100 Мбіт / с. Для сценаріїв з бездротовими точками

доступу очікується, що швидкість передачі даних користувачам досягне більш високих значень (наприклад, 1 Гбіт/с всередині приміщень).

- ефективність використання спектру збільшиться – обсяг інформації, яка може бути передана на одиницю частотного діапазону в мережі 5G, буде як мінімум в три рази вище, ніж в мережі 4G.

- швидкість, з якою користувач з терміналом 5G може переміщатися в зоні покриття мережі без втрати передачі між базовими станціями, в мережі 5G досягає швидкості 500 км/год, що дозволяє використовувати послуги 5G в високошвидкісних поїздах.

- затримка мережі 5G зменшується до 1 мс або менше, тоді як мережу 4G може досягати затримки не менше 10 мс. Це дозволяє використовувати технологію 5G для критично важливих комунікацій і відеоспостереження, тактильних Інтернет-послуг, AR/VR і т.д.

- щільність терміналів в мережі 5G збільшується на порядок і може досягати декількох мільйонів пристроїв на 1 кв. км, тобто на одному квадратному метрі поверхні може перебувати кілька десятків або навіть сотень мініатюрних пристроїв (таких як датчики Інтернету речей).

- енергоефективність мережі 5G на порядок краще, ніж в мережі попереднього покоління. Робоча ємність на одиницю площі, тобто швидкість передачі даних на квадратний метр зони покриття мережі, в 5G на два порядки вище, ніж в мережі 4G.

Проте, існує декілька труднощів, пов'язаних з розгортанням мереж 5G [1, с. 31-34]:

1. Волоконні транзитні лінії. Розгортання транзитних оптичних мереж для small cells, що підтримують високі швидкості передачі даних і короткі затримки, є однією з основних проблем, з якими оператори зіткнуться внаслідок відсутності таких мереж у багатьох містах.

2. Спектр. Координація зусиль світової спільноти, регіональних організацій електрозв'язку і Національного регуляторного органу (НРО) необхідна для виявлення і розподілу спектра, узгодженого на глобальному рівні. Для НРО це одна з найголовніших проблем для успішного розгортання мереж 5G. Гармонізований розподіл має багато переваг, оскільки зводить до мінімуму радіоперешкоди уздовж кордонів, полегшує міжнародний роумінг і знижує вартість обладнання. Така загальна координація є важливою роллю МСЕ-R під час Всесвітніх конференцій радіозв'язку (ВКР). Також слід розглянути можливість більш ефективного спільного використання існуючого спектру. Національні регулятори традиційно надають спектр операторам мобільного зв'язку в виняткових випадках. Однак, з огляду на зростаючий попит на частоти, одним із способів підвищення ефективності використання доступного спектра може бути його спільне використання.

3. Одна з основних проблем безпеки 5G, на думку фахівців [2], полягає в зростанні числа можливих векторів атак в міру збільшення кількості мережевих рівнів, призначених для різних типів трафіку. А з огляду на колосальну кількість датчиків Інтернету речей та інших кінцевих точок, які будуть обслуговуватися мережами 5G, для атакуючих стають потенційними мішенями

для атак. Своєрідним захистом може стати «розділення» опорної мережі на логічні сегменти, яка ізолює їх один від одного, розташовуючи кожен у своєрідний «карантин», що дасть мережі 5G більшу захищеність, ніж у «єдиної» 4G-мережі, так як зламувати треба буде кожен сегмент окремо.

Проте ця гіпотеза потребує більш детального аналізу. Можливо, що перехід на 5G зробить мережі більш уразливими внаслідок збільшення ризику компрометації особистих даних, зростання кількості підключених пристроїв та у складності процесу управління безліччю корпоративних мереж. Але це вже питання подальших досліджень.

Список використаних джерел:

1. Международный союз электросвязи Подготовка к внедрению 5G: возможности и проблемы. – Женева, 2018 г [Електроний ресурс]. – Режим доступу: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.5G_01-2018-PDF-R.pdf

2. Петров И. Какие трудности ждут сети 5G на предприятиях [Електроний ресурс]. – Режим доступу: https://www.cnews.ru/articles/2020-03-03_kakie_trudnosti_zhdut_seti_5g_na_pre_dpriyatiyah

СЕКЦІЯ 2

ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

УПРАВЛІННЯ ТРАФІКОМ В ІР-МЕРЕЖАХ

Петрунько Ростислав Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

В даний час швидкість розвитку телекомунікаційної галузі є найшвидшою. Оскільки зростання клієнтської бази оператора зв'язку сповільнився, трафік також збільшився завдяки впровадженню нових технологій та збільшенню частки послуг на основі ІР. З огляду на ці тенденції, оператори зв'язку впроваджують нові послуги, що призводить до переходу від телекомунікаційних мереж до декількох послуг.

У свою чергу, це накладає певні обмеження на роботу телекомунікаційних мереж. Потрібно відповідати вимогам до якості обслуговування-якості обслуговування (QoS), для різних категорій трафіка якість обслуговування, як правило, не тільки різна, але й суперечлива. Для того, щоб одночасно відповідати різним вимогам якості обслуговування в комунікаційній системі, необхідно впровадити систему управління дорожнім рухом, а система управління дорожнім рухом повинна враховувати характеристики різних категорій трафіку та забезпечувати ефективний перерозподіл мережевих ресурсів.

Для поліпшення якості обслуговування (QoS) переданого мережевого трафіку важливо знайти гнучкий спосіб управління мережевими ресурсами, щоб забезпечити збалансоване завантаження його ресурсів та гарантовану якість обслуговування для неоднорідного користувацького трафіку в мультисервісна мережа.

В даний час користувачі мультисервісних мереж все більше цікавляться такими послугами, як відеоконференції та доступ до Інтернет-послуг. Метод забезпечення якості обслуговування різнорідного трафіку ще не повністю вирішений.

Для вирішення цієї проблеми необхідно впровадити категорії послуг для різних типів трафіку та систему управління трафіком, яка забезпечить конкретні категорії послуг для різних типів трафіку шляхом перерозподілу мережевих ресурсів. В даний час тема управління дорожнім рухом є дуже актуальною, оскільки не існує єдиного способу вирішення цієї проблеми.

Одним із способів забезпечити ефективну передачу трафіку, підтримуючи параметри якості обслуговування (QoS), є використання технології комутації міток MPLS з кількома протоколами. Це досягається за рахунок використання технології інженерного руху (TE) за допомогою використання механізму збалансування навантажень мережевих ресурсів, вибору найкращого маршруту, застосування процесу утримання та розподілу мережевого трафіку та механізму збалансування трафіку та запобігання перевантаженню.

MPLS (Multi-Protocol Label Switching) - це технологія, що базується на етикетках, для швидкої комутації пакетів даних у мережі з декількома протоколами. MPLS розроблений і позиціонується як засіб для побудови високошвидкісної магістральної мережі IP, але його сфера застосування не обмежується IP-адресою, але може бути розширена на будь-який трафік мережевого протоколу маршрутизації.

MPLS заснований на принципі перемикання ярликів. Кожен переданий пакет даних асоціюється з тим чи іншим класом мережевого рівня (прямий еквівалентний клас, FEC), і кожен клас мережевого рівня ідентифікується певною міткою. Значення мітки унікальне лише для шляху між сусідніми вузлами в мережі MPLS, яка називається маршрутизатором перемикання міток (LSR). Мітка передається як частина будь-якого пакету даних, і спосіб прив'язки до пакету даних залежить від використовуваної технології каналного рівня.

Маршрутизатори LSR отримують відповідну інформацію про топологію мережі, беручи участь в алгоритмах маршрутизації-OSPF, BGP, IS-IS. Потім він починає взаємодіяти з сусідніми маршрутизаторами для розповсюдження міток, які будуть використовуватися для обміну в майбутньому. Розподіл міток між LSR Налаштуйте шлях перемикання міток (шлях перемикання LSP) у домені MPLS.

Кожен LSR містить таблицю, що відповідає потрійному префіксу адреси одержувача "вхідний інтерфейс, вхідна мітка", вихідний інтерфейс і пара вихідних міток. "Старе значення мітки замінюється новим ярликом у полі" джерельна мітка "таблиці, а потім пакет надсилається на наступний пристрій у шляху LSP - той, що має найдовший префікс адреси в таблиці маршрутизації, що використовується в традиційна маршрутизація Адреса відправника.

Мережа MPLS розділена на дві зони з різними функціями - основну зону та прикордонну зону. Ядро складається з пристроїв, які потребують підтримки MPLS і беруть участь у процесі маршрутизації потоку протоколу комутації MPLS. Маршрутизатор ядра підтримує лише комутацію.

Як результат, в прикордонній зоні проводяться інтенсивні розрахунки, а в ядрі - ефективна комутація, що дозволяє оптимізувати конфігурацію пристроїв MPLS на основі їх розташування в мережі.

Тому головною особливістю MPLS є відокремлення процесу комутації пакетів від аналізу IP-адреси в заголовку, що приносить багато привабливих особливостей.

Отже, технологія MPLS дозволяє дуже ефективно підтримувати необхідну якість обслуговування, не порушуючи гарантій, що надаються користувачам. Використання механізмів управління буфером та чергою (таких як WRED, WFQ або CBWFQ) в LSR дозволяє операторам мережі MPLS контролювати розподіл ресурсів та ізолювати окремий користувацький трафік.

Використання чітко визначених маршрутів у мережі MPLS не має недоліків стандартної IP-маршрутизації від джерела, оскільки вся інформація про маршрутизацію міститься в мітці, а пакети даних не повинні містити проміжних адрес вузлів, тим самим покращуючи управління балансуванням

навантаження мережі. Периферійний маршрутизатор визначає рівень обслуговування пакетів даних, які він отримує. Відповідно до цього типу послуги, пакунку буде присвоєно ярлик. Виходячи з цієї мітки, визначте наступний маршрутизатор, до якого буде потрапляти цей пакет. Там мітка буде перерозподілена, і пакет переміститься до наступного маршрутизатора. Це триватиме доти, доки пакет не дійде до маршрутизатора призначення. Там тег буде видалено та надіслано користувачеві.

Технологія оптимізації трафіку (інженерія TE) відіграє важливу роль в оптимізації управління трафіком у мережах MPLS (Multi-Protocol Label Switching). Технологія інженерного руху базується на ідеї збалансування використання різних мережевих ресурсів (інформації, буферів та каналів). Факти засвідчили, що ефективність технології інженерного руху була покращена в принципі багатьма інструментами управління мережевим трафіком. Протоколи резервування ресурсів RSVP-TE та LDP-TE, протоколи маршрутизації IS-IS-TE, OSPF-TE це трохи засвідчили . .

Одним з найефективніших методів є надання рекомендованих методів черг інженерної інженерії для управління чергами в мережі MPLS.

Література:

4. Li Y. Panwar S. Liu C.J. On the Performance of MPLS TE Queues for QoS Routing // Simulation series. – 2004. – Vol. 36; part 3. – P. 170–174.
5. Вегешна Ш. Качество обслуживания в сетях IP / Пер.с англ./ Ш. Вегешна // – М.: Издательский дом «Вильямс». – 2006. – 386 с
6. Huerta, M., Padilla, J. J., Hesselbach, X., Fabregat, Ramon, Ravelo O. Buffer Capacity Allocation: A method to QoS support on MPLS networks // Proc. EATIS2006 - Euro American Conference on Telematics and Information Systems, 2006. – P. 14–28.

ОЦІНКА ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ВУЗЬКОПОЛОСНИХ ТЕХНОЛОГІЙ ПРИ ПОБУДОВІ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

*Ярош Віталій Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Стрімкий розвиток технологій та необхідність автоматизації вимагає розробки нових підходів при створенні та розгортанні телекомунікаційних мереж, де одним із рішень є впровадження Інтернету речей, зокрема вузькополосного Інтернету речей

Інтернет речей (IoT) - це, мережа, що складається з унікально ідентифікованих об'єктів (за фактом «речей»), які можуть взаємодіяти між собою через IP-підключення без втручання людини.

Як свідчать всесвітні прогнози розвитку так званої Індустрії 4.0 і створюваних в її рамках цифрової економіки та цифрових підприємств, вже зовсім скоро прогресивному людству доведеться зіткнутися як мінімум з десятками мільярдів підключених пристроїв з пулу Інтернету речей та інформаційним обміном з величезним кількістю датчиків і впроваджених в виробничі процеси різних «кіберфізичних систем» (CPS - Cyber-Physical

System), зосереджених по значній площі. Передбачається, що існуючі мережі стільникового зв'язку не зможуть обслуговувати таку велику кількість пристроїв M2M (Machine-to-Machine). Саме тому виникає необхідність пошуку кардинально нових рішень, при розгортанні нових мереж, що і стало основним фактором для виникнення поняття Інтернету речей.[2]

Одним із рішень при плануванні даних мереж є впровадження вузькополосного Інтернету речей (NB-IoT), що дозволяє ефективно підключення великої кількості пристроїв до мережі.

Основними вимогами до мереж IoT є:

- ємність мережі, що виражається у кількості підключених пристроїв
- площа покриття
- надійність
- допускається невелика швидкість передачі даних
- ефективність використання енергетичних ресурсів

NB-IoT використовує несучу, шириною 200 кГц, яка може бути розташована в будь-якому вільному діапазоні, всередині каналів GSM, всередині каналу LTE або в захисному інтервалі між каналами LTE.

Частотний діапазон може бути будь-яким з тих, що визначені для мереж LTE з частотним поділом каналів (LTE FDD). У каналі «вниз» використовується технологія множинного доступу OFDMA, в каналі «вгору» - SC-FDMA. Слід зауважити, що в реальному житті базова станція не тільки повинна підтримувати одночасну роботу багатьох тисяч пристроїв IoT, а й забезпечувати їх підключення найкращим чином незалежно від якості покриття.

В результаті технологія NB-IoT підтримує широкий діапазон швидкостей передачі даних.

Швидкість передачі даних залежить від якості каналу зв'язку (відносини сигнал / шум), а кількість підключених пристроїв - від виділених ресурсів (пропускної спроможності).

У каналі «вниз» всі пристрої мають одну і ту ж енергетику радіоканалу і можуть одночасно приймати сигнали з базової станції. У каналі «вгору» кожен пристрій має свій власний енергетичний потенціал, що може бути використано для мультиплексування трафіку. При цьому створюваний сукупний сигнал від декількох пристроїв (і, відповідно, їх потужність) буде більше, ніж у одного пристрою.

Щоб отримати таку можливість в NB-IoT замість «колективного» каналу (загального блоку ресурсів) зі швидкістю передачі даних до 250 кбіт/с передбачено використання піднесучих частот зі смугою пропускання 15кГц (ефективна смуга пропускання загального каналу NB-IoT - 180 кГц) і швидкістю передачі даних до 20 кбіт / с. У свою чергу, термінальні пристрої можуть використовувати одну або кількох піднесучих у висхідній лінії зв'язку.[1]

Таким чином, використання технології NB-IoT, забезпечує:

- велику зону покриття
- ефективне використання частотного ресурсу

- ефективно використання енергетичного ресурсу
- можливість швидкої модернізації
- високу надійність
- сумісність з іншими технологіями діапазону частот.

Список використаних джерел:

1. Узкополосный доступ для широкого внедрения Интернета Вещей URL – <https://habr.com/ru/company/technoserv/blog/345850/>
2. INTERNET OF THINGS: ВСЕ, ЧТО НУЖНО ЗНАТЬ ОБ ИНТЕРНЕТЕ ВЕЩЕЙ И О БУДУЩЕМ СОВРЕМЕННОЙ ЦИВИЛИЗАЦИИ URL – <https://www.everest.ua/ru/internet-of-things-vse-chto-nuzhno-znat-ob-ynternete-veshhej-y-o-budushhem-sovremennoj-czyvylyzaczyy/>

ЗАСТОСУВАННЯ ПРОТОКОЛІВ ШИФРУВАННЯ В WI-FI МЕРЕЖАХ

*Осипець Олексій Анатолійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Останнім часом люди намагаються поліпшити спілкування, щоб зробити його максимально мобільним, зменшуючи тим самим залежність від зовнішніх пасивних об'єктів. Це є причиною створення бездротової мережі Wi-Fi.

Wi-Fi є товарним маркою Wi-Fi Alliance для бездротових мереж на основі стандарту IEEE 802.11. Технологія Wi-Fi спочатку стала стандартом, за яким слідували виробники мобільних пристроїв. Поступово мережі Wi-Fi почали використовувати малі та великі офіси для організації внутрішніх мереж та підмереж, а оператори створили власну інфраструктуру для забезпечення бездротового доступу до Інтернету. У бездротовій мережі доступ до переданої інформації набагато простіший, ніж у дротовій мережі, і може вплинути на канал даних. Досить розмістити відповідне обладнання в зоні покриття мережі. Втручання між клієнтом і точкою доступу третього пристрою переспрямовує зв'язок між ними самостійно, дозволяючи видаляти, спотворювати або нав'язувати неправдиву інформацію. Перехоплюючи та блокуючи інформацію на каналах Wi-Fi, щоб знищити конфіденційність інформації, питання цілісності та доступності є дуже актуальними.

Розробники стандарту IEEE 802.11 поставили собі за мету - забезпечити безпеку передачі даних через бездротові локальні мережі. Для забезпечення конфіденційності та захисту даних, що передаються авторизованими користувачами через бездротові мережі, були розроблені різні методи шифрування.

Першим способом захисту передачі інформації є стандарт шифрування WEP (Wired Equivalent Privacy). Він забезпечує можливість шифрування даних, переданих через бездротове середовище, забезпечуючи тим самим їх конфіденційність [1]. Шифрування WEP має багато недоліків: механізм обміну ключами та перевірку цілісності даних, малорозрядний розмір ключа та вектор ініціалізації, метод автентифікації та сам алгоритм шифрування.

З метою розробки більш безпечної версії бездротової локальної мережі було створено специфікації 802.11i, включаючи WPA та WPA2. Вони є розширеною та модифікованою версіями протоколу WEP. Основна відмінність полягає в тому, що повідомлення можна не тільки зашифрувати, але й аутентифікувати. Наприклад, WPA підтримує стандарт 802.1X та EAP (розширюваний протокол автентифікації), а WPA2 підтримує шифрування відповідно до AES (Advanced Encryption Standard) та IEEE 802.11i.

Усі атаки WEP базуються на недоліках шифру RC4, таких як можливість конфліктів між векторами ініціалізації та змінами кадрів. Усі типи атак вимагають перехоплення та аналізу бездротової мережі. Залежно від типу атаки, кількість кадрів, необхідних для хакерської атаки, також різна.

Для алгоритму WPA вже існує технологія вторгнення в мережу через недоліки TKIP (Тимчасовий протокол цілісності ключів). Використовуючи його, ви можете читати дані передачі з точки доступу на пристрій і навіть надсилати на пристрій помилкові повідомлення. Однак WPA2 не є вразливим до таких атак і забезпечує безпечну передачу даних. Сьогодні єдиним способом обійти захист WPA2 є метод "грубої сили", який заснований на зборі переданих пакетів даних, порівнянні їх між собою та подальшому пошуку ключів.

Використовуючи такі програми, як Aircrack, використання WEP-шифрування для атаки бездротових мереж відбувається дуже швидко і не вимагає спеціальних навичок. Це відрізняється від шифрування WPA та WPA2. Для шифрування WPA та WPA2 вибір пароля може зайняти багато часу. Процес вибору 8-значного пароля, що складається лише з цифр (середня швидкість вибору пароля становить 1280 ключів / сек) для злому не перевищуватиме 22 годин. При використанні літер у паролі його складність збільшиться на 8 символів. Навіть у таких протоколів, як WPA2, є лазівки, але в даний час це все ще найнадійніший протокол безпеки.

Тому для забезпечення безпеки Wi-Fi потрібно використовувати шифрування WPA2, і для ускладнення завдання вибору пароля рекомендується використовувати складний буквено-цифровий пароль.

Література:

1. В.Г.Олифер, Н.А.Олифер. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд.– СПб.: Питер, 2011. – 944 с.:ил.
2. WiFi: Все, что Вы хотели знать, но боялись спросить. Неофициальное пособие по глобальной системе местопределения. / под редакцией Щербакова А. К – Москва; Литературное агентство «Бук-Пресс», 2005 352 с.

ВПЛИВ WI-FI НА ЖИВІ ОРГАНІЗМИ

*Дурман Володимир
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Всесвітня павутина охопила весь сучасний світ. Сьогодні важко уявити роботу банків, магазинів, кафе, аеропортів та різних установ без Інтернету.

Багато з нас намагаються використовувати його без різних перешкод і бар'єрів. Цьому, звичайно, сприяє wi-fi, винайдений в 1991 році. Він використовується людьми майже чверть століття, і інформація про його шкідливий вплив на людину не поширюється.

Цей пристрій випромінює низькочастотні хвилі, рівні 2,4 ГГц, такі ж, як у мікрохвильовій печі. Американські вчені встановили, що радіохвилі з частотою 0,5-2,4 ГГц негативно впливають на людину. Нервова система першою відчуває негативні наслідки бездротового з'єднання. Американські лікарі все частіше приймають пацієнтів з головними болями, загальним нездужанням, різким погіршенням зору. Вчені з Данії вже попереджали: wi-fi - негативно впливає на живі організми та викликає головний біль. Також було виявлено, що деякі люди схильні до алергічних реакцій на «невидимі» бездротові мережі. Мігрень почастішала. Лікарі не говорять про те, що збільшення кількості пацієнтів пов'язано лише з повсюдною мережею Wi-Fi, оскільки її вплив на людину не вивчений до кінця.

Отже, наукова робота студентів є невід'ємною частиною застосування інформаційних технологій та сприяє розвитку інформаційних компетентностей та основи педагогічної майстерності майбутнього вчителя. У процесі наукової діяльності майбутній вчитель отримує знання, що становлять інформаційну основу евристичної діяльності, освоює педагогічні методи та заходи, що визначають оперативні основи когнітивно-дослідницької діяльності, та набуває досвіду в інформаційній діяльності в галузі програмного забезпечення.

Але вчені вже знайшли шкоду від цих частот. Наприклад, експерти зі Швеції виявили, що цей вид опромінення погіршує пам'ять, мислення, навіть поглинання кальцію в організмі погіршується, виникає «синдром втоми». Існують гіпотези про вплив Wi-Fi на живий організм на клітинному рівні. Зокрема, йдеться про зміни ДНК, появу хромосом - мутантів.

Західні вчені однозначно підтвердили шкідливість мережі для зростаючого організму. Багато зацікавлених та освічених батьків турбуються про здоров'я своїх дітей. Ось чому багато шкіл та дитячих садків США та Великобританії заборонили wi-fi.

Ще один добре відомий випадок спостереження впливу постійно діючого маршрутизатора поблизу посаджених рослин. Це сталося в Данії, повідомляє Newsru.com стосовно ABC News. Студенти почали помічати погіршення уваги, концентрації уваги та концентрації в класі, якщо вони засинали вночі із мобільним телефоном, підключеним до мережі. Вони не змогли провести експеримент без спеціальних інструментів, тому вирішили експериментувати з рослинами разом із викладачем біології Кімом Хорсвейдом.

Старшокласники кладуть крес-салат у коробки, половину з них розміщують у кімнаті з wi-fi, а другу половину - у кімнаті без бездротової мережі. Після двох тижнів перебування у другій кімнаті насіння проросло та проросло безпечно, насіння, що зазнали частоти, погано проростало, а слабкі паростки, які з'явилися, потемніли та загинули. Ясність експерименту незаперечна і привернула увагу світових вчених, наприклад, професора

Університету Кароліни у Швеції, який, можливо, вивчає це явище з науковою точністю в лабораторії.

Експерименти з рослинами змушують задуматися і захистити від шкідливого впливу такого відомого повсякденного гаджета.

Наприклад, у кількох канадських школах батьки учнів пропонують в школі використовувати лише дротові Інтернет-технології, оскільки студенти скаржились на головний біль, нудоту, безсоння та серцебиття через їх бездротового Інтернету. Звичайно, необхідні більш глибокі та глобальні дослідження, щоб ретельно дослідити негативний вплив Wi-Fi на організм людини. Технології повинні бути доступні та широко розгорнуті після більш детального та поглибленого вивчення.

У багатоквартирних будинках майже кожна сім'я використовує технологію бездротового Інтернету. Наприклад, якщо припустити з'єднання Wi-Fi у дворі, біля входу з'явиться кілька десятків логінів. Ми не звертаємо уваги на шкідливий вплив мережі на наші власні клітини, на здоров'я наших близьких. Поруч з нами живуть бабусі та дідусі, люди, яким не потрібен Інтернет, не кажучи вже про його негативний вплив на організм. Низькочастотні хвилі проходять великі відстані без бар'єрів та перешкод. Це схоже на "пасивне куріння".

Тому необхідно розглянути це питання, подбати про майбутнє та взяти заходів для захисту рідних від цієї, здавалося б, невидимої «загрози». Крім того, ми не повинні забувати людей поблизу і виявляти повагу, відповідальність та турботу. Хоча ми не можемо точно сказати, наскільки шкідливий Wi-Fi, він може бути менш шкідливим, ніж інші побутові прилади та засоби зв'язку. Однак, щоб ми і люди навколо нас були здоровими, ми повинні дотримуватися таких основних правил:

- Вимикайте маршрутизатор вночі або коли ви не користуєтесь Інтернетом;
- Максимально тримайте дітей подалі від бездротових джерел живлення;
- Встановіть маршрутизатор подалі від робочого місця;
- Не кладіть приймаючий пристрій собі на коліна.

Література:

7. Телекомунікаційні та інформаційні мережі :Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.: іл.

8. Развитие доступа на базе технологий 4G и 5G – основа для стимулирования экономического роста государства. Доктор технических наук, профессор Толубко Владимир Борисович.

МАРШРУТИЗАЦІЯ В МЕРЕЖІ СУЧАСНОГО ПІДПРИЄМСТВА

Китасєв Олексій

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Для організації комунікацій у мережі компанії зазвичай використовується мережева модель сучасного підприємства. Модель передбачає, що компанія має кілька географічно розділених філій, одним з яких є головний кампус. Для того, щоб офіс взаємодіяв між своїми локальними мережами (локальна мережа або локальна мережа), використовуйте з'єднання, створене за допомогою так званої технології World Area Network (або WAN).

Технології WAN, що використовуються в корпоративних мережах, включають:

- Канал другого або третього рівня, орендований через мережу передачі оператора зв'язку;
- Підключення через телефонну мережу загального користування;
- Тунель віртуальної приватної мережі (VPN) в Інтернеті.

У наш час з'єднання VPN в Інтернеті стали дуже поширеними, оскільки вони набагато дешевші за орендовані канали, забезпечуючи при цьому досить якісну передачу даних. Кожна гілка повинна бути підключена до Інтернету, щоб встановити з'єднання VPN між гілками.

У випадку єдиного головного офісу, де розміщені основні інформаційні ресурси підприємства (наприклад, Центр обробки даних), основні потоки даних передаються між головним та підрозділами. Оптимальною топологією з'єднання VPN в цьому випадку є зірка з головною гілкою посередині. Можна використовувати технологію динамічних багатоточкових VPN-з'єднань (Dynamic Multipoint VPN або DMVPN), коли концентратор DMVPN встановлений у штаб-квартирі, а зв'язок між штаб-квартирою та будь-яким підлеглим здійснюється у разі необхідності передачі даних між їх.

Якщо інформаційні ресурси розпорошені між різними підрозділами, крім того, існує потреба у постійній взаємодії між підрозділами, рекомендується використовувати постійні з'єднання VPN, такі як "точка-точка" (точка-точка), кожен з яких підключається два відділи. Для надійності потрібно зв'язати кожен підрозділ з кількома іншими. Цей підхід дозволяє зменшити шлях передачі пакетів, оскільки це відбувається безпосередньо між відділеннями відправника та одержувача, а також забезпечує стійкість мережі до окремих з'єднань VPN - пакети можуть передаватися через інші відділення, уникаючи пошкодженої області.

Якщо загальна кількість гілок не перевищує 4-5, можна створити VPN-з'єднання між кожною парою гілок, щоб створити повну мережу. Якщо у вас велика кількість філій, таких як Десятки, створення цілісної мережі з'єднань призводить до надмірної складності в конфігурації корпоративної мережі. У цьому випадку доцільно визначити 3-4 відділи як основні (основні) та створити цілісну мережу зв'язків між ними. Решта гілок для надійності з'єднані з двома стовбурами. Ця топологія називається "частковою сіткою".

Ефективність корпоративної мережі багато в чому залежить від системи маршрутизації, що в ній реалізована. Щоб розглянути маршрутизацію корпоративної мережі, внутрішню структуру мережі філій можна представити як логічну модель, що включає наступне:

- сегменти мережі для підключення кінцевих пристроїв;
- зв'язок з іншими відділами;
- підключення до інтернету;
- транспортна інфраструктура.

Транспортна інфраструктура забезпечує обмін даними між кінцевими пристроями в межах однієї гілки, між кінцевими пристроями, розташованими в різних гілках, і між кінцевими пристроями інтернет-філії.

Попередні підходи не використовують протоколи динамічної маршрутизації у локальній мережі філії. Це значно спрощує налаштування та обслуговування. Однак динамічна маршрутизація необхідна для переходу відсіву в офісі через з'єднання VPN.

Особливості динамічної маршрутизації між гілками:

- у процесі динамічної маршрутизації беруть участь лише маршрутизатори VPN;
- інформація про маршрути, якими обмінюються VPN-маршрутизатори філій, містить лише загальні префікси гілок типу 10..0.0 / 16;
- на процес маршрутизації між гілками впливає лише стан з'єднань VPN між ними, а зміни топології, що відбуваються в локальних офісних мережах, зовсім не змінюються;
- обмін інформацією про маршрути здійснюється маршрутизаторами VPN за принципом "партнер-партнер" (peer-to-peer).

Для переміщення трафіку між кожною парою гілок підключення VPN буде автоматично обрано безпосередньо між ними, оскільки відповідні маршрути матимуть найкоротшу довжину шляху, виміряну в AS (AS шлях). У разі втрати працездатності цього каналу трафік може передаватися через інші відділи. Стандартний набір атрибутів BGP використовується для ефективної реалізації внутрішньогалузевої політики маршрутизації.

Згідно з розглянутими підходами, відділи мережі можуть використовувати лише статичну маршрутизацію, або динамічну маршрутизацію з простою конфігурацією типу OSPF з однією областю (єдиною областю). Немає необхідності перерозподіляти процеси маршрутизації між гілками та в локальних мережах філій.

Література:

9. 802.1Q-Virtual LANs [Electronic resource]. – Mode of access: <http://www.ieee802.org/1/pages/802.1Q.html>. – Title from the screen.

10. Fundamentals of VLAN's – Router on a stick [Electronic resource]. – Mode of access: <https://learningnetwork.cisco.com/docs/DOC-23481>. – Title from the screen.

11. Network function virtualization [Electronic resource]. – Mode of access: https://en.wikipedia.org/wiki/Network_function_virtualization. – Title from the screen.

РОЗРАХУНОК ДАЛЬНОСТІ КАНАЛУ ЗВ'ЯЗКУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ WI-FI

*Цапренко Іван Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

WI-FI – це технологія бездротової локальної мережі, на основі стандартів IEEE 802.11. Під аббревіатурою WI-FI (Wireless Fidelity), яка дослівно перекладається як “Бездротова точність”. В даний час розвивається ціле сімейство стандартів передачі цифрових потоків даних по радіоканалах.

На різних відстанях відношення сигнал/шум має різне значення. В залежності від відношення сигнал/шум для забезпечення якості зв'язку, встановлюється відповідний тип модуляції. Значення сигнал/шум при якому відповідає необхідній якості зв'язку, для кожного із видів модуляції. У кожного із типів різне значення пропускну здатності каналу.

Зараз існує ряд стандартів із сімейства IEEE 802.11:

IEEE 802.11 – Стартовий стандарт бездротової локальної мережі, працює в діапазоні 2.4 ГГц для бездротової передачі даних. Який має здатність підтримувати обмін даними зі швидкість до 2 Мбіт/с.

IEEE 802.11a - стандарт передбачає швидкість передачі до 54 Мбіт/с, які були затверджено у 1999 році, три обов'язкові швидкості – 6, 12 і 24 Мб/с, і визначені з необов'язкових швидкостей – 9, 18, 36, 48 і 54 Мбіт/с. Реальна швидкість спостерігається в межах 22-26 Мб/с. В незалежності від базового стандарту, орієнтованість спрямована в область частот у 2.4 ГГц, а відповідно сертифікаціями передбачена робота у діапазоні 5 ГГц. Метод модуляції сигналу вибрано частотне проектування мультиплексування (OFDM). Найбільша відмінність між цими радіо-технологіями DSSS і FHSS полягає, що OFDM має припущення до паралельної передачі сигналу у декількох частотних діапазонів, тоді як технологія спектру розширення передає сигнали послідовно. В результаті чого підвищується якість сигналу і її пропускну спроможність. Недоліками стандарту 802.11a, є вища споживча потужність радіопередавачів на частоті 5 ГГц, так і незначний радіус дії (на відміну від частоти 2.4 ГГц, який має можливість працювати на відстані до 300 метрів, для частоти у 5 ГГц до 100 метрів). Для збільшення здатності пропускну спроможності використовують частоту 5.5 ГГц. Для передачі у стандарту 802.11a використовують метод множини, це коли діапазон частот розбивається на підканали, по яких сигнальний потік передається паралельно який розбитий паралельно. При використанні квадратурної фазової модуляції має можливість досягти пропускну спроможності каналу у 54 Мбіт/с.

IEEE 802.11b – це є стандарт бездротової локальної мережі, заснований на передачі даних у діапазоні частот 2.4 ГГц. При цьому діапазоні є три непересічні канали (на одній території), які не впливають один на одного, при якому можуть працювати три різні бездротові мережі. В якому передбачено два типи модуляції – DSSS і FHSS. Має максимальну швидкість роботи 11 Мбіт/с,

також при цьому доступні швидкості у 5.5 , 2 та 1 Мбіт/с. В стандарті 802.11b передбачено автоматичне зниження швидкості при погіршенні якості сигналу.

IEEE 802.11g – система передачі також заснована в діапазоні частоти 2.4 ГГц. Є одним із усіх найбільш поширених стандартів з бездротової передачі даних. Має максимальну швидкість передачі даних у бездротових мережах 802.11g, яка складає 54 Мбіт/с. Діапазон розділений на три канали які не пересікаються на одній території (вони не впливають один на одного). Для збільшення швидкості, використовується метод ортогональної частотної модуляції (OFDM - Ortogonal Frequency Division Multiplexing), також метод двійкового пакетного згорткового кодування PBCC (Packet Binary Convolutional Coding). Треба відзначити у числі переваг стандарту 802.11g, низьку споживчу потужність, більшу дальність дії та високу пропускну здатність сигналу.

Зовнішні Wi - Fi антени служать для посилення сигналу, що дозволяє збільшити зону покриття Wi - Fi мереж.

В основному поширені пасивні антени – кругові (все направлені) і спрямовані. Основна відмінність - характер поширення хвиль антеною.

Кругова антена випромінює сигнал по колу 360* (горизонталь) і зона покриття має вигляд тороїда.

Отже, враховуючи сучасні потреби користувача та можливості обладнання, найбільш актуальним є використання стандарту IEEE 802.11g передачі цифрових потоків даних по радіоканалах, оскільки передача даних по цьому стандарту має ряд переваг перед іншими. В залежності від вимог користувача, стосовно зони покриття сигналу, антени підбирають індивідуально.

Список використаних джерел

1. Андрианов В.И., Соколов А.В. Средства мобильной связи.- СПб: БХВ – Санкт-Петербург, 1999
2. Мікрохвильові технології в телекомунікаційних системах/ Т.М. Наритник, В.П. Бабак, М.Ю. Ільченко, С.О. Кравчук.- К.: Техніка, 2000
3. Наритник Т.Н. Радиорелейные и трансферные системы передачи. Учебное пособие.- К.: Вид. Дім „Ін Юре||”, 2003
4. ДСТУ 3008-95. Документація, звіти у сфері науки і техніки.- К.: Держстандарт України, 1995
5. Закон України "Про телебачення і радіомовлення" № 3759-ХІІ від 21.12.93р

КОМП'ЮТЕРНИЙ ЗІР: СУТНІСТЬ ТА ОСОБЛИВОСТІ

*Кравченко Ростислав Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій*

Повторювання людської взаємодії та поведінки - це те, чим завжди займався штучний інтелект. Останнім часом пік технологій і справді перевершив те, що спочатку вважалося тільки можливим, а зараз є повсякденним завданням ШІ та інших технологій, що вирішують проблеми у всьому світі.

Комп'ютерний зір - це ще один крок у напрямку розвитку ШІ. Метою комп'ютерного бачення - є відтворення сприйняття та розуміння зображення людиною, а потім отримання корисної інформації з цього зображення.

З часів коли розпізнавання зображень стало невід'ємною складовою комп'ютерного зору, воно використовується як для розпізнавання обличчя при підтвердженні здійснення банківських операцій так і для розпізнавання обличчя злочинців.

Проблеми що вирішуються за допомогою комп'ютерного зору:

- Відстеження злочинців – програмне забезпечення для комп'ютерного зору може бути додане до камер спостереження щоб допомогти реєструвати номерні знаки автомобілів, які проїжджають через зону дії дорожньої камери.

- Виглядати стильно та модно – штучний інтелект, комп'ютерний зір та машинне навчання можуть допомогти підібрати найкращий одяг, що пасує, наприклад, джинсовій куртці.

- Контроль якості навчання - комп'ютерний зір, може відстежувати поведінку учнів під час навчання онлайн або написання підсумкових тестів.

Що далі:

Роботи існують вже досить давно. Однак одне з гострих питань, яке залишається, полягає в тому, що коли ми будемо бачити, як роботи стають частиною нашого життя. Причина затримки розвитку робототехніки полягає в тому, що роботи погано бачать. Під добре бачити, мається на увазі наслідування часу реакції та поведінки людини на те, що бачать наші очі. Комп'ютерне бачення та виклики, що лежать в рамках цієї технології, були добре застосовані до програм, але роботи, здається, є наступним логічним кроком.

Електронні ресурси:

1. Computer Vision Is Solving Problems That Weren't Even On Our List - <https://hackernoon.com/computer-vision-is-solving-problems-that-werent-even-on-our-list-ybfu3ys2>

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ BIG DATA ОПЕРАТОРОМ МОБІЛЬНОГО ЗВ'ЯЗКУ

Прокопів Н.В.

*Навчально-науковий інститут інформаційних технологій
Державний університет телекомунікацій*

Важко знайти галузь, для якої проблематика великих даних не була б актуальною. Вміння оперувати великими обсягами даних, аналізувати взаємозв'язки між ними і ухвалювати зважені рішення, з одного боку, надає потенціал для компаній з різних вертикалей для збільшення показників прибутковості і підвищення ефективності. З іншого боку, це чудова можливість для додаткового заробітку партнерів вендорів-інтеграторів і консультантів.

Якщо повернутись до методів Big Data, які направлені на отримання ефекту для бізнесу оператора зв'язку, то тут, зокрема, розглядаються чотири основні напрямки – перші три націлені на покращення внутрішньої роботи самої компанії, а останнє являє собою додатковим ринковим продуктом для зовнішніх клієнтів [1,с.139]:

–високоточний маркетинг (precise marketing) – адресна пропозиція продуктів та послуг тим абонентам, які найбільш готові до їх придбання;

–управлінням якістю послуг для абонентів (Customer Experience Management) для підвищення задоволеності з метою запобігання відтоку абонентів;

–оптимізація внутрішньої роботи оператора і планування розвитку (ROI-based Network Optimization and Planning);

- тестування кращих варіантів пропозицій (A/B-тестування);

- аналітика і підстроювання контексту дослідження в реальному часі;

–монетизція інформаційних активів (Data Asset Monetization) – продаж в тій чи іншій формі (в тому числі у вигляді пайової участі в проектах) даних, які мають оператори, своїм партнерам, щоб вони могли з їх допомогою вирішувати свої задачі. Приклад реалізації можливостей Big Data на основі відкритого ПО Hadoop приведений на рис. 1.1.[3,с. 184-187].

Набір бібліотек та утиліт Hadoop включає в себе такі інструменти, як :

–SEM – Customer Experience Management – управління клієнтським досвідом;

–RA – Revenue Assurance – система «гарантованих доходів»;

API – Application Programming Interface – додаток з відкритим кодом для вбудовування в інтерфейси других програм.

Опитування телеком-компаній також свідчать, що, збираючи великі обсяги даних, пов'язаних з активністю клієнтів, і величезна транзакційні логи елементів мережі, телеком-компанії далеко не в повній мірі використовують ту цінність, яка в цих даних міститься. Так, дослідження компанії Heavy Reading показало, що проблеми неможливості інтегрованого аналізу всіх наявних у телеком-операторів джерел інформації і недостатня оперативність аналізу цих даних – основні бар'єри, які стоять перед компаніями при розвитку систем оперативної аналітики.

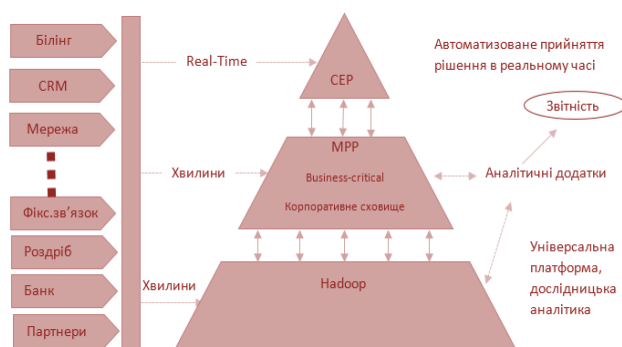


Рисунок 1.1 - Варіант реалізації Big Data в мережі оператора мобільного зв'язку

Дійсно, у телеком-компаніях рівень розвитку ІТ нижче, ніж в інтернет-компаніях, кількість ІТ-спеціалістів менше, а професіоналів в області великих даних може взагалі не бути в штаті. Тому телеком-компанії потребують не тільки в зовнішньому постачальнику технології Big Data, але і в консультанті, який би розбирався в їх бізнесі, їх ІТ-інфраструктурі, специфіку побудови систем Big Data для телеком-індустрії. Плануючи проект впровадження рішення Big Data, важливо продумати бізнес-схеми отримання прибутку від аналізу даних.

Перелік використаної літератури:

1. Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим/ В. М. Шенбергер, К. Кукьер; пер. с англ. Инны Гайдюк. – М.: Манн, Иванов и Фербер, 2014. – 240 с
2. Shakhovska N. Data space architecture for Big Data managing/ N. Shakhovska, O. Veres, Y. Bolubash, L. Bychkovska-Lipinska/ Xth International Scientific and Technical Conference "Computer Sciences and Information Technologies" (CSIT'2015).- P. 184-187, Lviv, 2015.

АНАЛІЗ ЗАСТОСУВАННЯ CISCO PACKET TRACER ДЛЯ РЕАЛІЗАЦІЇ ВІРТУАЛІЗОВАНОЇ МЕРЕЖІ

Союк Віталій Віталійович

Державний університет телекомунікацій

Навчально-науковий інститут інформаційних технологій

Найпопулярнішим емулятором мережевого обладнання є Cisco Packet Tracer, це емулятор, розроблений самою компанією Cisco Systems для навчання початківців фахівців. Packet Tracer отримав велике поширення за рахунок необхідності його застосування для проходження навчання в рамках програм Cisco Network Academy, мережевий академії, в якій щорічно проходять навчання десятки тисяч фахівців. Створення мережевої інфраструктури і наступна модифікація відбуваються через графічний інтерфейс, який є інтуїтивно зрозумілим і найбільш зручних з графічних інтерфейсів управління, що надаються розглянутими програмними засобами емуляції мережевого обладнання [2,с.142]. Інтерфейс добре адаптований для початківців фахівців і дуже сильно спрощує процес створення нових мережевих інфраструктур або запуск і налаштування необхідних для проведення практичних занять сервісів. Приклад інтерфейсу відображений на рис.1.1.

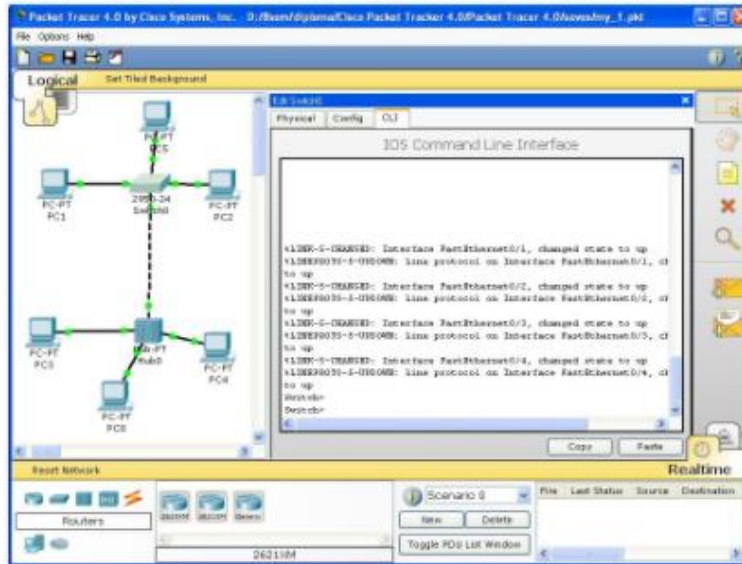


Рисунок 1.1 - Графічний інтерфейс емулятора Cisco Packet Tracer

Основне призначення емулятора Packet Tracer в створенні віртуальних мереж для проведення практичних робіт для підготовки до сертифікаційних іспитів CCNA (Cisco Certified Network Associate) і CCNA Security (Cisco Certified Network Associate Security). Крім стандартних маршрутизаторів і комутаторів Packet Tracer підтримує емуляцію IP-телефонів, бездротових точок доступу і серверів з набором стандартних служб. У Packet Tracer вбудовано безліч засобів, що спрощують вивчення роботи мережевої інфраструктури, таких як сніфери, що дозволяють отримати докладну інформацію про всіх блоках даних переданих того чи іншого пристрою, генератори мережевого трафіку, що дозволяють штучно створювати навантаження, і кошти відображення потоків даних, що дозволяють простежити маршрут проходження мережі будь-яким пакетом або процес зміни пакета при проходженні різних пристроїв. Packet Tracer є зручним засобом емуляції мережевого обладнання не тільки для того, хто навчається, а й для викладача.

В емулятор вбудовані засоби автоматичної перевірки виконання завдання. Викладач може розробити лабораторну роботу для Packet Tracer, яка буде автоматично перевіряти ступінь виконання завдання, і замість перевірки вручну правильності роботи всіх протоколів і коректності введених команд, досить скористатися автоматичною перевіркою, яка визначить відсоток виконання завдання і працездатність основних сервісів. Cisco Packet Tracer виробляє емуляцію як апаратної, так і програмної частини мережевого обладнання.

Таким чином, Packet Tracer дозволяє створювати копії великих мережевих інфраструктур, ось тільки емульованого пристрої не підтримують дуже велика кількість технологій, що використовуються в реальних великих мережах, багато функцій, доступні в реальних пристроях просто відсутні [1, с.234-245].

Головна перевага Cisco Packet Tracer - безкоштовність даного продукту.

Таким чином, емулятор Cisco Packet Tracer є оптимальним інструментом для проведення практичних занять при навчанні з базових курсам компанії Cisco і при підготовці до іспитів рівня спеціаліста. Але для вирішення більш складним завдань моделювання обчислювальних мереж ці програми не

підходить, оскільки є симулятором і не надає всіх можливостей реального обладнання, і далі розглядатися не буде.

Список використаних джерел:

1. Попов С., Баутин А. Cisco Packet Tracer для всех. Сетевые технологии. LAP LAMBERT Academic Publishing 2016г. 300с.

2. M. Bouet, J. Leguay, and V. Conan. Cost-based placement of vDPI functions in NFV infrastructures. In IEEE NETSOFT 2015. 281с.

АНАЛІЗ ВИМОГ ДО МОБІЛЬНОЇ ВЕРСІЇ САЙТУ ДЛЯ НАДАННЯ SMART-СЕРВІСІВ КЛІЄНТАМ B2C

Червоний А.С.

Державний університет телекомунікацій

Навчально-науковий інститут інформаційних технологій

Багато розробників при створенні сайтів звертаються до популярних фреймворків (наприклад, Bootstrap). Зрозуміло, такі інструменти можуть виявитися вельми корисними і значно скоротити час розробки. Але, при цьому, потрібно враховувати, яким чином поширений фреймворк буде працювати з вмістом і функціональністю конкретного сайту, а не як вона працює в цілому.

У таких випадках корисно проведення юзабіліті-тестування для дизайну сайту. Для адаптивного дизайну рекомендується виконувати тестування на різних платформах. Досить складно створити сайт, який буде максимально зручний на звичайних екранах, але набагато складніше реалізувати сайт, який буде не менш зручний при трансформації його елементів в умовах різних розмірів, роздільних здатностей та орієнтацій екрану. Той же елемент дизайну, який працює як слід при звичайному дозволі, може працювати некоректно на смартфоні, і навпаки [1, с.102].

Інформаційне наповнення також є одним з ключових аспектів успішного використання мобільного дизайну. На звичайному екрані текстовий зміст сторінки, як правило, видно цілком без використання прокрутки, на відміну від маленького екрану смартфона. Якщо на великому екрані користувачі не одразу знаходять те, що їм потрібно, то вони можуть легко розглянути всю сторінку, щоб відшукати бажане. На смартфоні ж користувачі змушені нескінченно прокручувати екран до тих пір, поки знайдуть те, що їм цікаво. Розумно скомпонований інформаційний зміст сторінки допомагає користувачам шукати більш ефективно. Питання продуктивності може стати негативним фактором для сайту з адаптивним дизайном. Справа в тому, що сервер видає один і той же обсяг коду на всі приймаючі пристрої, незалежно від того, чи весь обсяг коду використовується у даній конструкції макету. Підбір потрібного макету відбувається вже на стороні клієнта. Іншими словами, кожен пристрій (телефон, планшет або комп'ютер) отримує повний код сторінки, призначений для всіх пристроїв одразу і бере з нього те, що йому потрібно.

4-дюймовий смартфон отримує той же код, що і 24-дюймовий настільний монітор. Це може знизити продуктивність смартфона, якщо використовується повільне інтернет-підключення. Ось чому деякі сайти з адаптивним дизайном

використовують спеціальні запити хостінг-сервера для визначення пристрою, який зробив запит і відправляють йому тільки ту частину HTML коду, яка призначена саме для даного типу пристроїв [2,с.342].

Щоб по-справжньому протестувати зручність роботи з мобільним дизайном сайту, недостатньо перевірити своє дизайнерське рішення у комфортних умовах офісу тільки при високій швидкості з'єднання. Потрібно виходити зі смартфоном на вулицю, тестувати між високими будинками, виїжджати на природу, здійснити випробування в інтер'єрі конференц-залів або у підвалах, в місцях із нестабільним зв'язком, щоб побачити, як сайт буде завантажуватися в цих умовах. Метою якісного мобільного дизайну є надання еквівалентного доступу до інформації, незалежно від пристрою. Потрібно пам'ятати, що користувач смартфона не буде мати ті ж можливості, що і користувач настільного комп'ютера, якщо час завантаження є нестерпно довгим.

Список використаних джерел:

- 1.Ethan Marcotte Responsive Web Design. — A Book Apart, 2018. — 143 с.
- 2.HTML 4.0 в подлиннике / Матросов А., Сергеев А., Чаунин М., СПб.: БХВ-Петербург, 2018, 672 стр.

ОГЛЯД ОБЛАДНАННЯ РОБОТЕХНІЧНОГО КОМПЛЕКСУ

Шевченко В.І

*Навчально-науковий інститут інформаційних технологій
Державний університет телекомунікацій*

Була розроблена система управління сортувальних роботом. Ця система включає наступні компоненти як маніпулятор, показаний на рис.1.



Рисунок 1 - KR 40PA

KR 40 PA є найменшим і легким роботом для палетизації. Досягає найвищих рівнів швидкості і точності, спеціально розроблений для задач, пов'язаних з палетизацією - ідеально підходить для укладання європіддонів. KR 40 PA вибирає і упаковує товари в рекордні терміни. Він може палетірізирувати продукти вагою до 40 кілограмів і досягати чистої висоти штабелювання до 1,8 м; все в дуже маленькому просторі. Час циклу значно скорочується завдяки його малій масі [1].

Система управління KUKA KR C4 показана на рис. 2.



Рисунок 2 - KUKA KR C4

Система управління KR C4 від KUKA є інноваційною для автоматизації виробництва сьогоdnішнього і завтрашнього дня. Вона дозволяє скоротити витрати на інтеграцію, технічне обслуговування і догляд.

Одночасно підвищується ефективність і гнучкість систем - завдяки поширеним відкритим промисловим стандартам. Концепція KR C4 вважається революційною. Вперше в ній Robot/Motion органічно і інтерактивно з'єднані з системами управління для ПЛК, ЧПУ і забезпечення безпеки. Завдяки простому і гнучкому програмуванню робота за допомогою вбудованих формулярів і нового програмування переміщень Spline рішення автоматизації на базі KR C4 з усіх аспектів є неперевершеними. Крім того, KR C4 забезпечує можливості інтелектуального, гнучкого і розширюється використання.

KR C4 інтегрує в архітектуру вашого програмного забезпечення Robot Control, PLC Control, Motion Control (наприклад, KUKA.CNC) і Safety Control. Всі системи управління мають одну базу даних і інфраструктуру. Це дозволяє спростити автоматизацію і зробити її ефективнішою [2].

Список використаних джерел:

1. KR 40 PA [Электронный ресурс]. - Режим доступа:[https:// www.kuka. com/ru-ru /продукция-услуги /промышленная-робототехника/ промышленные-роботы/ kr-40-ра](https://www.kuka.com/ru-ru/продукция-услуги/промышленная-робототехника/промышленные-роботы/kr-40-ра) (дата обращения 23.03.21)
2. KUKA KR C4 [Электронный ресурс]. - Режим доступа:<https://www.kuka.com/ru-ru/продукция-услуги/промышленная-робототехника/ системы-управления-роботом/kr-c4> (дата обращения 23.03.21)

THE PROBLEMS OF TRAITS IN MODERN PHP

Trofymenko V.V.

State University of Telecommunications

This work illustrates the problems with traits in modern PHP and ideas or comments of the community about those problems.

PHP - is a widely-used open source general-purpose scripting language[1]. Created in 1994 by Rasmus Lerdorf, the very first incarnation of PHP was a simple set of Common Gateway Interface (CGI) binaries written in the C programming language. Originally used for tracking visits to his online resume, he named the suite of scripts "Personal Home Page Tools," more frequently referenced as "PHP Tools." Over time, more functionality was desired, and Rasmus rewrote PHP Tools,

producing a much larger and richer implementation. This new model was capable of database interaction and more, providing a framework upon which users could develop simple dynamic web applications such as guestbooks. In June of 1995, Rasmus » released the source code for PHP Tools to the public, which allowed developers to use it as they saw fit. This also permitted - and encouraged - users to provide fixes for bugs in the code, and to generally improve upon it[2]. In addition, in 2021, according to github analytics, php takes the 6th place in popularity among all programming languages presented on the platform.[3]

In August of 1999 was released the first beta version of PHP 4.0 with tools for object-oriented programming[4]. Since then, the object-oriented approach has become dominant in the language, and now we can confidently say that this approach is widely represented in the language.

In March 2012, so-called traits were added to PHP. Traits are entities in the language that allow you to reuse methods or properties using a trait in another class, without adding a type to this class and tied to its implementation, which greatly increases coupling.[4].

One part of the community was positive about the innovation. For example, Hallum Hopkins is extremely positive about traits and concludes that "They're not good; they are fantastic!"[6]. Others quite reasonably argued that if you use traits carefully, you can achieve good cohesion performance without significantly increasing coupling[7]. But in 2020, the community was shocked by the statement of Roman Popov and Dmitry Stogov, respected community members and PHP core developers, that "if they had made a decision in 2012, then traits would never have appeared in PHP"[8].

Thus, traits, which were added to the language in 2012, are now actively discussed by the community.

Literature:

1. What is PHP? [Электронный ресурс] – Режим доступа до ресурсу: <https://www.php.net/manual/en/intro-what-is.php>.
2. History of PHP [Электронный ресурс] – Режим доступа до ресурсу: <https://www.php.net/manual/en/history.php.php#history.php>.
3. The 2020 State of the OCTOVERSE [Электронный ресурс] – Режим доступа до ресурсу: <https://octoverse.github.com>.
4. PHP 4 Changelog [Электронный ресурс] – Режим доступа до ресурсу: <https://www.php.net/ChangeLog-4.php#4.0.0>.
5. PHP 5 Changelog [Электронный ресурс] – Режим доступа до ресурсу: <https://www.php.net/ChangeLog-5.php#5.4.0>.
6. Callum H. PHP Traits: Good or Bad? [Электронный ресурс] / Hopkins Callum – Режим доступа до ресурсу: <https://www.sitepoint.com/php-traits-good-or-bad/>.
7. Makarov A. ARE TRAITS EVIL? [Электронный ресурс] / Alexander Makarov – Режим доступа до ресурсу: <https://en.rmcreative.ru/blog/are-traits-evil/>.
8. PHP 8: что нового, туда ли движется, что будет дальше [Электронный ресурс] – Режим доступа до ресурсу: <https://www.youtube.com/watch?v=QSszmWIrRyw&t=6624s>.

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

Бойко М.Ю.

Навчально-науковий інститут інформаційних технологій

Державний університет телекомунікацій

В роботі досліджено технології доповненої реальності і їх використання. Наведені основні переваги та недоліки.

Додатки та пристрої доповненої реальності існують вже кілька десятиліть, але тільки недавно стали доступні технології, необхідні для розкриття потенціалу. По суті, вони перетворюють обсяги даних і аналітику в зображення або анімацію, які накладаються на реальний світ. Ключовими технологіями є: інтелектуальне відображення, тривимірна реєстрація та інтелектуальна взаємодія.

1. Тривимірна реєстрація

3D-датчики безпосередньо фіксують координати видимих точок на поверхні об'єкту. Використовуючи кілька тривимірних зображень об'єкта, отриманих з різних точок зору, обчислюється попарне перекриття тривимірних даних і виходить глобальна оптимізована форма. Ця технологія особливо підходить для 3D-реконструкції, тобто визначення тривимірні форми довільних об'єктів. Форма об'єкта може використовуватися в 3D-зіставленні для перевірки якості об'єктів або для розпізнавання положення об'єктів. Наприклад: MVТес HALCON.

2. Інтелектуальна технологія відображення

«Розумні окуляри» за допомогою відповідної технології забезпечує екран / дисплей комп'ютера перед очима людини для представлення даних з системи фонові інформації (Наприклад: Google Glass, Hololens). Настільні дисплеї пристроїв (ПК, смартфони, планшети), зіставляють інформацію захоплену з камер в тривимірну віртуальну модель і в кінцевому підсумку відображаються за допомогою різних платформ.

3. Інтелектуальна технологія взаємодії

У системах AR існує безліч інтелектуальних взаємодій, включаючи взаємодії з апаратними пристроями, взаємодії з місцем розташування на основі тегів або іншої інформації [1]. З розвитком технології інтелектуальної взаємодії, доповнена реальність не тільки накладає віртуальну інформацію на реальні сцени, але також реалізує взаємодію між людьми та віртуальними об'єктами.

Поширені варіанти використання доповненої реальності.

Освіта: доповнена реальність може поліпшити матеріли візуальними та іншими сенсорними компонентами (SMART фліпчарт), які надають учням додаткову інформацію і допомагають пояснювати складні предмети.

Продаж. На сьогодні можна віртуально приміряти або випробувати різні товари перед покупкою: додаток Sephora дозволяє переглядати косметику в AR на вашому обличчі; ІКЕА пропонує можливість «побачити» меблі в своєму будинку; марки фарб дозволяють віртуально переглядати кольору на стінах; Warby Parker дозволяє «приміряти» оправу для окулярів, не відвідуючи магазин

і не замовляючи зразки. QR-код на продукті або дисплеї в магазині може надати покупцям додаткову інформацію про товар або послугу[2].

Охорона здоров'я: студенти та практикуючі лікарі можуть вивчати складні методи і процедури за допомогою технології доповненої реальності, яка може дозволити їм візуалізувати тонкощі роботи органів і систем або етапи хірургії.

Виробництво: AR в виробничих умовах може надати співробітникам важливу інформацію, необхідну їм для виконання своєї роботи, таку як накладення інформації про температуру, статистику і безпеки на продукт, обладнання або механізми.

Переваги доповненої реальності:

- Поліпшує взаємодію і забезпечує кращий користувальницький досвід;
- AR стирає межу між тим, що є реальним, і тим, що генерується цифровим способом;
- Тестування критичних ситуацій, щоб підтвердити їх успіх, не впроваджуючи їх в реальному часі;
- Покрокові інструкції та вказівки подаються більш точно через доповнені елементи (3D-моделі, текст, картинки, відео), ніж звичайні відео;
- Безпечне навчання.

Основними недоліками є:

- Дорогими та складними в обслуговуванні ;
- Відсутність конфіденційності;
- Несанкціонована доповнена реклама;
- Спам.

Технології доповненої реальності ще належить вирішити безліч проблем. Поточний метод реєстрації стеження може використовувати тільки невеликий обсяг інформації, такий як характерна точка. Інформація, яка призводить до неповного розуміння системи для навколишнього середовища. З точки зору технології відображення, розмір і ціна пристроїв (очок, настільні дисплеї) доповненої реальності, які можуть забезпечити користувачам високе почуття занурення, не можуть задовольнити потреби громадськості. В цьому режимі ще належить вивчити більш природну і багато користувачів технологію взаємодії з доповненою реальністю. У найближчі кілька років застосування технології доповненої реальності, особливо в мобільних інтелектуальних терміналах, з'явиться у великій кількості. В майбутньому інтелектуальні пристрої та додатки, які можуть повністю розкрити переваги технології доповненої реальності, допоможуть зробити більш реалістичний світ інтеграції для людини.

Список використаних джерел

1. <https://iopscience.iop.org/article/10.1088/1742-6596/1237/2/022082/meta> - [Електронний ресурс] - An overview of augmented reality technology;
2. <https://www.fierceelectronics.com/electronics/what-augmented-reality-0> - [Електронний ресурс] - What is Augmented Reality?.

ОЦІНКА АЛГОРИТМІВ ВИДІЛЕННЯ ІНФОРМАТИВНИХ ОЗНАК ТА ЇХ ПОРІВНЯННЯ

Клименко Н.О.

Навчально-науковий інститут інформаційних технологій
Державний університет телекомунікацій

У даній роботі проведено порівняльний аналіз та вибір алгоритмів виділення ознак атрибутів класифікації на прикладі програм FTP, Web, Mail, SSH, Skype на етапі навчання (створення моделі класифікатора), а також здійснено порівняльну оцінку ефективності алгоритмів класифікації методами МН на етапі тестування.

Для аналізу було підготовлено два набори даних, що містять мережеві пакети, розбиті по потокам. Класифіковані потоки були розділені наступним чином: 66% від вихідних даних використовувалися як навчальний набір, решта 34% - для тестування і його оцінки [1,с.827].

В якості першого алгоритму виділення атрибутів трафіку, представленого в табл. 1. використовувався метод ранжирування на основі інформаційного виграшу InfoGain.

Таблиця 1 - Підготовлені дампи трафіку

Дамп трафіка	Кількість потоків мережевого трафіку по групам						Загальна кількість потоків
	Web (HTTP, HTTPS)	Mail (SMTP, IMAP)	FTP (FTP-DATA, FTP-COMMANDS)	SSH	Skype	P2P	
Навчаючий	3356	2209	2311	3975	2525	4677	19053
Загальний	1698	1151	1159	1849	1212	2315	9384
Web	1696	-	-	-	-	-	1696
Mail	-	1092	-	-	-	-	1092
FTP	-	-	1146	-	-	-	1146
SSH	-	-	-	2023	-	-	2023
Skype	-	-	-	-	1261	-	1261
Pear-to-Pear	-	-	-	-	-	2308	2308

Результати застосування алгоритму InfoGain, розташовані від гіршого до кращого, з урахуванням 10-кратної перехресної перевірки представлені на рис.1.

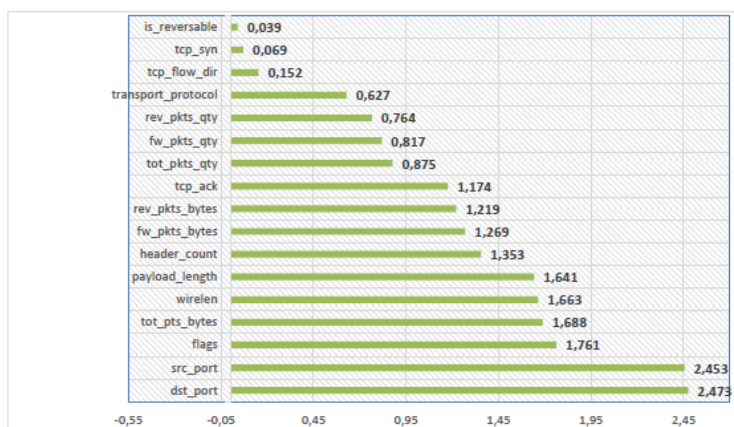


Рисунок 1 - Результат застосування алгоритму виділення атрибутів InfoGain

З рисунка видно, після 14-го рангу відбувається різке падіння інформаційного виграшу від використання атрибута. Встановити причини цього допомагає аналіз значень і діапазону зміни даних атрибутів. Так атрибут `tcp_flow_dir` показує, в якому напрямку рухається потік. При цьому в кожному використовуваному класі приблизно половина потоків - що входять, а половина – вихідні, що не дозволяє характеризувати клас даними атрибутом.

Атрибут `tcp_syn`, що відображає відсоток потоків, для яких встановлено прапор SYN, відповідає за синхронізацію номерів послідовності: його середнє значення незмінно і дорівнює нулю. Атрибут `is_reversable`, який показує, чи є потік двостороннім чи ні, в даному випадку завжди дорівнює одиниці, так як майже всі потоки двосторонні. Таким чином, атрибути `tcp_syn`, `tcp_flow_dir`, `is_reversable` не мають значного інформаційного виграшу і надалі можуть не використовуватися.

При пошуку і виділення ознак на навчальному наборі також використовувався алгоритм CFS, за допомогою якого було оцінено в цілому 151 підмножина. Результати вибору ознак з використанням алгоритму CFS досить передбачувані і в цілому збігаються з ознаками, обраними алгоритмом InfoGain. Третій використаний для виділення атрибутів алгоритм – обгортковий Wrapper - застосовується тільки спільно з цільовим алгоритмом класифікації. Одна з основних складових алгоритму виділення атрибутів – оцінка підмножин - була реалізована за допомогою класифікації і оцінки результатів на обраних параметрах класифікатора [2,с.322]

Оскільки при застосуванні різних цільових класифікаторів можливий вибір різних атрибутів, а також щоб уникнути «перенавчання» під конкретний класифікатор обгортковий алгоритм використовувався з різними класифікаторами табл.2. Такі атрибути, як `tot_pkts_qty`, `tot_pkts_bytes`, `rev_pkts_qty`, `fw_pkts_bytes`, `is_reversable`, `header_count`, `tcp_flow_dir` не були обрані обгорткового методом при використанні різних цільових класифікаторів.

Таблиця 2. - Атрибути, обрані обгорткового алгоритмом Wrapper, при використанні різних класифікаторів

	C4.5(J48)	SVM	AdaBoost	Bagging	Naïve Bayes
<code>rev_pkts_bytes</code>		+			+
<code>fv_pkts_qty</code>		+			+
<code>transport_protocol</code>	+	+			
<code>src_port</code>	+	+	+	+	+
<code>dst_port</code>	+	+		+	+
<code>wirelen</code>		+			+
<code>tcp_syn</code>		+			+
<code>tcp_ack</code>		+			+
<code>flags</code>	+	+		+	+
<code>payload_lenght</code>	+	+		+	+

Дослідження показують, що використання обгорткового алгоритму вибору ознак є ресурсномісткою обчислювальною операцією, яка при великій кількості

атрибутів займає тривалий час. Найбільш тривалі обчислення відзначалися при використанні алгоритму SVM: він реалізується лише для бінарної класифікації. Коли кількість класів перевищує два, SVM буде безліч моделей класифікаторів за принципом «один проти всіх», що збільшує час, необхідний для побудови класифікатора.

Список використаних джерел:

1. Yong Tang, Bin Xiao, and Xicheng Lu, «Using a bioinformatics approach to generate accurate exploit-based signatures for polymorphic worms», *Computers & Security*, vol. 28, no. 8, p. 827–842, Elsevier, 2019.

2. Denis Zuev and Andrew W. Moore, «Traffic Classification using a Statistical Approach», in *Proceedings of the 6th international conference on Passive and Active Network Measurement (PAM'05)*, p. 321-324, Boston, MA, USA, 2017.

ІОТ ДЛЯ РОЗУМНИХ МІСТ ТА ПРОМИСЛОВОСТІ

Дубчак Дмитро Костянтинович

Державний університет телекомунікацій

Навчально-науковий інститут інформаційних технологій

Постановка задачі. ІоТ простими словами означає мережу датчиків і «розумних» пристроїв, які збирають інформацію, обмінюються нею між собою і з хмарним сховищем, а платформа аналізує дані та видає відповідні команди

Мета дослідження. Аналіз сфери для виявлення переваг та подальшого потенціалу розвитку ІоТ в містах та промисловості.

Результати дослідження. Промисловий Інтернет речей виділяється масштабами і призначенням. ІоТ — це комп'ютерні мережі, до яких підключають фізичні промислові об'єкти зі встановленими датчиками, сенсорами і ПЗ. Що це дає? Можливість збирати та відправляти інформацію, дистанційно керувати процесами, автоматизувати виробництво. Отже, головне завдання ІоТ — спростити складні робочі процеси й підвищити рентабельність виробництва.

Сьогодні ІоТ в промисловості насамперед впроваджують великі компанії. Причина проста: невеликим стартапам часто немає звідки взяти гроші на подібні вкладення. Це одна з основних причин, чому промисловий Інтернет речей ще не підкорив абсолютно всі галузі. Другий неоднозначний момент — безпека даних, які потрапляють у мережу.

ІоТ в промисловості використовується буквально всюди, де є виробництво. На фермах — датчики контролюють наявність і якість води та корму у тварин; на заводах — щоб моніторити стан обладнання й запобігати поломкам або простоям; в енергетиці — щоб автоматично збирати дані лічильників та ін. Платформа допомагає керувати SIM-картами в смартпристроях: моніторити пристрої онлайн, збирати й обробляти статистику, контролювати витрати в особистому кабінеті.

Сьогодні чимало мегаполісів перенаселені. В цих умовах не завжди вдається ефективно справлятися з такими завданнями як забезпечення безпеки, прибирання сміття, ефективне використання комунальних ресурсів та ін. Тому в містах все частіше впроваджують інформаційні системи - вони забезпечують

збір і передачу даних представникам управління, дозволяють налагодити зворотній зв'язок між городянами і адміністрацією. Джерелами для отримання цих даних можуть слугувати різноманітні датчики, сенсори, відеокамери і т. д.

Висновки та перспективи. По мірі того, як кількість підключених пристроїв продовжує зростати, наше середовище для життя і роботи стане наповнюватися розумними продуктами – за умови, що ми готові прийняти компроміси щодо безпеки та конфіденційності. Адже ризики існують завжди і всюди. Наявність величезної мережі, яка контролює весь навколишній світ, глобальна відкритість даних та інші особливості можуть носити не лише позитивний, а й негативний характер. Однак, технології продовжать активно розвиватися, поглинаючи всі сумніви щодо доцільності та безпеки їх застосування в цілому.

Список використаних джерел

1. Інтернет речей в промисловості//<https://hub.kyivstar.ua/>
2. IOT – все, що потрібно знати про інтернет речей і про майбутнє сучасної цивілізації//<https://www.everest.ua/>

СИСТЕМА ЗБОРУ ІНФОРМАЦІЇ – ТЕХНОЛОГІЯ BIG DATA

*Вовчанська Діана Миколаївна
Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій*

В даний час соціальні мережі - є динамічними джерелами різномірної інформації, що відбиває різні процеси, які виникають в реальному суспільстві. Для їх кількісного аналізу застосовуються спеціальні технології, орієнтовані на збір і обробку величезних обсягів неструктурованих даних, до яких відноситься технологія BigData. Особливості адаптації технологій BigData до соціальних мереж пов'язані з необхідністю обліку топологічної структури віртуального суспільства користувачів. Дослідження ефективності збору та обробки великих обсягів даних з соціальних мереж.

До основних вимог, що пред'являються до краулера можна віднести наступні[1,с.19]:

1) Ввічливість. Потрібно дотримуватися накладаються сервером правила, що регулюють частоту звернення і запитувані ресурси.

2) Розподіленість і Масштабованість. Для обробки великих обсягів даних потрібно можливість функціонування краулер на декількох машинах. При цьому потрібно здатність збільшення робочого навантаження, шляхом додавання нових машин або збільшення пропускну здатності.

3) Можливість розширення. Потрібно «легкість» додавання або зміни компонентів краулера. Наприклад, зміна алгоритму впливає на роботу системи, підтримка нового формату даних або мережевого протоколу передачі даних.

4) Стійкість. Система повинна стабільно обробляти різного роду мережеві помилки, що неминуче виникають при обміні даних з серверами. при

зупинці роботи, краулер повинен підтримувати відновлення роботи з останньої точки.

5) Продуктивність. Робота з великими обсягами даних вимагає ефективного використання всіх ресурсів машини.

6) Якість. Зібрана краулер база даних документів повинна задовольняти вимогам клієнтів системи. Наприклад, при вирішенні задач моніторингу мережі, база даних повинна містити свіжі копії сторінок.

Конкретні вимоги до системи залежать від специфіки розв'язуваної задачі. Однак при роботі з сайтами, можна виділити дві головні вимоги до всіх систем збору даних: ввічливість і стійкість. Сайти накладають явні і неявні обмеження на число звернень до них. Більшість сайтів не рекомендують встановлювати більше ніж одне з'єднання з ними, при цьому між двома послідовними з'єднаннями повинен бути витриманий часовий інтервал, достатній для того щоб не створювати сайту 'проблем. Ці обмеження вимагають ефективного використання доступного числа звернень до сайтів, щоб якість одержуваної бази було якомога вище [2,с.238].

Збір даних з мільярдів сайтів вимагає реалізації розподіленої системи збору даних, при якій ресурси кожної окремої машини будуть використовуватися максимально ефективно і самі машини ефективно обмінюються даними один з другом. Однак якщо специфіка розв'язуваної краулер завдання вимагає збору даних невеликого обсягу з невеликого числа сайтів, то реалізація розподіленої системи не є обов'язковою.

Список використаних джерел

1. Shubham Sharma. Big Data Landscape/ Shubham Sharma // International Journal of Scientific and Research Publication. – 2016. – №6.
2. White T. Hadoop: The Definite Guide/ Tom White. – Boston: O'Reilly Media, Inc., 2018. – 657 с.

АНАЛІЗ МЕТОДІВ ПРОГНОЗУВАННЯ ЕЛЕКТРОСПОЖИВАННЯ ПРОМИСЛОВОГО ПІДПРИЄМСТВА

Ковальов Михайло Юрійович

Державний університет телекомунікацій

Навчально-науковий інститут інформаційних технологій

Прогнозування величини електроспоживання промислового підприємства є важливою науково-технічною задачею. Необхідність точного прогнозування електроспоживання обумовлена технологічними і економічними причинами. У великих енергоємних виробництвах частка плати за електроенергію в собівартості продукції може досягати десятків відсотків, а в умовах ринкової економіки собівартість продукції підприємства буде визначати його конкурентоспроможність.

Для того щоб вибрати оптимальний метод для подальшого побудови на його основі прогнозної моделі електроспоживання промислового підприємства, необхідно, перш за все, чітко сформулювати ряд вихідних вимог: мета прогнозу, інтервал прогнозування, точність прогнозу, адаптивність прогнозної

моделі, її швидкодію і т.д. Вихідні вимоги будуть визначаються діючими правилами оптового ринку електроенергії і потужності України.

Споживання електричної енергії підприємством залежить від множини мінливих чинників. У їх число можуть входити (в залежності від характеристики технологічного процесу підприємства):

1. Параметри навколишнього середовища (температура повітря, наявність опадів, хмарність, швидкість та напрям вітру);
2. Обсяг випуску продукції, пуск / зупинка технологічних ланцюжків;
3. Цінова ситуація на ринку електроенергії (в разі можливості регулювання графіка навантаження) ;
4. Проведення планових і позапланових ремонтів;
5. Аварійні ситуації, збої в роботі технологічних ланцюжків.

Оптимальна прогнозна модель повинна враховувати як можна більше факторів, що впливають. Крім того, фактори можуть бути взаємозалежними один від одного. Тому визначити «внесок» кожного фактора у зміну величини споживання електроенергії в складній, постійно мінливих системі, якою є промислове підприємство, досить важко.

Методи прогнозу електроспоживання, що відносяться до статистичних методів, при прогнозуванні в режимі, близькому до реального часу, вимагають постійної перебудови параметрів, а найчастіше, і типів моделі прогнозування. Це обумовлює складність їх використання для вирішення завдань автоматизованого прогнозування. Крім того, для статистичних методів прогнозу необхідні великі масиви вихідних даних [1,с.28-29], яких може не бути у, наприклад, новостворюваних підприємств. Статистичні методи, крім цього, пов'язані з великою кількістю обчислень [2, с.232].

В умовах ринкової економіки, коли обсяги виробництва продукції підприємства, а значить і споживання ним електроенергії, багато в чому визначаються кон'юнктурою ринку, статистичні методи практично не дозволяють враховувати коротко- і середньострокові тенденції в споживанні електричної енергії підприємством.

Методи, засновані на інтуїтивних оцінках експертів, не піддаються автоматизації в процесі роботи підприємстві на ринку електроенергії. Істотним недоліком таких методів є і те, що точність прогнозу дуже сильно залежить від кваліфікації експерта. Моделі прогнозування, засновані на ШНМ, мають можливість навчання, що дозволяє адаптувати нейронної мережі свої синаптичні ваги до змін навколишнього середовища. Більш того, для роботи в нестационарному середовищі (а саме таким середовищем є процес споживання електроенергії підприємством) можуть бути створені нейронні мережі, що змінюють синаптичні ваги в режимі близькому до реального часу Ці властивості нейронних мереж, а так само їх висока відмовостійкість, разом з нелінійністю (а значить можливістю точного опису складних функцій), дозволяють зробити висновок про те, що найкращим за сукупністю характеристик методом для автоматизованого короткострокового прогнозування електроспоживання буде методика, заснована на ШНМ [3,с.164].

Використання ШНМ дозволить враховувати короткострокові тенденції в споживанні електроенергії підприємством, дозволить автоматизувати процес здійснення прогнозу. Крім того, прогнозна модель, заснована на ШНМ, менш інших моделей залежить від наявності повного обсягу вхідних даних.

У той же час для усунення недоліків, пов'язаних зі складністю настройки внутрішньої конфігурації нейронної мережі доцільно застосувати гібридну систему, в якій настройка буде проводитися за допомогою методу генетичного відбору.

Список використаних джерел:

1. Ивченко, В. Д. Применение нейросетевых технологий в различных областях науки и техники/ В. Д. Ивченко, С. С. Кананадзе// Приборы и системы. Управление, контроль, диагностика. - 2019. - № 6. - С. 28 - 29.

2. Каллан, Р. Основные концепции нейронных сетей/ Р. Каллан. - М.: Издательский дом Вильямс, 2017. - 288 с.

3. Hirota, K. A Disturbed Model of Fuzzy Set Connectives/ K. Hirota, W. Pedrycz// Fuzzy Sets and Systems. -2018. - V. 68. - P. 157 - 170.

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ

Герасимчук М.В.

*Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій*

У сучасному суспільстві центр економічного розвитку переноситься з матеріальних сфер виробництва (енергетично-сировинної базис) на наукомісткі та високотехнологічні сфери. Поступальний рух, в тому числі в області економіки, визначається сьогодні та буде визначатися в найближче десятиліття вдосконаленням інформаційних технологій.

Інформаційне суспільство - це етап соціальної еволюції людства. Рушійною силою інформаційного суспільства є знання - інтелектуально-інформаційний ресурс (ІВР). Це нова і незвична категорія, активно включається сьогодні у сферу діяльності людини.

Щодо ІВР людині невідомі закони збереження або обмеження, так характерні для матеріально-енергетичної (матеріальної) субстанції. За багатьма параметрами (динаміка розвитку, ефективність впровадження та ін.) ІВР має незаперечні переваги в порівнянні з матеріальними ресурсами.

Сучасні обсяги даних надзвичайно великі, і людина просто не в змозі проаналізувати їх самостійно, хоча необхідність проведення такого аналізу цілком очевидна, адже в цих "сирих даних" є важливі знання, які можуть бути використані для різноманітних цілей та прийняття рішень.

Традиційна математична статистика, довгий час претендувала на роль основного інструменту аналізу даних, проте з плином часу вже не відповідала проблемам, що з'являлись. Тому виникла необхідність у розвитку нових сучасних методологій обробки та аналізу даних. Такою новою методологією і став інтелектуальний аналіз даних ІАД. Причини популярності ІАД такі:

- Надзвичайно стрімке накопичення даних (рахунок йде вже на ексабайти);
- Загальна комп'ютеризація бізнес-процесів;
- Проникнення Інтернету в усі сфери діяльності;
- Прогрес в області інформаційних технологій: вдосконалення СУБД і сховищ даних;
- Прогрес в області виробничих технологій: стрімке зростання продуктивності комп'ютерів, накопичувачів, впровадження Grid систем.

В даний час ІАД існує у двох іпостасях. Ряд фахівців робить акцент на обробці надвеликих обсягів даних. Тут пред'являються підвищені вимоги до швидкодії алгоритмів, але на шкоду оптимальності результатів.

Інша група фахівців концентрує увагу на глибині розкопки даних. У розумінні цієї групи основні відмінності технології наступні:

- ІАД - це завжди суто багатовимірні завдання - пошук зв'язку між значенням цільового показника і набором значень інших показників БД.

- Технології ІАД призначені для обробки різних видів інформації, тобто поля можуть бути представлені кількісними, якісними та текстовими змінними.

- Технологія ІАД, на відміну від традиційних статистичних методів, не претендує на пошук взаємозв'язків, характерних для повного обсягу даних (всієї вибірки). Шукаються правила, що зв'язують значення показників, для підвбірок даних. При цьому ці правила завжди високоточні, а не розмиті.

- Алгоритми ІАД виробляють пошук зазначених вище підвбірок даних і точних взаємозв'язків для цих підвбірок в автоматичному режимі.

Таким чином, ключові слова ІАД: точність, багатовимірність, різнотипність даних, автоматичний пошук. Тут, звичайно, ще потрібно додати важливу вимогу до інтерпретування одержуваного результату.

До методів і алгоритмів ІАД належать такі:

- штучні нейронні мережі;
- дерева рішень;
- методи найближчого сусіда і к-найближчого сусіда;
- метод опорних векторів;
- Баєсові мережі;
- лінійна регресія та кореляційно-регресійний аналіз;
- ієрархічні та неієрхічні методи кластерного аналізу;
- методи пошуку асоціативних правил, зокрема алгоритм Аргіогі;
- метод обмеженого перебору;
- еволюційне програмування і генетичні алгоритми.
-

Більшість вищезазначених методів ІАД були розроблені у межах теорії штучного інтелекту. Єдиної думки щодо того, які задачі необхідно зараховувати до ІАД, немає.

Для ознайомлення, розглянемо декілька методів та алгоритмів, описаних вище:

Класифікація (Classification). Це найпростіша і найпоширеніша задача ІАД. В результаті розв'язання задачі класифікації виявляються ознаки, які

характеризують групи об'єктів досліджуваного набору даних – класи; за цими ознаками новий об'єкт можна зарахувати до того чи іншого класу. Для розв'язання задачі класифікації можуть використовуватися методи: найближчого сусіда (Nearest Neighbor); к-ближнього сусіда (k-Nearest Neighbor); Баєсових мереж (Bayesian Networks); індукції дерев рішень; нейронних мереж (neural networks).

Кластеризація (Clustering). Кластеризація є логічним продовженням ідеї класифікації. Це є складніша задача. Особливість кластеризації полягає у тому, що класи об'єктів спочатку не визначені. Результатом кластеризації є розбиття об'єктів на групи. Прикладом методу задачі кластеризації є особливий вид нейронних мереж (карти Кохонена), що самоорганізуються без вчителя.

Асоціація (Associations). У процесі розв'язання задачі пошуку асоціативних правил відшукуються закономірності між зв'язаними подіями в наборі даних. Відмінність асоціації від двох попередніх задач ІАД: пошук закономірностей здійснюється не на основі властивостей об'єкта, що аналізується, а між кількома подіями, які відбуваються одночасно.

Відомий алгоритм пошуку асоціативних правил – алгоритм Apriori.

Системи інтелектуального аналізу даних застосовуються як масовий продукт для бізнес-додатків і як інструменти для проведення унікальних досліджень (генетика, хімія, медицина тощо).

Не зважаючи на достатню кількість методів ІАД, пріоритет поступово зміщується у бік логічних алгоритмів пошуку в даних причинно-наслідкових правил. За їх допомогою розв'язуються задачі прогнозування, класифікації, розпізнавання образів, сегментації БД, здобування з даних “схованих” знань, інтерпретації даних, установлення асоціацій в БД тощо. Результати таких алгоритмів ефективні й легко інтерпретуються.

До того ж головною проблемою логічних методів виявлення закономірностей є проблема перебору варіантів за прийнятний час. Відомі методи або штучно обмежують такий перебір (алгоритми КОРА, WizWhy), або будують дерева рішень (алгоритми CART, CHAID, ID3, See5, Sipina та ін.), що мають принципові обмеження ефективності пошуку причинно-наслідкових правил. Інші проблеми пов'язані з тим, що відомі методи пошуку логічних правил не підтримують функцію узагальнення вищерозглянутих правил і функцію пошуку оптимальної композиції таких правил. Вдале розв'язання зазначених проблем може бути покладене в основу нових методик ІАД та відповідних розробок.

Список літератури

1. Hand DJ, Manila H, Smyth P. Principles of data mining. Cambridge (MA): The MIT Press, 2001
2. Hand DJ, Blunt G, Kelly MG, et al. Data mining for fun and profit. Stat Sci 2000; 15(2): 111–31
3. Sarra, A., Fontanella, L., Di Zio, S.: Identifying students at risk of academic failure within the educational data mining framework. Soc. Indic. Res. **146**(1–2), 41–60 (2019)

WEBASSEMBLY

*Печериця Віталій Валентинович
Держаний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій*

Ця робота ілюструє інструмент який створений для швидкого виконання коду в браузері під назвою WebAssembly.

Проблеми, якою вирішується даною (щодо нової) технологією. Проблема це - швидкість виконання коду в браузері. Швидко - це означає, «швидше ніж JavaScript», в ідеалі настільки швидко, наскільки дозволяє наявний у нас процесор.

Крім того, історично, навколо цієї проблеми поступово виникли важливі додаткові вимоги:

Zero configuration - це повинно бути рішення яке не потрібно встановлювати в машину, нічого крім браузера.

Безпечно - нова технологія не повинна створювати нових загроз.

Крос-платформенно - браузери працюють на всіх основних процесорах, включаючи мобільні платформи.

Зручно для розробників - тобто для що б був вищий поріг входу в технологію.

Існувало безліч варіантів виконання коду в браузері. Можна сказати, що на цьому полі є переможці і переможені.

Переможці: це, безумовно, JavaScript; двигун V8, який зробив JS таким швидким; а також HTML5.

WebAssembly (або Wasm) - це бінарний формат, який запускається в браузері, віртуальна машина, і результат компіляції з мови високого рівня.

Wasm це не мова програмування, подібно до того як байт-код Java це не мова програмування, а результат компіляції і запускається блок коду.

Хтось дуже розумний сказав, що назва web assembly (тобто «асемблер для інтернету») повністю неправильне, тому що це не асемблер (не мова програмування) і він ніяк не пов'язаний з Інтернетом (бо це просто віртуальна машина).

Напевно, це один з головних питань - «А як я можу використовувати Wasm?»

Уже зараз WebAssembly активно застосовується:

- Ігри, ігрові движки, движки фізики, VR / AR - наприклад, Godot, Doom 3;
- Емулятори, віртуальні машини - наприклад, DOSBox;
- Графічні / 3D редактори - Figma, AutoCAD;
- Веб-клієнти для фінансових торгових майданчиків;
- Кодеки і фільтри аудіо / відео - наприклад, ffmpeg;
- Бази даних - наприклад, sqlite.

Продуктивність Wasm була одним з його головних «продають» чинників, але що з нею відбувається насправді?

У порівнянні з JavaScript, виходить, що в середньому Wasm швидше, але в кожному окремому випадку потрібно робити порівняння JS / Wasm, тому що може статися й у багато разів краще, і в кілька разів гірше. Також це може сильно залежати від використовуваного браузера.

Насправді, пікова продуктивність JS і Wasm однакова, оскільки обидва в підсумку перетворюються в рідний код процесора. Але JS набагато легше втрачає в продуктивності, а Wasm забезпечує більш «рівний» підхід.

Як правило, Wasm добре показує себе на об'ємних обчисленнях. Там де багато операцій з пам'яттю, Wasm програє.

Отже, WebAssembly цілком можна використовувати, він уже два роки як «production ready».

Застосування Wasm цілком може дати деяке прискорення, в порівнянні з аналогічним кодом на JavaScript, але завжди потрібно перевіряти, вийшов чи приріст швидкості.

Підтримка Wasm з боку мов програмування постійно розвивається.

Ну і найголовніше, WebAssembly кілька «змінив ландшафт» веба - надав нам нові сценарії використання, які ми можемо реалізувати в своїх додатках.

Література:

1. WebAssembly [Електронний ресурс] – Режим доступу до ресурсу: <https://developer.mozilla.org/ru/docs/WebAssembly>

2. WebAssembly RoadMap [Електронний ресурс] – Режим доступу до ресурсу: <https://webassembly.org/roadmap/>

СУТНІСТЬ ТА ОСОБЛИВОСТІ APACHE CORDOVA

Печериця Віталій Валентинович

Держаний університет телекомунікацій

Навчально-науковий інститут заочної та дистанційної освіти

Apache Cordova - це фреймворк з відкритим кодом, який дозволяє веб-розробникам використовувати вміст HTML, CSS та JavaScript для створення власного додатку для різноманітних мобільних платформ.

Cordova приймає вашу веб-програму та відображає її у власній програмі WebView. WebView - це компонент програми (наприклад, кнопка або панель вкладок), який використовується для відображення веб-вмісту в рідній програмі. Ви можете уявити WebView як веб-браузер без будь-яких стандартних елементів інтерфейсу користувача, таких як поле URL-адреси або рядок стану. Веб-програма, що працює в цьому контейнері, подібна до будь-якої іншої веб-програми, яка працює в мобільному браузері - вона може відкривати додаткові HTML-сторінки, виконувати код JavaScript, відтворювати медіа-файли та спілкуватися з віддаленими серверами. Цей тип мобільних додатків часто називають гібридним додатком.

Зазвичай веб-програми виконуються в пісочниці, тобто вони не мають прямого доступу до різних апаратних та програмних функцій пристрою. Хорошим прикладом цього є база даних контактів на вашому мобільному пристрої. Ця база даних імен, телефонних номерів, електронних листів та інших

фрагментів інформації недоступна для веб-програми. Окрім того, що надає базовий фреймворк для запуску веб-програми в межах власної програми, Кордова також надає API-інтерфейси JavaScript, що дозволяють отримати доступ до широкого спектру функцій пристрою, таких як база даних контактів. Ці можливості виявляються завдяки використанню колекції плагінів. Плагіни забезпечують зв'язок між нашим веб-додатком та власними функціями пристрою. Команда Ionic пішла на крок далі і створила Ionic Native з інтерфейсами TypeScript для понад 200 найпоширеніших плагінів та корпоративними версіями для команд, які хочуть отримати перевагу від Ionic для управління поточними оновленнями, виправленнями безпеки, сумісністю та іншими аспектами. власного доступу до пристрою.

Розробників часто бентежить різниця між Apache Cordova і PhoneGap. Для того, щоб усунути цю плутанину, нам слід зрозуміти витoki цього проекту. Наприкінці 2008 року кілька інженерів з Канади, компанія з веб-розробки Nitobi, відвідали табір розробки iPhone для офісів Adobe у Сан-Франциско. Вони дослідили ідею використання власного WebView як оболонки для запуску своїх веб-додатків у рідному середовищі. Експеримент спрацював. Протягом наступних кількох місяців вони розширили свої зусилля та змогли використати це рішення для створення основи. Вони назвали проект PhoneGap, оскільки він дозволив веб-розробникам подолати розрив між їх веб-програмами та власними можливостями пристрою. Проект продовжував дозрівати, і було створено більше плагінів, що дозволяють отримати більше функціональних можливостей по телефону. Інші учасники долучились до зусиль, розширивши кількість мобільних платформ, які вона підтримувала.

Apache Cordova проти Adobe PhoneGap

Оскільки існують як Apache Cordova, так і Adobe PhoneGap, плутати проекти досить легко. Ця проблема з іменами може викликати розчарування при дослідженні проблеми під час розробки та необхідності пошуку за допомогою Cordova і PhoneGap як ключових слів, щоб знайти рішення, або навіть читання відповідної документації, оскільки два проекти настільки переплетені.

Хороший спосіб зрозуміти різницю - подумати про те, як Apple має свій браузер Safari, але він базується на механізмі відкритого коду WebKit. Те саме справедливо і тут: Cordova - це версія фреймворку з відкритим кодом, тоді як PhoneGap - це фірмова версія Adobe. Зрештою, між цими зусиллями мало різниці. Існують деякі незначні відмінності в інтерфейсах командного рядка, але функціональність однакова. Єдине, що ви не можете зробити, це змішати два проекти в одному додатку. Хоча це не настільки небезпечно, як коли Мисливці за привидами перетнули свої потоки, використання Кордови та PhoneGap в одному проекті не призведе до нічого, крім проблем.

Отже, використання Cordova дозволяє нам взяти наш веб-додаток і зробити його мобільним додатком, який ми зможемо подати в магазини додатків.

Література:

3. Cordova [Електронний ресурс] – Режим доступу до ресурсу: <https://cordova.apache.org/>

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

*Аврамчук Артем Ігорович,
Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій*

Наше сьогодні – епоха відкриття та технологій, результат об'єднання важкої праці безлічі спеціалістів різних сфер і напрямків. Досягти цього рівня розвитку було в неможливо без активного обміну інформацією та аналізу напрацювань між фахівцями в різних частинах земної кулі. Саме активне використання різноманітних інформаційних технологій та штучного інтелекту зокрема призводять до полегшення щоденного життя.

Небагато існує термінів на сьогодні, про яких недостатнє розуміння, проте поняття штучного інтелекту відноситься саме до таких. Проведені опитування доводять, що навіть у провідних очільників бізнесу відсутнє конкретне уявлення про штучний інтелект, а пересічні громадяни приймають його за дужих роботів або над розумних приладів.

Він трактується дуже абстрактно, як: здатність системи самостійно підбирати найбільш якісний варіант вирішення проблеми з набору наперед запропонованого набору варіантів; вміння вирішувати складні завдання; здатність до навчання, узагальнення і аналогій; можливість взаємодії із зовнішнім світом шляхом спілкування, сприйняття й усвідомлення сприйнятого [1].

Штучний інтелект – це те, що радикально перемінило всесвіт. Вектор очікуваних трансформувальних – результат вибору та точки зору його розробників. Поглянемо детальніше, які перспективи приведе за собою ера штучного інтелекту та технонауки взагалі.

Штучний інтелект може підняти потенціал всесвітньої економіки. За даними PwC, до 2030 року він здатний укріпити її на 15,7 трлн дол. Кращі здобутки від ШІ прогнозують для Китаю (ріст ВВП на 26% у 2030 році) та Північної Америки (збільшення ВВП на 14,5%), що рівнозначно 10,7 трлн дол.

Провідними чинниками економічних змін від впровадження штучного інтелекту є автоматизація робочої сили, яка до 2030 року має додати до 11% світового ВВП або біля 9 трлн дол, та інновації у царині товарів та послуг, які до 2030 року можуть збільшити ВВП приблизно на 7% або на 6 трлн дол.

Виділяють три основні напрямки, де алгоритми ШІ будуть використані найактивніше.

Перша – держава, що регулює напрямки та пріоритети, державні заявки, залучення інвестицій та фінансування проектів. Наприклад, залучення ШІ в публічних сервісах, формування політики відкритих даних, створення програм підтримки стартапів з ШІ та залучення їх до GOVTech-діяльності.

Друга – бізнес, який завдяки гнучкості, добротному управлінню і високій швидкості впровадження може розбудовувати машинне навчання, IoT, AR/VR, робототехніку.

Третя — державно-приватне партнерство, яке експерти вважають найбільш оптимальним різновидом формування нової індустрії. Тут мова йде

про розвиток ШІ, освоєння космічного простору, смарт-міста, нову енергетику і транспорт[2].

Також хотілося б виокремити такий напрям застосування штучного інтелекту як медицина – в умовах нинішньої ситуації в світі застосування алгоритмів в момент діагностики могло б значно прискорити процеси лікування.

Зокрема, важко не звернути увагу на таку подію, як фінансування \$1 млрд. Массачусетським технологічним університетом відкриття коледжу штучного інтелекту у 2018 році.

А вже в 2020 році вчені того ж таки університету виявили за допомогою спеціального алгоритму молекулу, яка має вражаючі властивості. «Наш підхід виявив цю дивовижну молекулу, яка, можливо, є одним з найбільш потужних антибіотиків, які були виявлені», — сказав Джеймс Коллінз, професор в Інституті медичної інженерії і науки Массачусетського технологічного інституту.

Дивно, та цей потужний антибіотик має зовсім незвичайну побудову, що значно відрізняється від інших. Якби пошуком з'єднання займалися тільки люди, дуже ймовірно, що цей антибіотик не був би виявлений взагалі, тому що він виглядає занадто незвичайним[3].

Згідно з усеукраїнським опитуванням, проведеним Інститутом Горшеніна спільно з групою компаній Everest у рамках дослідження «Штучний інтелект: український вимір», українці дуже позитивно налаштовані до перспектив розвитку технологій штучного інтелекту. Зокрема, 43,4% опитаних українців вважають, що, порівнюючи нові можливості та ризики, розробки в галузі ШІ потрібно продовжувати.

Серед ризиків виділяли: можливу концентрацію влади над людством у руках власника штучного інтелекту (36,0%), встановлення диктатури штучного інтелекту (21,6%), знищення людської цивілізації штучним інтелектом - (16,7%).

Українці виділили такий позитив від ШІ: звільнення людей від важких, небезпечних робіт (69,5% опитаних) і збільшення продуктивності у всіх галузях промисловості (50,4%), порятунок людства від стихійних лих і катастроф (18,1%) і запобігання злочинності і війнам (14,1% респондентів вважають так) [4].

Очевидно одне: швидкий розвиток штучного інтелекту створює не тільки додаткові можливості й загрози для його сторонніх споживачів, а й підштовхує пересічну людину ставати більш обізнаною та відповідальною.

Література:

1. Єфремов М. Штучний інтелект, історія та перспективи розвитку / М. Єфремов. URL: <http://vtn.ztu.edu.ua/article/view/81625/79214>.
2. Кравцова О. Вперед в будуще: почему правительство должно обратить внимание на искусственный интеллект URL: <https://www.epravda.com.ua/rus/columns/2019/09/4/651230/>
3. Удар по супербактериям. Штучний інтелект вперше створив новий антибіотик URL: <https://nv.ua/ukr/health/medicine/shtuchniy-intelekt-dopomig-znayti-noviy-antibiotik-50071954.html>
4. Соціологічне дослідження на тему "Штучний інтелект: український вимір" було проведено Інститутом Горшеніна на замовлення і в співпраці з групою компаній Everest у вересні 2018 року URL: <http://gorshenin.ua/wp-content/uploads/2018/12/Iskusstvennyj-intellekt.pdf>

БЕЗПЕКА WEB-ДОДАТКІВ

Божок Роман Юрійович

Державний університет телекомунікацій

Навчально-науковий інститут інформаційних технологій

Актуальність теми дослідження. Актуальність проблем безпеки WEB-додатків полягає в тому, що вони використовують конфіденційну інформацію, а також важливі трансфери компаній.

Постановка проблеми. Більшість атак на інформаційні системи спрямовані саме на вразливість веб-додатків за допомогою зовнішніх чинників.

Аналіз останніх досліджень і публікацій. В останні роки тема безпеки додатків дуже наповнилася галасом, є багато статей, обговорень та пошуку рішень. Для вирішення цих проблем було сформовано міжнародний проект із захисту WEB-додатків (OWASP) [1]. Проблеми та їх вирішення за допомогою OWASP описані більш докладно в статті [2]. Також у статті [3] описаний сертифікований метод, який допоможе розробникам мінімізувати появу дірок у програмі.

Виділення недосліджених частин загальної проблеми. There is no unified protection against all threats and security tools are developing more slowly than methods of application attacks.

Постановка завдання. Не існує єдиного захисту від усіх загроз, а засоби безпеки розвиваються повільніше, ніж методи атак на програми..

Викладення основного матеріалу. Веб-програма - це програма клієнт-сервер, де клієнт - це браузер, який відображає користувальницький інтерфейс, генерує запити до сервера та обробляє відповіді з нього. А серверна частина - це WEB-сервер, який обробляє запити клієнтів. Взаємодія між клієнтом і сервером, як правило, здійснюється за протоколом HTTP [4]. Архітектура веб-додатків має три рівні [5], які показані на рисунку 1.

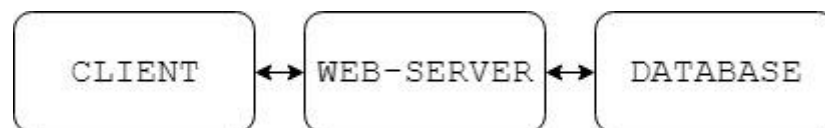


Рис. 1. Архітектура веб-додатків [6].

У зв'язку зі швидким зростанням популярності інформаційних технологій серед розробників з'явилися рекомендації щодо забезпечення безпеки веб-додатків, результатом чого став проект під назвою: Проект захисту відкритих веб-додатків (OWASP).

OWASP - це проект із захистом веб-додатків із відкритим кодом, який включає корпорації, освітні організації та окремих розробників, які разом формують статті, рекомендації та навчальні посібники, які є у вільному доступі та рекомендуються при розробці веб-додатків.

OWASP Top 10 Application Security Risks – 2017 [7]

- A1:2017-Injection
- A2:2017-Broken Authentication
- A3:2017-Sensitive Data Exposure

- A4:2017-XML External Entities (XXE)
- A5:2017-Broken Access Control

Експеримент. Ми вивчаємо сайт [8] "Кафедри обчислювальної техніки" Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" для забезпечення безпеки.

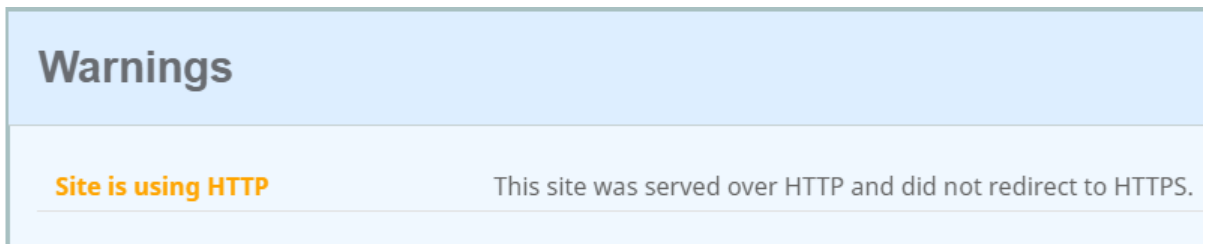


Рис.2 Тест з SecurityHeaders.io service [9]

Неправильна конфігурація безпеки є найбільш часто зустрічається проблемою. Зазвичай це результат небезпечних конфігурацій за замовчуванням, неповних або спеціальних конфігурацій, відкритого хмарного сховища, неправильно налаштованих заголовків HTTP та детальних повідомлень про помилки, що містять конфіденційну інформацію. Не тільки всі операційні системи, фреймворки, бібліотеки та програми повинні бути надійно налаштовані, але вони повинні бути вчасно виправлені / оновлені.

Redirection	✘	-20	Does not redirect to an HTTPS site
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)
X-Content-Type-Options	✘	-5	X-Content-Type-Options header not implemented

Рис.3 Тест з Observatory by Mozilla service [10]

Redirections. Сайти, які прослуховують порт 80, повинні перенаправляти лише на той самий ресурс на HTTPS. Як тільки відбудеться переспрямування, HSTS повинен переконатися, що всі майбутні спроби перейти на сайт через HTTP натомість надсилаються безпосередньо на захищений сайт.

Referrer Policy. Коли користувач переходить на сайт за гіперпосиланням або веб-сайт завантажує зовнішній ресурс, браузері інформують цільовий сайт про походження запитів за допомогою заголовка HTTP Referrer.

X-Content-Type-Options це заголовок, що підтримується Internet Explorer, Chrome та Firefox 50+, який повідомляє йому не завантажувати сценарії та таблиці стилів, якщо сервер не вказує правильний тип MIME. Без цього заголовка ці браузери можуть неправильно виявляти файли як сценарії та таблиці стилів, що призводить до атак XSS.

Висновок. У статті розглянуто список популярних загроз. На сайті відділення також перевірили безпеку. З досліджень видно, що сайт ненадійний і потребує вдосконалення. OWASP може допомогти знайти та виправити недоліки.

Література:

1. OWASP. The Open Web Application Security Project. [Electronic resource]. — Access mode: https://www.owasp.org/index.php/Main_Page

2. БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ. [Electronic resource] / Королев О.Л., Лукьянова М.А.// Международная научно-практическая конференция "Проблемы информационной безопасности". — 2016. — №6. — С.166-167. — Log Access Mode : <http://ieu.cfuv.ru/sites/default/files/2018-12/sbornik-trudov-2-megd-konf-problemy-inform-bezopasn-2016.pdf#page=166>

3. Разработка типовой методики анализа уязвимости в веб-приложениях при проведении сертификационных испытаний по требованиям безопасности информации. [Electronic resource] /Баранов А. В., Федичев А.В. // Вопросы кибербезопасности. — 2016. — №2(15). — С.2-8 — Log Access Mode: <https://cyberleninka.ru/article/v/razrabotka-tipovoy-metodiki-analiza-uyazvimostey-v-veb-prilozheniyah-pri-provedenii-sertifikatsionnyh-ispytaniy-po-trebovaniyam>

4. ОБЗОР УГРОЗ БЕЗОПАСНОСТИ WEB-ПРИЛОЖЕНИЙ. [Electronic resource] / Елисеев Н.А., Федоров С.А., Антонов О.Д. // Вопросы технических наук в свете современных исследований: сб. ст. по матер. V-VI междунар. науч.-практ. конф. — 2018. — № 1(4). — С. 18-23. Log Access Mode: <https://sibac.info/conf/technolog y/v/95451>

ДОСЛІДЖЕННЯ МЕТОДІВ ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ СИСТЕМ РАДІОЗВ'ЯЗКУ 4G

*Комащенко Борис Дмитрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій*

На сьогодні найбільш актуальною є технологія рознесення передачі, в якій об'єднуються переваги не тільки тимчасового кодування, але і просторового рознесення, в добавок підвищується простота обробки сигналу. У цій техніці використовуються особливі просторово-часові коди (STBC) для незалежної обробки декоррелірованих і перевідбитих сигналів. Сучасна радіотехніка використовує системи з декількома передавальними і приймальними антенами (технологія MIMO), вона входить в сучасні стандарти передачі даних, наприклад, WiMAX (IEEE 802.16e) або Wi-Fi (802.11n). Вивчаючи і аналізуючи наведені наукові дослідження, які присвячені багатопроменевим середовищам, вдалося виявити підходи до вирішення завдань сучасного радіозв'язку, що дозволяє вважати актуальним подальше дослідження техніки з рознесеними антенами.

Підвищення швидкості передачі інформації в системах LTE і WiMAX досягається в основному не тільки збільшенням розташування модуляції сигналів, а й за допомогою застосування OFDM (частотного ущільнення). Проте, збільшення швидкості передачі інформації часто обмежене запізненням променів в багатопроменевих каналах. У подібних системах для повного розкладання сигналів ортогональний порядок піднесує частот необхідно обробляти когерентно.

Вивчаючи сучасні наукові публікації можна зробити висновок, що актуальна тема технологій, які отримують користь з недоліків, таких як ефект багатопроменевого поширення. Одна з таких технологій передбачає застосування систем з декількома антенами. Ці системи базуються на механізмі просторово-часової обробки (STP) цифрових сигналів. В STP застосовується адаптивна обробка цифрових сигналів системою, яка складається з декількох антен, використовуючи особливості просторової і тимчасової областей

радіоканалу. Раніше технологія STP застосовувалася в основному в станціях або точках доступу, але не була застосована до мобільних пристроїв. Причиною цього була недостатня обчислювальна потужність, необхідна для реалізації STP-алгоритмів, а також їх малої ємності батарей. Сьогодні ж ці технології стали доступні так само і для них.

Техніка STP може застосовуватися на передавальному, приймальному або на обох кінцях каналу. Технологія STP застосовна на обох кінцях радіоканалу. Система, що використовує інтелектуальні антени в передавальному тракті, то вона називається MISO (Multiple Input Single Output), а якщо ж на приймальному - SIMO (Single Input Multiple Output).

У системах, які базуються на основі MISO і SIMO багаторазово поліпшується якість каналу, але не збільшується швидкість передачі даних. Для підвищення пропускної здатності каналу можна застосовувати технологію STP на обох кінцях радіоканалу (передавальному і приймальному). Такі системи прийнято називати MIMO (Multiple Input Multiple Output).

Щоб збільшити ємність каналу в системах MIMO використовується ефект розсіювання сигналу, що передається на різних фізичних об'єктах (гори, будівлі, дерева). Чим більша кількість передавальних (N_t) і відповідно їм прийомних (N_r) антен, тим теоретично велика ($N_t \times N_r$) пропускна здатність каналу. Причиною цього є розбиття потоку даних передавача на незалежні послідовності бітів, які пересилаються на приймач одночасно, використовуючи масив антен. Таку техніку прийнято називати просторовим мультиплексуванням.

Список використаних джерел:

1. Бараш Л.Є. - Технологія MIMO - нова ставка у бездротових мережах [Електронний ресурс] – Режим доступу до ресурсу: https://itc.ua/articles/tehnologiya_mimo_novaya_stavka_v_besprovodnyh_setyah_15263.
2. Корж В.А. - WiMAX 802.1e : Підходи до якісного поліпшення робочих характеристик систем мобільного широкосмугового доступу стандарту 802.1e [Електронний ресурс] – Режим доступу до ресурсу: <http://www.mforum.ru/news/article/058869.htm>.

РОЗГЛЯД ТЕХНОЛОГІЇ POWER LINE

Пригода А.О.

*Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій*

PLC (англ. Power Line Communication) — відносно нова телекомунікаційна технологія категорії «остання миля». Так званий «Інтернет з розетки», що базується на використанні внутрішньо-будинкових і внутрішньо-квартирних електромереж для високошвидкісного інформаційного обміну.

У цій технології, заснованої на частотному поділі сигналу, високошвидкісний потік даних розбивається на декілька низько-швидкісних, кожен з яких передається на окремій частоті з подальшим їх об'єднанням в один сигнал.

При цьому PLC-пристрої можуть «бачити» і декодувати інформацію, хоча звичайні електричні пристрої — лампи розжарювання, двигуни і т. п. — навіть

«не здогадуються» про присутність сигналів мережевого трафіку і працюють у звичайному режимі.

У наш час технологія широко використовується як в Україні, так і в Європі та Америці.

Основою технології PowerLine є використання частотного поділу сигналу, при якому високошвидкісний потік даних розбивається на декілька відносно низько-швидкісних потоків, кожен з яких передається на окремій частоті з подальшим їх об'єднанням в один сигнал. Реально в технології PowerLine використовуються 84 частоти в діапазоні 4-21 МГц.

PLC включає:

BPL (англ. Broadband over Power Lines) — широкопasmову передачу через лінії електропередачі, яка забезпечує передачу даних зі швидкістю більше 1 Мбіт/с, і

NPL (англ. Narrowband over Power Lines) — вузькопasmову передачу через лінії електропередачі з набагато меншими швидкостями передачі даних.

При передачі сигналів по побутовій електромережі можуть виникати великі загасання в передавальній функції на певних частотах, що може призвести до втрати даних. У технології PowerLine передбачений спеціальний метод розв'язання цієї проблеми — динамічне включення та вимкнення передачі сигналу (англ. dynamically turning off and on data-carrying signals). Суть даного методу полягає в тому, що пристрій здійснює постійний моніторинг каналу передачі з метою виявлення ділянки спектру з перевищенням певного порогового значення загасання. У разі виявлення даного факту, використання цих частот на час припиняється до відновлення нормального значення загасання.

Існує також проблема виникнення імпульсних перешкод (до 1 мікросекунди), джерелами яких можуть бути галогенні лампи, а також включення і виключення потужних побутових електроприладів, обладнаних електричними двигунами.

PDSL — технологія сімейства xDSL, що забезпечує симетричну передачу даних зі швидкістю до 2Мбіт/с силовими кабелями (4-20 кВ) одночасно з постачанням електроенергії. Пристрої для підключення обладнання PDSL до високовольтних ліній встановлюють у трансформаторних шафах.

Переваги

- Не потрібно прокладати кабель, укладати його в короби, свердлити стіни й опорні конструкції

- Простота використання

- Швидкість монтування

У порівнянні з Wi-Fi

- Не потребує встановлювання

- Стабільніший зв'язок

- Більша безпека інформації

- Підходить для передавання Multicast-трафіку, наприклад, IPTV

- На якість зв'язку не впливає матеріал і товщина стін у квартирі

Недоліки

– Порушення прийому радіосигналу в приміщеннях, де працюють PLC-модеми, особливо на середніх та коротких хвилях, але на дуже невеликій відстані близько 3—5 метрів від модему.

– Пропускна здатність мережі по електропроводці ділиться між усіма його учасниками. Наприклад, якщо в одній Powerline-мережі дві пари адаптерів активно обмінюються інформацією, то швидкість обміну для кожної пари буде складати приблизно по 50% від загальної пропускної здатності.

– На стабільність і швидкість роботи PLC впливає якість виконання електропроводки, наявність стиків з різних матеріалів (наприклад, мідного і алюмінієвого провідника), а також просто кількість з'єднань провідника.

– Не працює через мережеві фільтри і джерела безперебійного живлення, якщо вони не обладнані спеціальними розетками «PLC READY».

– На якість зв'язку можуть негативно впливати дешеві енергозберігаючі лампи, тиристорні диммери, імпульсні блоки живлення та зарядні пристрої, особливо в разі їх підключення безпосередньо біля PLC-модему.

Список літератури:

1. Що таке powerline-adapter і для чого він потрібен <https://www.moyo.ua/news/chto-takoe-powerline-adapter-i-zachem-on-nuzhen-5-ischerpyvayushchikh-otvetov.html>
2. Powerline-adapter. // <https://uk.go-travels.com/57014-what-is-a-powerline-adapter-1846813-6061639>

ВПРОВАДЖЕННЯ КОНЦЕПЦІЇ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ТРАНСПОРТНОЇ ГАЛУЗІ

*Андрійко Володимир Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій*

Використання мережевих технологій управління, а також розподілених систем управління є актуальним підходом, що дозволяє реалізувати нову цифрову модель вантажоперевезень. Прикладом об'єднання технологій і систем подібного класу є концепція Інтернету речей. Поширення цієї концепції стало початком масштабного технологічного прориву, який став можливий завдяки повсюдному впровадженню інтернет технологій [1, с.18]. Технологічні рішення побудовані на основі технологій Інтернету речей, часто об'єднуються в інтелектуальні мережі в результаті чого виходить цілий «Smart» або розумні галузеві рішення. Найбільш розвиненими в цій області є такі напрями «Розумне місто», «Індустрія 4.0», «Smart транспорт і логістика», «Розумний будинок», «Розумна мобільність», «Розумні контракти», «Розумні машини» і кількість галузей в яких будуть розвиватися і все більше впроваджуватися «Розумні» технології буде тільки зростати і розвиватися. Всі ці розумні рішення будуть підключати в інтелектуальні мережі все більше нових сегментів виробничих і технологічних ринків.

В основі Інтернету речей або «Internet of things (IoT)» лежить міжмережева цифрова взаємодія фізичних пристроїв, інтелектуальних

автономних пристроїв (в тому числі транспортних засобів і транспортної інфраструктури), інтелектуальних датчиків і камер, керуючих пристроїв, інтегрованих в єдину мережу і взаємодіючих між собою за допомогою обміну даними і передачі інформації по захищених каналах зв'язку [2, с.106].

На основі концепції Інтернету речей будуються кібер-фізичні системи, завдяки яким можливий контроль і дистанційне керування об'єктами реального світу через їх віртуальний, цифровий прототип. У разі реалізації транспортної системи на основі технологій цифрового двійника «Digital Twin» транспортні об'єкти можуть віддалено контролюватися і навіть управлятися через комп'ютерні мережі, завдяки наявності прямого інтернет зв'язку між транспортним об'єктом у реальному світі і його комп'ютерної реалізацією. При реалізації цифрового управління в транспортних і транспортно-логістичних системах скорочується роль людського фактора в управлінні, завдяки чому збільшується точність і ефективність транспортно-логістичних та економічна вигода транспортно-експедиційних операцій і функцій [3, с.27].

Кібер-фізичні транспортні системи або віртуальні транспортні системи реалізуються за рахунок впровадження додаткових сенсорів і сервоприводів, об'єднуючи в мережу розумні пристрої та організовуючи інтелектуальний транспорт і інтелектуальні транспортні системи міст.

Список використаних джерел

1. Капитанов В.Т., Хилажев Е.Б. Управление транспортными потоками в городах [Текст] / В.Т. Капитанов, Е.Б. Хилажев //– М.: Транспорт, 2008. – 94 с
2. Никифоров О.Ю. Базовые технологии интернета вещей // Символ науки. – 2015. – № 9-1. – С. 105-107.
3. Розенберг И.Н. Интеллектуальное управление транспортными системами [Текст] / И.Н. Розенберг // Государственный Советник. – 2016. – № 3 – С. 26–32.

АНАЛІЗ СЕРВЕРНИХ ОПЕРАЦІЙНИХ СИСТЕМ ДЛЯ ДОМАШНЬОГО ВИКОРИСТАННЯ

Цвик Олександр Сергійович

Державний університет телекомунікацій

Навчально-науковий інститут інформаційних технологій

Сервер – це комп'ютер, але спеціалізований для вирішення завдань компанії або інших користувачів мережі. Завдяки серверу, ІТ-фахівці можуть налаштувати роботу всередині компанії, між містами та країнами. Також сервер використовують звичайні користувачі чи ІТ-спеціалісти в домашніх умовах для саморозвитку чи покращення праці на дому.

На ринку серверних ОС з кожним роком з'являється різні кастомні систем, що можливо використовувати безкоштовно, але вони являються небезпечними, якщо користувач не вивчав внутрішню систему ОС. На сьогоднішній день є декілька перевірених роками систем, що можуть надати все, що потрібно для домашнього використання. Це системи: Ubuntu server, CentOS, RedHat, FreeBSD, Windows Server.

Ubuntu server, CentOS, RedHat є Unix-системами, що можуть бути використовуватися в компанії на серверах й в домашніх системах.

FreeBSD являється старою системою, які вже понад 20 років, яку ще можливо встановити та використовувати. Система FreeBSD не підходить для користувачів мало-знайомих с старими системами, тому що цю систему вже не підтримують на достатньому рівні.

Windows Server являє собою комерційну систему з великою частиною платними програмами, що заважає стабільній праці системи. Для використання в домашніх умовах підходить, але має багато недоліків.

Linux та його системи

Ubuntu server - безкоштовна серверна ОС на ядрі від UNIX. Ubuntu перевершує інші дистрибутиви Linux для серверів - починаючи від простої інсталяції, до відновлення після проблем з обладнанням або класної підтримки. Стабільність системи відповідає дійсності, часто використовується на високо навантажених серверах. Легкість використання допомагає швидко та зручно розгорнути систему та завдяки допоміжним програмам (Docker, Hypervisor)

CentOS – серверна ОС що направлена на управління гіпервізором. Цей клон RHEL не є строго комерційним продуктом, але ви можете користуватися платною підтримкою.

RedHat - це надійний дистрибутив, заснований на Fedora з додатковим фокусом на стабільності і підтримки. Дебют ОС відбувся в 2014 року, з того часу було декілько апдейтів, після яких ОС отримала можливості масштабування, включаючи нову файлову систему, яка може підтримувати до 500 терабайт, а також підтримку контейнерів Docker. Також система підходить для домашнього використання, але її можливості більш направленні на комерційний підприємств.

Функції гіпервізора та допоміжні механізми.

Для домашнього використання системи є можливість не встановлювати допоміжні програми , але для стабільності чи більш продуктивної роботи вони можуть знадобитись

Гіпервізор - програма або апаратна схема, що забезпечує або дозволяє одночасне, паралельне виконання декількох операційних систем на одному і тому ж хост-комп'ютері.

Docker - програмне забезпечення для автоматизації розгортання і управління додатками в середовищах з підтримкою контейнеризації, контейнерізатор додатків. Дозволяє розгорнути програми, без зайвих зусиль, та «упакувати» свої системи для переносу їх на іншу станцію.

Отже, для домашнього використання з усіх представлених операційних систем підходить Ubuntu Server, який надає можливості в безкоштовному та легкому встановленні системи на комп'ютер й допоміжних програм. Також Ubuntu Server має велику бібліотеку для перших кроків в системі та вивчення, як його використовувати на повну силу.

Список використаних джерел

1. Что такое операционная система Linux URL: <https://te-st.ru/2017/11/01/linux-advantages-and-disadvantages/>

2. Компьютерная документация Базы данных URL: <http://www.compdoc.ru/bd/sql/understanding/>

ПРОБЛЕМИ НА ШЛЯХУ ПІДВИЩЕННЯ ТЕХНОЛОГІЧНОЇ ЦІННОСТІ УКРАЇНИ

*Тарчанський Артур Ігоревич
Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій*

Сьогоднішній світ кидає багато різноманітних викликів для країн. До середини ХХ століття багатими і успішними економіками могли бути ті, які мали у своєму розпорядженні велику кількість природних ресурсів. Зараз же країни, які розвиваються як сировинні придатки можуть відноситися до третього світу з дуже низьким ВВП на душу населення. У той же час, країни, які не мають природних ресурсів, знаходяться на лідируючих позиціях у рейтингах ВВП на душу населення. Одну з визначальних ролей у такому положенні відіграє рівень розвитку інформаційних технологій.

Україна має велику територію, багато різноманітних природних ресурсів. Варто відзначити, що кількість чорноземів на території країни є одною з найбільших серед держав світу. При цьому номінальний ВВП на душу населення за даними МВФ за 2018 рік складає лише 2963 дол. США, що поміщає Україну на 131 місце у рейтингу країн світу. При цьому середнє значення по світу 11565 дол. США. Серед лідерів рейтингу знаходяться країни, які дають світу не сировину, а різноманітні продукти: матеріальні блага, послуги, інтелектуальні продукти і т. п. Для досягнення таких результатів можна виділити декілька базових чинників.

1. Низький рівень корупції.
2. Високий рівень розвитку освіти та науки.
3. Свобода ведення підприємницької діяльності.
4. Захист інвестицій у різні сфери бізнесу: реальний та інформаційний.

Коли країна працює у вказаних напрямках, то бізнес інвестує кошти у різноманітні проекти, з'являється велика кількість спеціалістів, які мають робочі місця і не планують еміграцію. Населення такої держави живе у такому положенні, що їх базові потреби вирішені і більша кількість людей намагається реалізувати свій підприємницький таланти. Тим самим збільшуючи ВВП країни. Зараз велика кількість нових продуктів реалізується саме у технологічній сфері: біотехнології, сервіси, штучний інтелект. Такі продукти часто оптимізуються витрати підприємств і держави в цілому, що також веде до збільшення конкурентоспроможності економіки.

Наразі в Україні є велика кількість перешкод, які гальмують її розвиток як технологічної держави. Хоч на території існує певна кількість компаній, які розробляють саме інформаційні сервіси, але часто це просто офіс з консультантами, які працюють з іноземною компанією через ФОП. Така структура веде до того, що в економіку України заходить лише 5% від оплати праці консультантів, а податки з прибутку компанії платяться в ту країну, де вона зареєстрована. Це великі втрати бюджету країни. Крім того втрати самих технологій. Деякі компанії виходять на ринок України тільки після декількох

років роботи на експорт, тому що не вважають локальний ринок цінним. Через це технологізацію підприємств України сильно відстає від розвинених країн.

Можна виділити деякі основні проблеми в устрою економіки країни, які заважають розвиватися технологіям.

1. Незахищеність інвестицій: судова система, законодавча. Інвестори бояться вкладати кошти через те, що у випадку проблем захистити їх буде складно або навіть неможливо.

2. Відсталість законодавства в сфері інформаційних технологій. Багато чого не врегульовано, що уже давно працює в розвинених країнах.

3. Корумпованість посадовців усіх рівнів. Часто з'являються стартапи, які намагаються вирішити якусь проблему у соціальній чи державній сфері, але запустити продукт у користування часто може бути неможливо без зв'язків.

4. Якість освіти. Наразі багато університетів готуються спеціалістів за застарілими програмами. Проводяться реформи, які понижують рівень освіти у школах.

Отже основною перешкодою на шляху технологічного прогресу України є недостатній рівень зусиль з боку державного апарату. Вільна конкуренція веде до того, що ефективні компанії розвиваються, а неефективні банкрутують або стають ефективними. Глобалізація дозволяє компаніям мінімізувати свої ризики і витрати змінюючи країну реєстрації. Отже просто змусити компанію працювати на території країни вже не можна. Потрібно створювати умови, коли компаніям буде вигідно працювати у юрисдикції України, тоді інформаційні технології почнуть розвиватися в усіх сферах діяльності.

СИСТЕМА ГЕОПОЗИЦІОНУВАННЯ НА ОСНОВІ RFID-МІТОК

Висоцький А.Ю

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

Для визначення місця розташування рухомих об'єктів широке застосування знайшли системи глобального позиціонування GPS і ГЛОНАСС, які забезпечують точність позиціонування до 5-10 метрів практично в будь-якій точці земної кулі. Однак така висока точність цих систем досягається тільки в умовах відкритої місцевості. Всередині будівель точність визначення місця розташування значно погіршується, або взагалі неможлива, що пов'язано, в першу чергу, з ослабленням сигналів всередині приміщень.

На сьогоднішній день найбільш доступною і масовою технологією для геолокації всередині приміщень є технологія, реалізована на базі вже існуючих мереж Wi-Fi. Рішення для мереж Wi-Fi на ринку, пропонуються багатьма зарубіжними компаніями, такими як Cisco, D-Link, Mikrotik, Huawei, ZyXEL та ін. Але ці компанії надають опцію геолокації як додаткову і дуже дорогую опцію.

Сучасні технології локального позиціонування можна згрупувати наступним чином [1, 2]:

- системи супутникової навігації;
- радіочастотні системи;
- інфрачервоні й ультразвукові системи.

Радіочастотні системи - це найбільш об'ємна група технологій, багато з яких використовуються для традиційних послуг зв'язку, і можуть застосовуватися для визначення місця розташування об'єктів. До них відносяться: стільниковий зв'язок, Wi-Fi; Bluetooth; RFID; UWB; NFER та ін. З точки зору простоти реалізації і точності результатів, найцікавішими з-поміж усіх виділяються системи, засновані на технологіях IEEE 802.11 (Wi-Fi) і RFID, а також їх комбінації.

Системи локального позиціонування в Wi-Fi мережах можуть використовувати методи визначення місця розташування мобільного об'єкта по найближчій точці доступу, а також триангуляцію або трилатерацію і визначення відстаней з допомогою вимірювання фізичних параметрів AOA, TOA або рівня сигналу RSS. Точність цих систем зазвичай становить від 3 до 15 м. Підвищити точність дозволяє застосування більшої кількості точок доступу [3, 4].

Системи з радіочастотними ідентифікаторами RFID (англ. Radio Frequency Identifier) є основою інтелектуального управління даними на цифровому підприємстві для забезпечення прозорості промислових процесів. Радіус дії систем позиціонування на основі RFID становить близько 100 м, а точність таких систем може досягати значень 5-50 см.

RFID-система складається з зчитувача і транспондера, званого також RFID-міткою. Мітки можуть бути трьох видів: пасивні, напівпасивні і активні. Більшість вироблених на сьогоднішній день RFID-міток є пасивними і складаються з мікросхеми та антени і отримують електроживлення від зчитувача. В основному, пасивні мітки застосовуються в системах розпізнавання товарів і вантажів, розпізнавання людей, контролю і управління доступом.

Для систем відстеження об'єктів на порівняно великій площі використовуються активні RFID-мітки, які на відміну від пасивних володіють власним акумулятором і генерують сигнал незалежно від зчитувача [1, 5]. Для цілей позиціонування, як правило, застосовують активні RFID-метки, що працюють в режимі маяка, які посилають сигнал із заданою періодичністю декільком приймачів (не менше трьох), розташованим по периметру контрольованого приміщення. Відстань від маяка до приймачів може бути визначено виміром параметрів AOA, TOF або TOA. Активні RFID працюють в діапазонах частот 455 МГц, 2,4 ГГц або 5,8 ГГц. Застосування частоти 2,4 ГГц дає можливість комбінувати технологію RFID з мережею Wi-Fi. Архітектура

системи визначення місця розташування мобільного об'єкта з використанням RFID-міток представлена на рис. 1.

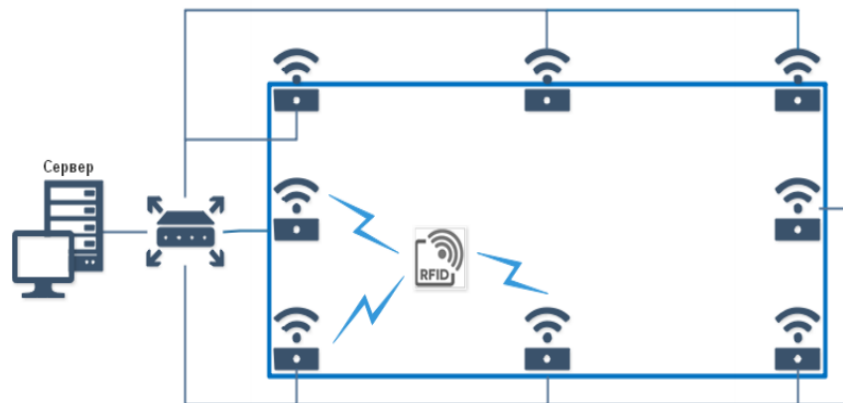


Рисунок 1 – Архітектура RFID-міток

Таким чином, вивчивши переваги і недоліки різних технологій, застосовуваних для цілей позиціонування, можна зробити висновок, що найбільш придатними є системи, що поєднують простоту реалізації і велике поширення мереж Wi-Fi з точністю, порівняно низькою вартістю і великим радіусом дії активних RFID-міток.

Література

1. Wi-Fi Location-Based Services 4.1 Design Guide. San Jose, CA. Americas Headquarters Cisco Systems, Inc. 2008. – 206 p.
2. Bensky A., Wireless Positioning Technologies and Applications. 2nd Ed. Boston. London Artech House. 2016. – 450 p.
3. Вахрушева А.А. Технологии позиционирования в режиме реального времени // Вестник СГУГиТ. Том 22. – № 1, 2017. – С. 170-177.
4. Кокорева Е.В., Костюкович А.Е., Дошинський І.В. Оцінка похибки вимірювань місцезнаходження абонента в мережі Wi-Fi // Програмні системи і обчислювальні методи, 2019. – № 4. С. 30-38.
5. Kokoreva E., Kostyukovich A., Doshchinsky I. Analysis of the error in determining the location inside the logistics warehouse complexes // Advances in Intelligent Systems and Computing. Springer Verlag, TransSiberia, 2019. Vol. II.106. – pp. 1086-1094.

КОНЦЕПЦІЯ «ІНТЕРНЕТУ РЕЧЕЙ (IOT)» ТА ЗВ'ЯЗОК ІЗ МЕРЕЖАМИ 5G

Маковійчук Іван Ігорович

Державний університет телекомунікацій

Навчально-науковий інститут інформаційних технологій

Інтернет речей (англ. *Internet of Things, IoT*) — концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами в автоматичному

режимі, за допомогою використання стандартних протоколів зв'язку. Окрім давачів, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові чи бездротові мережі. Ці взаємопов'язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів.

Основною концепцією є можливість підключення всіляких об'єктів (речей), які людина може використовувати в повсякденному житті, наприклад, холодильник, кондиціонер, автомобіль, велосипед і навіть кросівки. Всі ці об'єкти (речі) повинні бути оснащені вбудованими давачами або сенсорами, які мають можливість обробляти інформацію, що надходить з навколишнього середовища, обмінюватися нею і виконувати різні дії в залежності від отриманої інформації. Прикладом впровадження такої концепції є система «розумний будинок» або «розумна ферма». Ця система аналізує дані навколишнього середовища і в залежності від показників регулює температуру в приміщенні. У зимовий період регулюються інтенсивність опалення, а в разі спекотної погоди будинок має механізми відкривання і закривання вікон, завдяки чому провітрюється будинок, і все це відбувається без втручання людини.

Що означає 5G для IoT?

5G забезпечує швидший, стабільніший та безпечніший зв'язок, який просуває все, починаючи від автономних автомобілів, закінчуючи розумними мережами для відновлюваної енергії і закінчуючи роботами з підтримкою ШІ на заводських поверхах.

Це розкриває величезну екосистему IoT, де мережі можуть обслуговувати мільярди підключених пристроїв, з правильними компромісами між швидкістю, затримкою та вартістю. Пропускна здатність даних у новій мережі повинна досягати до 20 гігабіт в секунду і дозволяти коротший час відгуку.

За допомогою 5G також можна буде передавати дані в режимі реального часу. Це означає, що 100 мільярдів мобільних пристроїв у всьому світі будуть доступні одночасно.

Іншими словами, щільність з'єднання становить приблизно один мільйон пристроїв на квадратний кілометр. У той же час нова технологія сприяє збільшенню відносної швидкості руху. Це означає, що якість з'єднання буде набагато стабільнішою до швидкості 500 кілометрів на годину, що принесе величезні переваги, особливо для залізничних пасажирів.

Незалежно від смартфонів, збільшення обсягу даних неминуче в інших сферах застосування. Цифри звучать не просто величезно, вони величезні. З цих і багатьох інших причин 5G IoT стане новою ключовою технологією підключення.

Література:

5. 5G – IOT // <https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/resources/innovation-technology/5G-iot>
6. Інтернет речей // <https://www.qualcomm.com/research/5g/internet-of-things>

ІНТЕГРОВАНІ РІШЕННЯ НА ОСНОВІ HYPERFLEX

Тищенко Сергій Вікторович

Державний університет телекомунікацій

Навчально-науковий інститут інформаційних технологій

Система Cisco HyperFlex надає готове гіперконвергентне рішення, що об'єднує програмно-конфігуровану мережу і обчислення з платформою даних Cisco NX нового покоління. В основі цієї системи - платформа Cisco UCS. Cisco HyperFlex робить робочі процеси ефективніше і підвищує адаптивність ЦОД, розкриваючи потенціал гіперконвергентної інфраструктури (рис. 3.1) [1].

Гіперконвергентні системи (HyperConvergedSystems - HCI) на сьогоднішній день займають міцні позиції на ринку інфраструктурних рішень і показують стабільну тенденцію до зростання, незважаючи на свою молодість [2]. Довіра до них зростає, паралельно зростає попит на HCI-рішення, а пропозиції не змушують себе довго чекати, вступаючи від все нових гравців в цій сфері IT-рішень. Але що ж зробило їх такими популярними в порівнянні з «класичною» моделлю, що розділяє рівні обчислювальних потужностей, системи зберігання та питання комутації? Все досить просто.

Інтеграція і супровід подібних систем вимагає набагато менших накладних витрат, знижує ризик експлуатаційних помилок, а також з'являється незрівнянна гнучкість в масштабуванні даних систем, роблячи їх привабливими для розгортання будь-якого масштабу.

Незважаючи на явні переваги, HCI на сьогоднішній день поки що не здатні витіснити класичні рішення, тому легко інтегруються з ними, дозволяючи зробити перехід більш плавним, уникаючи великих витрат на етапі впровадження і не закопуючи вже вкладені інвестиції в поточну інфраструктуру. Модель HCI, з одного боку, сильно спрощена архітектурно, що дає можливість оперативніше реагувати на вимоги бізнесу. З іншого боку, дані системи часто виграють в продуктивності у інших рішень і краще масштабуються, що підвищує конкурентоспроможність бізнесу без надмірних капіталовкладень.

Можна заперечити, що всі ці питання легко закриваються і на системах, побудованих за принципами трирівневої моделі інфраструктури (сервер, SDN, мережа). Все це так, але, вважаючи витрати на експлуатацію, коли часто в розділених схемах існує необхідність оплачувати фахівців на кожному з рівнів цієї системи, можна прийти до висновку, що класична схема має вкрай багато нюансів, які роблять її менш гнучкою і більш вимогливою до експертизи, інтеграційним і експлуатаційним витрат, не кажучи вже про тимчасові.

Яскравим представником HCI від компанії Cisco, просунувшись її вгору по квадрату Гартнера на ринку гіперконвергентних систем поряд з Nutanix, VMWare, Dell EMC і HPE, стало представлене в 2016 році рішення HyperFlex.

Рішення розроблено на базі платформи Cisco Unified Computing System (Cisco UCS), поєднуючи в собі з боку обчислювальної частини як стійку NOD NX2xx, так і бездискове реалізацію блейд-систем (рис. 3.2) [1, 3].

Система зберігання отримала назву HX Data Platform і створена за принципом SDS (Software Defined Storage). Вона дозволяє зібрати в єдиний пул зберігання всі носії інформації в межах кластера. Природно, підтримується All-Flash і в найближчому майбутньому - NVMe-реалізацію. Як мережі використовується обов'язковий компонент обчислювальної фабрики Cisco UCS - Fabric Interconnect з колосальною швидкістю роботи і мінімальними показниками затримок, що є вкрай важливими параметрами в гіперконвергентних рішеннях.

Первісне конфігурування і подальша настройка серверів (firmware, raid, bios та інші) здійснюється з допомогою так званих сервісних профілів, коли, маючи в розпорядженні переднастроєні шаблони, нам стає байдуже - один сервер додається в кластер або 100.

Для управління платформою зберігання даних (HX Data Platform) також доступні плагіни для консолей управління MSSC і VMWare.

В результаті ми отримали готове до роботи з коробки, кероване з єдиного місця, надійне, потужне і гнучке рішення, масштабування якого зводиться до простого додавання необхідних блоків. Це можуть бути бездисківі блоки обчислення або, навпаки, блоки, що розширюють можливості системи зберігання даних, суміщені з обчислювальною частиною. HyperFlex, крім гіпервизора від компанії VMWare, підтримує Hyper-V і контейнерну віртуалізацію.

Література:

1. Анатомия гиперконвергентных систем на примере Cisco Hyperflex [Електронний ресурс]. — Режим доступу: <https://www.computerra.ru/235735/anatomiya-giperkonvergentnyh-sistemy-na-primere-cisco-hyperflex/> (дата звернення: 15.05.20)

2. Anders Nygren. OpenFlow Switch Specification / Anders Nygren, Ben Pfaff, Bob Lantz [Електронний ресурс]. — Режим доступу: <https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-switch-v1.5.1.pdf> (дата звернення: 23.04.20)

3. The SDN Solutions Showcase [Електронний ресурс]. — Режим доступу: https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/ONF_SDN%20Solutions%20Showcase%20WhitePaper_2015.pdf (дата звернення: 15.05.20)

ENTITY-RELATIONSHIP MODEL: VERSATILE SYSTEM DESIGN APPROACH

*Іванченко Микита Олександрович
Державний Університет Телекомунікацій
Навчально-науковий інститут інформаційних технологій*

Entity-relationship model is a way to express a high-level design of units and their associations in a given system. It's commonly used at one of the early stages of system design and is mostly applied to the design of database systems, although it might be freely used to model arbitrary systems as well. It comes in three flavors, which operate on three different abstraction levels: conceptual, logical and physical,

but the principles will hardly differ between the three. The notion of entity-relationship model was formalized and further developed (variants of the idea were already present) by Peter Chen in his 1976 seminal paper “The Entity-Relationship Model – Toward a Unified View of Data”.

Entity-relationship model is expressed graphically in what is, unsurprisingly, called “entity-relationship diagram”, such diagram uses three primary element types:

1. Entity set
2. Relationship
3. Attribute (present in Chen’s version, but absent in some of the later variations)

The definition of an entity set might be deduced as a collection of similar entities, but what is an entity? In this context we might say that entity is an abstract object that can exist independently and can be uniquely identified in a given ontology (our “subject area”). In plain terms, it’s an autonomous unique thing that represents something; usually it’s something from the real world that we often try to model.

Relationship is a connection between two or more entity sets. These connections can represent associations, dependencies or any other type of relation. Most commonly used type of relation is binary, between only two entity sets.

Attribute is an additional way to characterize an entity, along with its relations. Attributes may be used to express arbitrary information about the entity in a set and is also the place where entity’s unique identifier, which will provide it’s required “uniqueness” property.

In original Chen’s version those entity types are distinguished by their graphical representation on a diagram, as seen in Figure 1:

1. Entity set is drawn as a rectangle
2. Relationship – as a diamond
3. Attribute – as an oval

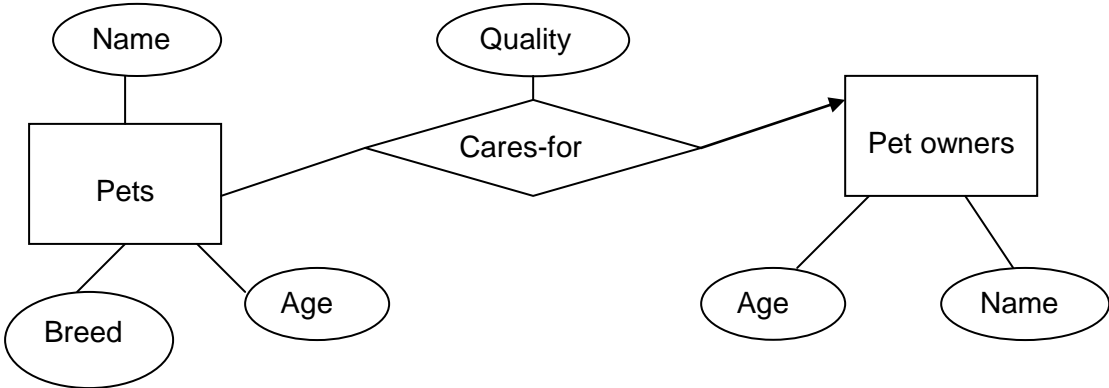


Figure 1: Entity-relationship diagram between pets and pet owners

Arrow at the end of “cares-for” relationship near “Pet owners” entity set indicates that each entity in “Pets” entity set is cared for by at most one pet owner and its absence on the end of “cares-for” near “Pets” indicates that one pet owner may

have many pets. Notice that relationships can have attributes in a similar fashion to entities.

This relationship constraint is captured in the notion of “uniqueness constraints” for binary associations. There are three types of such constraints: one-to-many, one-to-one and many-to-many. Figure 1 illustrates one-to-many relationship between pet owners and pets (you can also say that’s many-to-one between pets and pet owners).

As was mentioned earlier, entity-relationship model and diagram are frequently seen on the whiteboards during database schema design sessions and there’s good reason for that – once you have entity-relationship diagram in place, it’s trivial to move from there to a proper database schema, you could map it almost directly. One of the reasons for its wide adoption, along with conciseness, is also its flexibility – you can do many design iterations fast.

If we were tasked to draft a schema of any given system, old or new, we could follow a simple four-stage process to accomplish that in an optimal amount of time:

1. Start with a rough idea of the system constituents and their connections
2. Draft high-level design expressed in the form of entity-relationship diagram
3. Check if your design is sound, faithful to the specification and meets the requirements
4. If it does – map it to the target presentation (e.g. relational database schema), else (easily) adjust the diagram and check again

I hope that this quick overview has shown entity-relationship model for what it is: an extremely expressive and powerful system design approach, which not only facilitates fast design iteration cycles, but also provides tooling which allows vivid presentation of logical units and their associations in systems of practically any domain and complexity. Despite the presence of alternative visual expression approaches in the form of Unified Modeling Language and Object Description Language, entity-relationship model remains a personal favorite for a great number of system architects and, apparently, will hold its positions for an observable future.

Reference:

1. Chen P. The Entity-Relationship Model - Toward a Unified View of Data. – Cambridge: MIT Press. – 1976. – с. 9-36
2. Garcia-Molina H., Ullman J., Widom J. Database Systems: The Complete Book - Toward a Unified View of Data. – New York: Pearson. – 2014. – с. 122-166

СПЕЦИФІКАЦІЯ ВИМОГ ДО ПРОГРАМНОГО КОМПОНЕНТУ АНАЛІЗУ УРАЗЛИВОСТЕЙ ВЕБ ЗАСТОСУНКІВ

М.І. Гітько

Державний університет телекомунікацій

Навчально-науковий інститут інформаційних технологій

Важливим інформаційним активом будь-якої організації є веб застосунки. Вимоги до забезпечення їх (зокрема, сторінок) безпеки від несанкціонованого

доступу викладено в [1]. Тоді як настанови зі запобігання реалізуванню загроз через уразливості програмних застосунків описано в [2]. За основу такого підходу стосовно веб застосунків взято OWASP [3, 4]. Тому специфікування вимог до програмного компоненту аналізування уразливостей веб застосунків є актуальним.

Для специфікування вимог до програмного компоненту застосовано графічну нотацію UML. Це дозволило відобразити специфікацію діаграмою варіантів використання. Серед них основним є аналізування уразливостей веб застосунків. Він розширяється такими варіантами використання [3, 4]: визначення основних метрик, визначення часових метрик, визначення контекстних метрик. Значення даних метрик аналізуються за шкалою [4]: відсутнє – 0,0; низьке – від 0,1 до 3,9; середнє – від 4,0 до 6,9; високе – від 7,0 до 8,9; критичне – від 9,0 до 10,0. Результати аналізування уразливостей веб застосунків представляються послідовністю метрик. Ця послідовність починається міткою «CVSS». Наступний складник – поточна версія системи оцінювання уразливостей, наприклад [4], «3.1». Далі через роздільник «/» вказується набір метрик. Тому відповідно до синтаксису вимог [Тема] [Дія] [Значення] отримуємо [5]:

[Програмний компонент] [Аналізування уразливостей] [Метрика]

Отже, специфікацію вимог до програмного компоненту відображено діаграмою варіантів використання у графічній нотації UML. Для цього враховано їх представлення за синтаксисом вимог.

Література:

1. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу : наказ ДСТСЗІ СБ України від 02.04.2003 № 33 (зі змінами). URL: <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106344> (дата звернення: 29.04.2020).
2. ДСТУ ISO/IEC 27034-1:2017 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 1. Огляд і загальні поняття (ISO/IEC 27034-1:2011; Cor 1:2014, IDT). [Чинний від 2019-11-01]. Вид. офіц. Київ : ТК «Інформаційні технології», 2019. 79 с.
3. OWASP Web Security Testing Guide. URL: <https://owasp.org/www-project-web-security-testing-guide/> (дата звернення: 29.04.2020).
4. Common Vulnerability Scoring System SIG. URL: <https://www.first.org/cvss/> (дата звернення: 29.04.2020).
5. ISO/IEC/IEEE 29148:2011. Systems and software engineering. Life cycle processes. Requirements engineering. [First edition 2011-12-01]. Geneva, 2011. 94 p.

СЕКЦІЯ 3
ІНФОРМАЦІЙНА БЕЗПЕКА
ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ І МЕРЕЖ

**ПРОБЛЕМИ БЕЗПЕКИ ТА ЗАХИСТУ ТЕЛЕКОМУНІКАЦІЙНИХ
МЕРЕЖ**

Ткачук Владислав Ігорович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Проблеми безпеки телекомунікаційних мереж хвилювали міжнародне співтовариство протягом останніх двох десятиліть. Телекомунікаційна інфраструктура, яка забезпечує необхідну основу для обміну інформацією, така як голос, відео, дані та підключення до Інтернету, була особливо вразливою до різних атак. Деякі з цих атак можуть призвести до відмови в обслуговуванні, втрати цілісності та конфіденційності мережевих служб. Таким чином, захист цих мереж від атак є важливим аспектом, який не можна ігнорувати.

В першу чергу слід сказати про фізичку безпеку телекомунікаційних мереж, для того щоб уникнути руйнування встановленого обладнання, тобто запровадити необхідну технологію для захисту критичної телекомунікаційної інфраструктури. У регіонах, де відбуваються військові конфлікти з високим рівнем терактів, зовнішні телекомунікаційні інфраструктури, такі як радіоблабднання та електростанції, повинні розташовуватися в більш безпечних районах. Також може знадобитися наявність взаємної згоди між державними органами безпеки та мережевими провайдерами для забезпечення ключових телекомунікаційних установок.

Важливим кроком для керівників компаній є навчання свого персоналу. Слід розробити систематичний метод запобігання атакам або боротьби з ними в їх установі. Для цього персонал повинен часто проходити навчання. Якщо за мету є досягнення систематичного забезпечення безпеки до їх виникнення проблем, слід використовувати відповідні комп'ютерні ресурси. Телекомунікаційні приміщення повинні бути захищені та позначені як зони обмеженого доступу. Доступ до цих районів повинен контролюватися та обмежуватися лише уповноваженими та належним чином перевіреними особами. Організаціям також слід вести журнал контролю з метою аудиту безпеки.

Основним аспектом безпеки є впровадження таких інфраструктурних рішень:

1. Захист кабельних мереж від перешкод
2. Фізичні механізми контролю доступу, такі як смарт-картки та біометричні зчитувачі.
3. Брандмауери в мережі для загальнодоступних систем

4. Системи управління подіями (SIEM) для обробки подій та журналів
5. Управління системою захисту програмного забезпеченням за допомогою антивірусів, антишпигунських технологій на внутрішніх системах та поштових серверах.

6. Практика безпечної розробки додатків

7. Застосування методів шифрування даних

8. Проведення перевірок безпеки телекомунікаційного обладнання

Електронні ресурси:

1. Convergence and Next Generation Networks, Ministerial Background Report (OECD), 2007

2. M. Sif & L. Newell, Optimizing Broadband Aggregation Networks for Tripple Play Services, Alcatel Telecommunications Review, 4th Quater, 2004

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Нікітін Олексій Геннадійович
Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій

Постановка задачі. Діяльність із забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у сукупності й складають методи. Проаналізувати методи на меті конкретного плану. Продемонструвати певні приклади методів, які застосовуються в сфері інформаційної безпеки.

Мета дослідження. Ознайомитись з деякими методами забезпеченнями інформаційної безпеки, знати їх зміст принцип роботи в окремо взятому середовищі. Дослідити та запропонувати план по модернізації та покращенню роботи методів інформаційної безпеки.

Результати дослідження. Важливими методами аналізу стану забезпечення інформаційної безпеки є методи описи і класифікації. Для здійснення ефективного захисту системи управління слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними. Вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту. В залежності від загрози уможливорюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери інформаційної безпеки, то у ній зазвичай виділяють:

- фізичний;
- програмно-технічний;
- управлінський;
- технологічний;
- рівень користувача;
- мережевий;

– процедурний.

На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються і управлінських технологій.

На програмно-технічному рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення інформаційної безпеки.

На технологічному рівні здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.

На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на об'єкти інформаційної безпеки, унеможливлення інформаційного впливу з боку соціального середовища.

На мережевому рівні дана політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою.

На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт [1, с. 75-85].

Специфіка методів, що використовуються, значно залежить від суб'єкта діяльності, об'єкта впливу, а також переслідуваних цілей. Так, методи діяльності індивіда у зв'язку із його обмеженою можливістю по забезпеченню інформаційної безпеки здебільшого зводяться до джерела загрози, апелювання до суспільної думки, а також до держави, яка має вживати рішучих заходів по нейтралізації інформаційних загроз. Саме суспільство почасти використовує у своїй діяльності методи соціального регулювання, надання допомоги окремим індивідам і суспільним організаціям, яким спричинена шкода внаслідок виявлення загрози [2, с. 31].

Вельми важливим є застосування аналітичних методів пізнання і дослідження стану суспільної свідомості у сфері інформаційної безпеки. Наприклад, усвідомлення важливості забезпечення інформаційної безпеки на рівні індивіда, суспільства і організації заважає розповсюджений міф про те, що захист інформації і криптографія одне й те саме. Водночас таке розуміння є наслідком використання застарілих підходів до інформаційної безпеки, коли інформаційна безпека лише ототожнюється із захистом інформації шляхом шифрування.

Нині важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від різних загроз. Отже, система має відповідно реагувати і гарантувати ефективну діяльність у цьому напрямі.

Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передачі, тобто забезпечення її цілісності. Таким чином конфіденційність інформації, яка забезпечується за допомогою криптографічних методів не є головною вимогою при проектуванні систем захисту інформації [2, с. 98]. Виконання процедур криптокодування і декодування може уповільнити передачу даних та зменшити доступ до них через те, що користувач буде позбавлений можливості своєчасного і швидкого доступу до цих даних та інформації. Саме тому забезпечення конфіденційності інформації має відповідати можливості доступу до неї [3, с. 11-12]. Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки в першу чергу має гарантувати доступність і цілісність інформації, а її конфіденційність у випадку необхідності.

Висновки та перспективи. У цілому ж слід зазначити, що вибір цілей і методів протидії конкретним загрозам та небезпекам інформаційній безпеці становить собою важливу проблему і складову частину діяльності по реалізації основних напрямів державної політики інформаційної безпеки. У межах вирішення даної проблеми визначаються можливі форми відповідної діяльності органів державної влади, що потребує проведення детального аналізу економічного, соціального, політичного та інших станів суспільства, держави і особи, можливих наслідків вибору тих чи інших варіантів здійснення цієї діяльності. У роботі проведено теоретичне узагальнення і нове вирішення наукової задачі, що дає можливість сформулювати принципові положення, висновки і рекомендації (теоретичної і практичної спрямованості) щодо організаційно-економічних складових інформаційної безпеки телекомунікаційних мереж загального користування.

Список використаних джерел:

1. Тардаскіна Т.М. Управління персоналом системи інформаційної безпеки // Економіка: проблеми теорії та практики: Зб. наук. праць. - Дніпропетровськ, 2005. - Т. І, вип. 208. - С. 290-294. - 0,27 д.а.
2. Редькін О.С., Тардаскіна Т.М. Функціонально-вартісний аналіз системи інформаційної безпеки АТС // Економічний вісник Національного гірничого університету. - 2005. - № 4 (12). - С. 47-53. - 0,6 д.а. (Особистий внесок здобувача: здійснено функціонально-вартісний аналіз системи забезпечення інформаційної безпеки на прикладі цифрової АТС та з методичних позицій обґрунтовано доцільність витрат на її створення і впровадження. - 0,3 д.а.).
3. Тардаскіна Т.М. Оцінка витрат на систему інформаційної безпеки телекомунікаційних мереж // Економіка і управління. - 2006. - № 4. - С. 73-78. - 0,25 д.а.

ВИКОРИСТАННЯ ПРИСТРОЇВ АУТЕНТИФІКАЦІЇ ДЛЯ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

УДК:681.3.

Ільїн Д.В.

Національний університет оборони України імені Івана Черняховського

Виклики та загрози з якими зіштовхуються органи державної влади, місцевого самоврядування України та збройні формування України в сучасних реаліях протистояння агресії Російської Федерації, вимагають сучасних та ефективних рішень, щодо вирішення проблемних питань забезпечення кібербезпеки інформаційно-телекомунікаційних систем (згідно Закону України “Про основні засади забезпечення кібербезпеки України” [1] відносяться до об'єктів інформаційної критичної інформаційної інфраструктури), що використовуються для автоматизації процесів управління та забезпечення процесів повсякденної життєдіяльності.

Складовими інформаційно-телекомунікаційної системи є лінії зв'язку, комутатори, маршрутизатори, сервери та персональні електронно-обчислювальні машини. І якщо для активного мережевого обладнання, серверів та персональних електронно-обчислювальних машин може бути створена комплексна система захисту інформації та забезпечені належні умови захисту від ведення технічної розвідки, то лінії зв'язку, переважно, простягаються поза межами зони в якій може бути забезпечений такий захист. Наслідком можуть стати: несанкціоноване підключення до ліній зв'язку та перехоплення трафіку, як на обладнанні провайдера так і вздовж всієї довжини ліній зв'язку, та проведення комп'ютерних атак з подальшим несанкціонованим доступом до серверів та персональних електронно-обчислювальних машин.

В умовах поширення пандемії COVID-19 з'явилась необхідність в дистанційній роботі працівників, що створює додаткові загрози для інформаційно-телекомунікаційних систем. Забезпечити безпеку використання віддалених робочих місць набагато складніше порівняно з локальними користувачами організації.

Віддалене робоче місце користувача породжує, в порівнянні з локальним офісним робочим місцем, три додаткових чинника загроз:

- віддалений користувач знаходиться поза зоною фізичного контролю організації, необхідний доказ того, що до корпоративного ресурсу підключається саме співробітник компанії, а не зловмисник;
- дані віддаленого користувача поширюються по каналах, які знаходяться поза зоною контролю організації;
- для віддаленого робочого місця компанія не може забезпечити фізичну безпеку.

При організації віддаленого доступу повинні забезпечуватися три основні принципи інформаційної безпеки:

- конфіденційність (інформація повинна бути доступна тільки особам, яким надано право користуватись даною інформацією);

- цілісність (зміни інформації, що призводять до її втрати чи руйнуванню, повинні бути виключені);
- доступність (інформація повинна бути доступна авторизованим користувачам, коли вона їм необхідна).

Для організації захисту ліній зв'язку та роботи віддалених робочих місць необхідно використовувати наступні механізми захисту:

- надійні засоби аутентифікації користувачів;
- систему розмежування доступу до інформаційних ресурсів на основі аутентифікаційних даних;
- засоби організації VPN (апаратні пристрої та програмні рішення).

VPN з'єднання забезпечує підключення віддаленого користувача до ресурсів організації, об'єднання філіалів організацій, доступ віддалених користувачів до мережі інтернет через захищений сервер доступу організації, захист від перехоплення трафіку сторонніми особами на лініях зв'язку та обладнанні провайдерів.

Безпека VPN з'єднання досягається необхідною та достатньою довжиною ключа шифрування, частотою заміни ключа шифрування, забезпеченням безпечної аутентифікації користувача та системи сертифікації.

Використання логіну та паролю в класичному розумінні для аутентифікації у VPN не є безпечним варіантом. Користувач може забути свої аутентифікаційні дані, використовувати нестійкі паролі, пароль може бути отриманий від користувача внаслідок впливу на нього, інша людина яка дізналася пароль може скористатися їм без відома користувача.

Рішенням є використання пристрою аутентифікації, що забезпечує двофакторну перевірку для забезпечення доступу користувача. Ключ на пристрої є стійким, унікальним, його не можна скопіювати з пристрою та відтворити. Також апаратний носій забезпечує регламентовану зміну аутентифікаційних даних користувача. При компрометації пристрою його дія може бути припинена на сервері організації.

Таким чином використання в комплексі шифрування каналу зв'язку засобами VPN та двофакторної аутентифікації за допомогою пристрою аутентифікації забезпечить підвищення рівня кібербезпеки інформаційно-телекомунікаційних систем органів державної влади, місцевого самоврядування, збройних формувань України, підвищить рівень ефективності їх використання для забезпечення автоматизації процесів управління та повсякденної життєдіяльності.

Література:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 24 жовт. 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 10.03.2021).

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

Грищенко Ярослав Олександрович

*Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації*

Анотація: Розглядаються соціальні мережі, основні методи поширення інформації в соціальних мережах, зроблено аналіз переваг і недоліків різних методів захисту інформації. Проаналізовано метод визначення стратегії розповсюдження інформації в соціальній мережі, виділено основні параметри, які є базовими для забезпечення захисту інформації, можливість втрати інформації, а також методи її захисту.

Ключові слова: Інформація, інформаційна безпека, соціальні мережі.

Характерною особливістю сучасності є та обставина, що до активної участі в інформаційних процесах у дуже стислі строки долучилися широкі маси користувачів, що в переважній більшості не мають відповідного рівня підготовки до участі в суспільно корисній інформаційній діяльності.

Однак останнім часом з розвитком інформаційних технологій, удосконаленням загальносуспільної системи соціальних інформаційних комунікацій в Україні ми спостерігаємо характерний також і для інших країн світу процес самоорганізації вітчизняного інформаційного простору, формування системи соціальних інформаційних мереж [3]. Є два різні способи, за допомогою яких людина отримує інформацію в мережі: – через зв'язки в соціальних мережах і під впливом зовнішніх немережових джерел, таких як традиційні ЗМІ [2].

Соціальна мережа (від англ. Social networking service) – це платформа, онлайн сервіс або веб-сайт, призначені для побудови, відображення та організації соціальних взаємовідносин, візуалізацією яких є соціальні графи [4, с.39-58]. Наразі кількість соціальних мереж в Інтернеті і число їх користувачів швидко зростає (соціальні мережі стартували в 1995 р, в 2000-і набули глобального розмаху).

Для того, щоб соціальна мережа існувала, користувачі повинні ділитися один з одним певною частиною своєї особистої інформації. В останні 3 – 4 роки тема інформаційної безпеки та приватності в соціальних мережах привертає багато уваги. Це цілком зрозуміло: мережі все більше відкриваються зовнішньому світу, були випадки витоку особистих даних, аккаунти користувачів легко зламуються, а в адміністрації мереж є доступ до будь-якої інформації [1]. Тому виділимо основні параметри, які є базовими для забезпечення захисту інформації:

✓ конфіденційність – гарантія того, що конкретна інформація доступна тільки тому колу осіб, для кого вона призначена; порушення цієї категорії називається розкраданням або розкриттям інформації;

✓ цілісність – гарантія того, що інформація зараз існує в її початковому вигляді, тобто при її зберіганні або передачі не було проведено

несанкціонованих змін; порушення цієї категорії називається фальсифікацією повідомлення;

✓ автентичність – гарантія того, що джерелом інформації є саме та особа, яку заявлено як її автора; порушення цієї категорії також називається фальсифікацією, але вже автора повідомлення;

✓ апелюємість – гарантія того, що при необхідності можна буде довести, що автором повідомлення є саме заявлена людина, і не може бути ніхто інший; відмінність цієї категорії від попередньої в тому, що при підміні автора, інша людина намагається привласнити собі авторство повідомлення, а при порушенні апелюємісті – сам автор намагається «відхреститися» від своїх слів.

На жаль, на законодавчому рівні проблема щодо захисту інформації користувача недостатньо опрацьована. Забезпечення безпеки персональних даних в більшості випадків регламентується виключно правилами захисту інформації про користувачів і правилами користування сайтом.

Висновки: Розвиток електронних технологій дозволяє мільйонам людей вільно користуватись мережею, що дає змогу використовувати їх творчий потенціал для вирішення інтелектуальних, наукових, суспільно значимих питань. Тому можна зробити висновок, що тема захисту інформації користувачів в соціальних мережах залишатиметься актуальною як мінімум в найближчі роки. Проблеми захисту інформації в даній сфері досі остаточно не вирішені і можуть вирішитися тільки в результаті комплексного підходу, що включає в себе спільну роботу творців і розробників мережі, користувачів і держави.

Література:

1. Баловсяк Н. Соціальні мережі вбивають приватність / Тиждень.ua., 2013/ - Режим доступу: <http://tyzhden.ua/Society/70950>.

2. Соціальні мережі – реальні загрози віртуального світу. – Режим доступу: <http://ogo.ua/articles/view/2011-02-23/26490.html>.

3. Соціальні мережі як чинник розвитку громадянського суспільства : [монографія] / [О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.] ; НАН України, Нац. б-ка України ім. В. І. Вернадського. – К., 2013. – 220 с.

4. Barnes J. A. Class and Committees in a Norwegian Island Parish // Human Relations. 1954. №7. Рр. 39-58.

ПРОБЛЕМАТИКА В ПОБУДОВІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Григоренко Дмитро Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації

Побудова КСЗІ є однією з найважливіших проблем в інформаційній безпеці телекомунікаційних систем. В даній роботі ми розглядаємо труднощі з якими може зіткнутися кожен кому потрібно захистити свою систему.

В результаті проведеного аналізу можна виділити дві основні проблеми [1, с. 15]:

- Комплексна система захисту інформації не повинна заважати роботі користувачів.
- Реалізація захисту ідентифікації. Тобто зробити неможливим виток інформації людям, які не мають доступу до неї.

Багато керівників не розуміють цінності інформації, наприклад на підприємствах, тому на захист не витрачають багато коштів і в решті втрачають всю компанію. Але не потрібно розтрачувати майже весь бюджет, слід виділити час на знаходження балансу. Організації мають встановлене управління виправленнями та намагаються мінімізувати вразливі місця в інфраструктурі. Їх оцінка проводиться за допомогою сканерів на вразливість, тестів на проникнення, автоматичних сканувань, аудитів. Вразливості з точки зору управління завжди мають технічний характер. Зокрема, під ними розуміються відомі вразливості в системах та програмному забезпеченні. Загальноприйняте розуміння експертів полягало в тому, що вразливість є темою управління виправленнями та проблемою не виправлених систем.

Якщо звертати увагу на сегменти мережі, обмеження відкритих точок доступу або зовнішніх з'єднань, зміцнення систем, шифрування зв'язку або очищення проблем з конфігурацією, то деякі експерти розглядають цей фактор як тему вразливості. Фахівці використовують настанови щодо зміцнення, безпечне розгортання, процедури встановлення, огляди конструкцій та бази даних управління конфігурацією для запобігання атакам без відомих вразливих місць

Варто зазначити, що труднощі виникають навіть у складності перевірки правильно виконаних інструкцій людей, які створюють систему безпеки, також є дефіцит у знаннях про сам процес вдосконалення безпеки. Крім того, доступність базових даних є проблемою на практиці. Деякі адміністратори мають проблеми з поєднання факторів для визначення ризиків, зрозумілих для технічних працівників або для вищого керівництва [2].

Таким чином немає якогось одного комплексу, для кожної системи потрібно проводити детальну роботу з аналізом. Потрібно розуміти труднощі з якими потрібно зіткнутися та виділити час і гроші на побудову безпеки.

Список використаних джерел

1. Комплексні системи захисту інформації : навчальний посібник / Ю. Є.Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін. – Вінниця : ВНТУ, 2017. – 120 с
2. Diesch R. A comprehensive model of information security factors for decision-makers [Електронний ресурс] / R. Diesch, M. Pfaff, H. Krcmar // Технічний університет Мюнхена. – 2020. – Режим доступу до ресурсу: <https://www.sciencedirect.com/science/article/pii/S0167404820300341#sec0003>.

АНАЛІЗ БЕЗПЕКИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

*Івахненко Маріанна Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації*

Постановка задачі. Модернізація та вдосконалення інформаційного суспільства (ІС) визначають нові вимоги до сучасних інформаційно-комунікаційних технологій (ІКТ) для вирішення різних проблем глобалізації, віддаленого доступу до інформаційних ресурсів та хмарних обчислень, розподіленого інформаційного обслуговування та віртуального середовища та визначення адекватної політики інформаційної безпеки на підприємствах. До цієї групи слід також включити соціальні мережі та соціальні медіа, оскільки сучасні ІКТ дозволяють розширення соціальних відносин та підтвердження поля «соціальних обчислень», пов'язаних із побудовою мереж веб-сайтів (MySpace, Facebook, Twitter, XING, LinkedIn, YouTube, Pinterest, Foursquare, Newshub, e-Britanica тощо). Інформаційне суспільство створило різні можливості для віддаленого доступу до розподілених інформаційних ресурсів та комунікацій між користувачами (віртуальне середовище, хмарні сервіси, соціальні медіа тощо). Усі ці аспекти глобалізації змушують користувачів створювати власний профіль із особистими даними та публікувати особисту інформацію.

Мета дослідження. Права на конфіденційність пов'язані з особистою інформацією, яка може бути зібрана в процесі використання соціальних мереж. Можна збирати та фіксувати будь-яку особисту інформацію без відома користувача, крім того, персональні дані можуть бути розповсюджені законно або незаконно для будь-якої третьої особи. Отже, існує потреба обговорити проблеми соціальних мереж для захисту даних як компоненту конфіденційності.

Конфіденційність у соціальних мережах стосується захисту інформації користувача та забезпечення прав користувача. Деякі проблеми соціальних медіа для PDP [1]:

- Важливим обов'язком контролерів даних є створення надійного PDSS для реалізації принципів усіх структурних рівнів та чітке, зрозуміле та прозоре інформування кожного користувача для використання персональних даних. Це вимагає як початковий крок визначення ролі "контролера даних", "процесора даних" та "суб'єкта даних" у соціальних мережах та визначення відповідальності за процедури захисту даних (правила, заходи, конфіденційність та права суб'єктів даних, тощо). Проблема в соціальних мережах полягає в тому, що функції замовника, постачальника та постачальника та взаємозв'язок між ними можуть бути визначені лише для конкретного випадку [2].

- Ще однією проблемою, яку можна визначити в соціальних мережах, є право суб'єкта даних бути поінформованим. Це інтегрована

проблема, оскільки особи мають різні права під час обробки персональних даних.

- **Обов'язок контролерів** - гарантувати легкий доступ до власних персональних даних користувачів. Це дозволить реалізувати права користувача на перегляд, доступ, блокування або видалення своїх персональних даних у профілі (що є основним правом, гарантованим законами про захист даних). Іншою стороною проблеми є доступ до інформації у профілі - контролер повинен гарантувати, що кожен користувач може визначити обмеження для доступу до власного профілю. Це запобіжить несанкціонованому доступу та неправильному поширенню особистої інформації.

- **Міжнародна передача даних** може бути визначена наступною можливою проблемою конфіденційності в соціальних мережах. Згідно з основними принципами PDP, особисті дані можуть бути передані іншій країні, якщо їх рівень PDP адекватний. Передача даних між різними постачальниками послуг є типовою процедурою в соціальних мережах, оскільки вузли (сервери, клієнти, сховища тощо) можуть бути розташовані в будь-якій точці світу.

- **Видалення даних.** Якщо будь-який користувач хоче видалити дані у своєму профілі, він / вона повинен бути впевнений, що ці дані будуть дійсно видалені. У деяких випадках дані можуть бути передані іншому постачальнику послуг, а копія даних може зберігатися в інших місцях. Це буде проблемою конфіденційності особистості. Інший випадок, коли інформація, яку видалили або видалили користувач, передається третій стороні перед видаленням.

- **Спільна інформація** - соціальна мережа реалізується в Інтернеті, і всі інформаційні ресурси можуть бути доступними з різних точок світу. Це провокує традиційну небезпеку у глобальній мережі (втрата даних, руйнування цілісності, проблеми з підзвітністю, атаки хакерів тощо). Кожен користувач завантажує інформацію, якою обмінюватиметься набір користувачів соціальної мережі, і її можна буде розповсюджувати в різних місцях. У цьому випадку суб'єкт даних не знає, яка політика та заходи використовуються для протидії можливим атакам.

- **Технічні та організаційні заходи щодо захисту даних** - реалізація відповідних заходів щодо захисту інформації є важливим обов'язком для контролерів даних. Ці заходи повинні бути протидією всім формам знищення або втрати персональних даних, несанкціонованому доступу (під час обробки або передачі персональних даних за допомогою ліній зв'язку), а також усім незаконним формам обробки. Постачальники послуг повинні гарантувати ефективний захист цілісності та доступності даних.

Висновок. За результатами аналізу безпеки щодо захисту інформації в соціальних мережах встановлено, що конфіденційність у соціальних мережах може бути підірвана багатьма факторами, обумовленими неправильним використанням персональних даних. Справа в тому, що молоді люди воліють спілкуватися через соціальні мережі, і до цих форумів легко дійти. Однак доступ до персональних даних користувачів повинен бути обмежений.

Список використаних джерел:

1. Romansky R. SOCIAL MEDIA AND PERSONAL DATA PROTECTION [Електронний ресурс] / Radi Romansky. – 2014. – Режим доступу до ресурсу:

НЕЙРОННІ МЕРЕЖІ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Свертока Владислав Валерійович

Державний університет телекомунікацій

Навчально-науковий інститут Захисту інформації

Одним з найбільш перспективних напрямків прийнято вважати штучні нейронні мережі, які є (подібно біологічним) обчислювальною системою з величезним числом паралельно функціонуючих простих процесорів з безліччю зв'язків. Незважаючи на те, що при побудові таких мереж зазвичай робиться ряд припущень і значних спрощень, вони багато в чому демонструють властивості, притаманні людському мозку, - навчання на основі досвіду, узагальнення, витяг істотних даних з надлишкової інформації, здатність вирішувати неформалізовані завдання.

У коло завдань, які можуть бути вирішені з використанням ІНС, входять завдання класифікації, прогнозування, оптимізації, управління і багато інших, які потребують обробки різнопланової інформації, вилучення знань, проведення інтелектуального аналізу і знаходження оптимального рішення. У порівнянні з традиційними математичними методами нейромережеві технології забезпечують досить високу якість рішень при менших витратах. Вони дозволяють виявляти нелінійні закономірності в сильно зашумлених неоднорідних даних, дають хороші результати при великому числі вхідних параметрів і забезпечують адекватні рішення при відносно невеликих обсягах даних.

Нейронні мережі – це потужний і на сьогодні, мабуть, найкращий метод для вирішення завдань розпізнавання образів в ситуаціях, коли відсутні значні фрагменти інформації, а наявна інформація гранично зашумлена. Застосовується система автоматичного виявлення правопорушників в системах відеоспостереження на основі нейронних мереж, що дозволяє фіксувати інформацію і повідомляти правоохоронні органи про застосування вогнепальної зброї.

У системах забезпечення інформаційної безпеки нейронні мережі вельми ефективні при вирішенні завдань аналізу трафіку, аудиту баз даних, евристичного детектування шкідливих атак і нових типів вірусів, аналізу поведінки зловмисника і виявлення аномалій в діях користувачів.

Раніше нам доводилося займатися розбором вразливостей вручну - тільки так можна було зрозуміти, чи коректно спрацювали системи захисту, чи дійсно існує знайдена ними вразливість і чи настільки вона серйозна. Нейронна мережа допомагає економити до 70% часу на розбір. А також ефективно доповнює інші системи безпеки.

Література:

1. Нейросетевые технологии в безопасности [Электронный ресурс] // - Режим доступа: <https://lib.itsec.ru/articles2/Oborandteh/neyrosetevye-tehnologii-v-biznese>
2. Как мы анализируем уязвимости с помощью нейронных сетей и нечеткой логики [Электронный ресурс] // - Режим доступа: <https://habr.com/ru/company/pt/blog/323436/>
3. Брюхомицкий Ю.А. Нейросетевые модели для систем информационной безопасности. Учебное пособие. – Таганрог: Изд-во ТРТУ, 2005. – 160 с.

ЗАСОБИ ТА МЕТОДИ ВИЯВЛЕННЯ ЗАКЛАДНИХ ПРИСТРОЇВ ПРИХОВАНОГО АУДІО ТА ВІДЕО СПОСТЕРЕЖЕННЯ

*Царенко Богдан Віталійович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації*

Що таке відео та аудіо сигнал, особливості сигналів, методи передачі сигналів, засоби прихованого відеоспостереження і зйомки, типи спостереження, методи виявлення закладних пристроїв

Особливості відеосигналу

Відеосигнал завжди носить імпульсний характер і чим чіткіші контури переданих об'єктів, тим крутіші фронти імпульсів його компонентів. Сигнал від відеопередавача може бути переданий за межі контрольованої зони по існуючих дротяних лініях. Відеосигнал широкосмуговий, для якісної передачі на істотну відстань потрібно екранований кабель. По двопровідним лініям відеосигнал може передаватися або на невелику відстань, або з низькою якістю і низькою частотою дотримання кадрів.

Аудіоканал як складова відеопередачі

Застосування в відеопередавачі відкритого аудіоканали полегшує виявлення відеопередавачі. Аудіоканал може бути прослуханий або ідентифікований автоматично коррелятором по акустичному.

Для аналогових видів модуляції (АМ і ЧМ) аудіоканал є таким, що окрему, що несе в загальному спектрі сигналу.

Особливості сигналів

Спектр відеосигналу залежить від переданої відеоінформації. Спектр АМ та ЧМ відеопередавачів в темряві являє собою несучу частоту, модульовану частотами рядкової і кадрової розгортки, і не є широкосмуговим сигналом. При аналізі характеристик сигналу з передачею аудіо інформації оператор може використовувати акустичний тест-сигнал, спостерігаючи зміну характеристик. Також змінивши освітлення увімкненням \ вимкненням приладів освітлення можна простежити зміну характеристики сигналу відео- передавача, таким чином ідентифікувавши відеопередавач встановлений в приміщенні.

Передачі сигналів

Сигнал від відеопередавачі може бути переданий за межі контрольованої зони за існуючими провідних лініях. Двopовідними лініями відеосигнал може передаватися або на невелику відстань, або з низькою якістю і низькою частотою проходження кадрів.

Зараз же головними партнерами в роботі безпроводних мінівідеокамер є мобільні оператори зв'язку і безпроводного WI-FI інтернету. Так виходячи з цього можна виділити три головних види безпроводного прихованого відеоспостереження:

- Приховане радіо відео спостереження;
- Приховане WI-FI відео спостереження;
- Приховане GSM відео спостереження.

Засоби прихованого відеоспостереження і зйомки.

Безпроводне та дротове відеоспостереження. Безпроводне відеоспостереження застосовується в ситуації, коли немає можливості прокласти провідний канал передачі відеосигналу, або в разі, коли прокладка кабелів такої кількості і довжини нераціональна з тих чи інших причин. Наприклад, дуже зручно виконувати тимчасову систему відеоспостереження на основі бездротові технології. Одним з плюсів дротових відеокамер спостереження є що живлення та відео можна отримувати по одному і тому ж кабелю. Немає перешкод від телефонів, Bluetooth, бездротових мереж, мікрохвильових печей, відеонянь або автосигналізацій. Для використання доступний більш широкий спектр стилів відеокамери.

Типи спостереження

Аналогові відеокамери - цей тип камери характеризується простотою установки та підключення коаксіальним кабелем.

TVI та CVI - це технології Hikvision та Dahua із закритим HD телебаченням відповідно.

AHD - тип аналогової камери високої чіткості, який є альтернативою між високою чіткістю та аналоговим відео.

IP відеокамери - це сучасні цифрові відеокамери, передача сигналів яких відбувається через локальну мережу та Інтернет.

Гібридна відеокамера - це камера високої чіткості, яка дозволяє записувати та передавати сигнали різних форматів за своїми можливостями.

Порівняно новий продукт на ринку відеоспостереження - це підвид IP-камер - Wi-Fi камери.

Методи виявлення закладних пристроїв:

- Підготовка та первинне обстеження приміщення;
- Оцінка ймовірності супротивника;
- Оцінка умов, в яких відбувається рішення;
- Первинний огляд та технічна перевірка;
- Методи пошуку прихованих відеокамер (радіомоніторинговий, оптичний метод, пошук нелінійним локатором).

Література:

1. Лопатин В. В. Правовые аспекты информационной безопасности / В. В. Лопатин // Системы безопасности связи и телекоммуникаций. 1998.
2. Хорев А. А. Способы и средства защиты информации / А. А. Хорев. – М. : МО РФ, 1998
3. Халяпин Д. Б. Основы защиты промышленной и коммерческой информации / Д. Б. Халяпин, В. И. Ярочкин. – М. : ИПКИР, 1994

ПОШУК ВРАЗЛИВОСТЕЙ ЗА ДОПОМОГОЮ ФАЗЗІНГУ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Монастирський І.В.

*Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій*

Анотація. У міру розвитку і ускладнення інформаційних систем загострюються проблеми їх інформаційної безпеки. Вразливість безпеки є однією з першопричин загроз кібербезпеки. Цей факт ставить особливі вимоги до своєчасного виявлення вразливостей використовуваного програмного забезпечення та проведення аудиту інформаційної системи. Щоб виявити вразливості та виправити їх заздалегідь, дослідники запропонували кілька прийомів, серед яких найпоширеніший - фаззінг, тому в цій роботі

У сучасних інформаційних системах актуальна тема вразливостей різного роду: переповнення буфера, витоку пам'яті, погане шифрування, недостатня перевірка вхідних даних тощо. Атакуюча сторона активно використовує ці найбільш поширені вразливості систем, тому в даний час інформаційні ресурси стають головною метою атак з боку злоумисників. Для захисту програмно-інформаційних ресурсів часто використовуються стандартні методики забезпечення інформаційної безпеки системи і її програмного забезпечення. Об'єктом дослідження виступає процес виявлення вразливостей в програмному забезпеченні під час аудиту безпеки. Предметом дослідження є технології фаззінга, застосовувані під час пошуку вразливостей. Завдання роботи полягає в розробці та використанні системи фаззінгу-тестування програмного забезпечення на предмет наявності в ньому вразливостей та розробка нових методів і вдосконалення існуючих засобів для проведення фаззінгу.

Фаззінг - це технологія автоматизованого тестування програмного забезпечення з метою виявлення потенційних вразливостей, яка охоплює велику кількість граничних випадків шляхом породження некоректних вхідних даних. Фаззінг використовується в основному в якості автоматизованої техніки виявляти вразливостей безпеки критично важливих програм, які можуть бути експлуатовані злоумисно. У більш загальному плані, фаззінг використовується для демонстрації наявності помилок, а не їх відсутність. Перевага такого підходу полягає в тому, що при даному тестуванні практично повністю відсутні помилкові спрацьовування, на відміну від статичних аналізаторів. Залежно від методики генерування вхідної інформації існуючі технології фаззінга можна умовно розділити на два класи: мутація існуючих даних та генерація нових даних. В якості вхідних даних при цьому можуть виступати оброблювані додатком файли, інформація, що передається по мережевим протоколам, функції прикладного інтерфейсу і т. д. Однією із основних проблем напрямку фаззінгу є вузьконаправленість, тобто під кожен систему для ефективного етапу фаззінгу слід генерувати окремі насадки вхідних даних, та налаштовувати програму для фаззінгу під особливості інфраструктури системи. Такі проблеми

формують затримки в виконанні роботи системи та її відлагодженні, що є критичним фактором для подальшої оптимізації та поліпшенням ефективності роботи методу фазинга.

У сфері аудиту безпеки фаззінг - це зазвичай автоматизований процес пошуку критичних помилок програмного забезпечення шляхом випадкового впорядкування різних перестановок даних у цільовій програмі, доки одна з цих перестановок не виявить вразливості. Основними категоріями програмного тестування є тестування чорного, сірого та білого ящиків. Різниця між цими категоріями визначається тим, який рівень інформації доступний для фазингу. В даний час технологія фаззінга дуже затребувана в інформаційному співтоваристві, оскільки дозволяє виявити уразливості в додатках і системах перш, ніж ними встигнуть скористатися зловмисники.

Висновки. У даній роботі основна увага була приділена вирішенню завдання практичної реалізації методики фаззінга як інструменту аудиту. Проблема виявлення вразливостей в програмах є однією з найважливіших в сфері інформаційних технологій. Для ефективного пошуку вразливостей, постійно розробляються і вдосконалюються різні методи. Фаззінг є одним із таких методів, який з плином часу набув популярності та виділяється своєю ефективністю. Практична значимість фаззінгу полягає в тому, що виявлення навіть однієї уразливості за короткий термін в автоматичному режимі можна вважати свідченням надійності технології, що дозволяє досить ефективно блокувати можливі атаки зловмисників. Однак на основі проведеного аналізу методів фаззінгу, можна однозначно охарактеризувати їх, як не досконалі, з своїми недоліками та перевагами, а отже існує можливість їх оптимізації та поліпшення, або створення нових методів на основі комбінації існуючих.

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

Бурлій Дмитро Вадимович

Державний університет телекомунікацій

Навчально-науковий інститут інформаційних технологій

При створенні інформаційної інфраструктури автоматизованої системи (АС) на базі сучасних комп'ютерних мереж виникає ряд питань, щодо організації захисту даної інфраструктури від загроз, які загрожують безпеці інформації. Під загрозами інформаційної безпеки традиційно розуміли можливість порушення інформаційних властивостей, таких як конфіденційність, доступність та цілісність [1].

Термін "безпека" використовується в розумінні мінімізації вразливості активів і ресурсів. Актив - це те, що має якесь значення (вартість), вразливість - це певна слабкість, яка може бути використана, щоб порушити систему або інформацію, що є в системі. Загроза безпеці інформації - потенційне порушення системи, це подія або дія, яка може призвести до спотворення,

несанкціонованого використання або руйнування інформаційних ресурсів системи, а також програмних і апаратних засобів [2].

Найважливішим аспектом інформаційної безпеки є керуваність системи. Керуваність - це і підтримка високої доступності системи за рахунок раннього виявлення і ліквідації проблем, і можливість зміни апаратної і програмної конфігурації відповідно до умов, що змінилися, або потреб, і сповіщення про спроби порушення інформаційної безпеки практично у реальному часі, і зниження числа помилок адміністрування.

Найгостріше проблема керуваності встає на клієнтських робочих місцях і на стику клієнтської і серверної частин інформаційної системи. Причина проста - клієнтських місць значно більша, чим серверних, вони, як правило, розкидані за значно більшою площею, їх використовують люди з різною кваліфікацією і звичками [3].

На практиці важко отримати точні значення інформаційних властивостей, оскільки поняття загрози важко сформулювати. Наприклад, оцінка збитків, заподіяних несанкціонованим доступом до політичної та військової інформації, взагалі не може бути точно визначена, а визначення ймовірності загрози не може ґрунтуватися на статистичному аналізі. Оцінка ступеня надійності захисних механізмів завжди є суб'єктивною. В даний час не існує стандартизованих методів аналізу безпеки АС. Отже, алгоритми дій у певних ситуаціях можуть суттєво відрізнятися [1].

Висновки. Отже, на даний час існує проблема відсутності алгоритму оцінювання захищеності інформаційних систем. Саме значення захищеності залежить від багатьох факторів, але зазвичай ґрунтується на цінності інформації в самій системі. Інформаційних систем в які не можливо проникнути не існує, система вважається захищеною якщо її взлом коштує більше, ніж інформація яку вона зберігає.

Список використаних джерел:

1. Охріменко О.Ю. (2021). Проблеми та виклики забезпечення захищеності корпоративної інформаційної системи. <https://ojs.ukrlogos.in.ua/index.php/scientia/article/download/8232/8204>
2. Проблеми захисту інформації на підприємствах [Електронний ресурс]. URL: https://pidru4niki.com/1427040647714/informatika/problemi_zahistu_informatsiyi_pidpriyemstvah
3. Гафіяк А.М., Головка Г.В. Сучасні проблеми захисту інформації. http://www.rusnauka.com/21_NIEK_2007/Informatica/23650.doc.htm

СЕКЦІЯ 4

СОЦІАЛЬНО-ЕКОНОМІЧНІ АСПЕКТИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

ВПЛИВ ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НА ЕКОНОМІЧНЕ ТА СОЦІАЛЬНЕ ЖИТТЯ

*Костюк Каріна Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Вивчення економічного та соціального впливу виробництва телекомунікацій не є новою науковою дисципліною. Економісти, політологи, соціологи та дослідники менеджменту вже давно цікавляться цією темою - з тих пір, як вони почали усвідомлювати, що інформаційно-комунікаційні технології (ІКТ) широко застосовуються в індустріальному світі. Питаннями, що викликали цей інтерес, були не лише оцінка справжнього економічного впливу ІКТ, але й те, які уроки можна витягнути з його впливу в індустріальних країнах для країн, що розвиваються.

«Телефонна компанія» - це вже не просто телефони, а телефон - це не просто зручний спосіб спілкування. Продукти та послуги, пропоновані телекомунікаційними компаніями, по черзі переходили до цікавинок, багатих на інструменти для будь-якої торгівлі.

Забезпечення цієї зміни поставило телекомунікаційні компанії на перше місце в галузі побутової електроніки. Простота використання їх продуктів, а також доступність та надійність їхніх послуг можуть мати значний вплив на ділове та приватне життя своїх клієнтів.

Суспільне значення телекомунікацій є загальновизнаним і широко зрозумілим, що відображається у його майже повсюдному проникненні та використанні. Нижче зазначено деякі ключові сфери впливу:

- Телекомунікації забезпечують технологічну основу для спілкування в сучасному суспільстві. Спілкування відіграє центральну роль у фундаментальних операціях суспільства - від бізнесу до уряду та сімей. Насправді спілкування між людьми є суттю того, що відрізняє організацію, громаду чи суспільство від сукупності індивідів. Спілкування від перегляду веб-сторінок до дзвінків на стільникові телефони і до обміну миттєвими повідомленнями - все більше інтегрується в те, як ми працюємо, граємо та живемо.

- Телекомунікації відіграють все більш важливу роль у забезпеченні участі та розвитку людей у громадах та країнах, що зазнають неблагополуччя, незалежно від того, чи є це у сільській місцевості США чи в країнах, що розвиваються, у світовому суспільстві та економіці.

- Телекомунікації забезпечують життєво важливу інфраструктуру національної безпеки. Починаючи з ліквідації наслідків стихійного лиха, закінчуючи внутрішньою безпекою, передаючи життєво важливі розвідувальні дані, продовжуючи військову перевагу, телекомунікації відіграють ключову роль. Коли проблема полягає у протидії противнику, важливо не тільки зберегти телекомунікаційні можливості, але й мати вищі можливості. Існують також і потенційні ризики, пов'язані з використанням зарубіжних джерел інновацій, технологій, додатків та послуг.

Дослідження ж економічного впливу телекомунікаційних технологій підтверджують важливість та необхідність технологій в економіці. Встановлено, що телекомунікаційні мережі мають позитивний вплив на економіку в усіх сферах:

- покращення якості життя в результаті здатності працювати віддалено;
- продуктивність праці: більша ефективність в обробці завдань, пов'язаних з інформацією ;
- швидкість транзакцій: швидше завершення міжфірмових операцій транзакції з подальшим зменшенням витрат;
- інноваційний потенціал: інновації можуть бути збільшені за рахунок впорядкованої співпраці між фірмами екосистеми.

Зараз важко передбачити майбутній вплив телекомунікаційних технологій, послуг та програм, які ще не винайдені. Адже у перші дні досліджень та розробок Інтернету, наприкінці 1960-х, хіба хтось міг передбачити повний вплив широкого використання Інтернету сьогодні?

Електронні ресурси

1. <https://www.nap.edu/read/11711/chapter/3#5> (дата звернення: 18.04.2021)
2. <http://ctmaworld.com/Industries-Telecomms.htm> (дата звернення: 16.04.2021)

РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЧНОМУ РОЗВИТКУ УКРАЇНИ

*Олійник Тимофій
Державний Університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Україна все частіше підіймає питання про рівень розвитку та частоту впровадження інформаційно-телекомунікаційних технологій, що контролюється у всьому світі шляхом складання офіційних рейтингів найбільш передових країн у галузі інформаційно-телекомунікаційних технологій.

Важливим фактором рівня національного економічного розвитку є підтримка державою впровадження інноваційних інформаційно-телекомунікаційних технологій. Іншими словами, розвиток ІКТ здійснюється не лише у сфері компаній, асоціацій та окремих видів діяльності, а й у всій країні.

Сучасні інформаційні технології ставлять високі вимоги до гнучкості та масштабованості комп'ютерних мереж. Очікується, що програмно налаштовані мережі будуть використані для вирішення багатьох існуючих проблем та створення автоматизованої, програмованої, гнучкої та економічно ефективної мережевої інфраструктури, але провідні постачальники мають дуже різні стратегії SDN.

Програмно визначена мережа (SDN) - це не просто мережа, це також новий метод проектування, побудови, експлуатації та управління мережею, який розділяє контроль та управління мережею для досягнення кращої оптимізації мережі. Основні переваги мережі конфігурації програмного забезпечення (PCN) включають: централізоване управління в середовищі декількох постачальників, зменшення складності мережі за допомогою автоматизації, підвищення інноваційної швидкості, підвищення надійності та безпеки мережі, забезпечення стратегій контролю доступу, інженерії трафіку та якості консенсусу, безпека та інші аспекти, централізоване управління ("точка") управління мережею, тим самим покращуючи сприйману користувачем якість послуги.

SDN і OpenFlow з'являються в новій мережевій парадигмі. Оскільки мережі SDN більше не закриті та важкі для програмування, вони перетворені у відкриті програмовані компоненти більшої хмарної інфраструктури. SDN дозволяє власникам мереж та операторам краще контролювати свою інфраструктуру для налаштування та оптимізації, тим самим зменшуючи капітальні та експлуатаційні витрати. SDN дозволяє постачальникам послуг створювати нові можливості для отримання прибутку, створюючи програмні додатки на базі ПК, мобільної та веб-індустрії, які успішно працюють протягом багатьох років.

Переваги впровадження мережі SDN:

1. Знизити експлуатаційні витрати та витрати на обладнання;
2. Адаптованість;
3. Збільшення часу безвідмовної роботи;
4. Удосконалити управління та планування;
5. Безпека та жорсткість.

Звіт про ринок SDN (маршрутизація SDN, контролер, віртуалізація в хмарі, віртуалізація мережевої безпеки, кінцевий користувач) - Глобальні досягнення, прогнозування та аналіз ринку (2014-2019) вказує на те, що рішення SDN використовуються в банківській діяльності, фінансових послугах та страхуванні (BFSI) та інших галузях, навчальних закладів, уряду та ІТ-галузі [1].

Тому BFSI: Фінансові та страхові організації покладаються на цифрові мережі для повсякденної діяльності; великі компанії платять багато комісій за транзакції в такому форматі. Рішення типу SDN зменшать ці витрати і дозволять компаніям здійснювати більш жорсткий контроль над мережею за допомогою централізованого інтерфейсу.

Навчальні заклади: Навчальні заклади повинні впроваджувати подібні процеси, включаючи організацію навчального процесу, безпеку навчальних

закладів та запровадження ІКТ для покращення якості освіти. SDN зменшує витрати на управління завдяки системам моніторингу та контролю в режимі реального часу, впроваджує ІКТ-рішення та підвищує рівень безпеки. Уряд: Урядова інфраструктура знаходиться на найвищому рівні в кожній категорії. Технологія SDN дозволяє адміністраторам мережі не тільки зрозуміти стан своєї інфраструктури, але й ефективно оптимізувати їх для впровадження різних ІКТ-рішень у режимі реального часу.

Інформація та телекомунікації: Ця сфера отримує вигоду від запровадження SDN, як і уряд. В даний час створення великої магістральної інфраструктури, поширеної по всій країні, є непростим завданням. У SDN всі зміни обробляються легко і швидко в Центрі мережевих операцій або в NOC [2].

Впровадження мережі SDN на національному рівні дозволяє не лише економити гроші та заробляти, а й створювати високоякісне інформаційне суспільство. Інтерес світових компаній до мереж SDN очевидний: новітні технології дозволяють їм вирішувати свої проблеми ефективніше і, що найголовніше, за значно менші гроші. Лише спільними зусиллями державного та комерційного секторів, спрямованих на розвиток країни, її економіку та доходи загалом, можна досягти рівня розвитку прогресивної країни та побудувати інформаційне суспільство.

Література:

12. Крайчук С. О. Стан запровадження інформаційних технологій в управлінні сучасними підприємствами / С. О. Крайчук // Електронний журнал «Ефективна економіка». – 2016. – № 4.
13. Бившев В. О. Інформаційні технології в економіці / В. О. Бившев, О. І. Богомолів, В. І. Костюнін // Науковий журнал «Бізнес інформ». – 2012. – №10.
14. Мельник П.І. Інформаційне забезпечення фінансів підприємства / П. І. Мельник // Науковий журнал «Проблеми і перспективи економіки та управління». – 2012.

ПРОБЛЕМИ ТА ПЕРЕВАГИ КРИПТОВАЛЮТ ЯК ФІНАНСОВОГО АКТИВУ

Вавринчук Е.М.

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

На сьогоднішній день важко зустріти людину яка б не чула про криптовалюту. В Україні не передбачається нормативно-правової бази, що могла б регулювати криптовалюти, проте її відсутність не забороняє використання віртуальних валют. Термін “криптовалюта” розуміє поняття цифрової валюти, що працює на складних обчисленнях, але яку легко перевірити зворотними математичними діями. Такий принцип роботи цифрової валюти передбачає використання великих комп'ютерних потужностей для виконання обчислювальних задач. Щоб визначити чи можна використовувати криптовалюти у вигляді фінансового, тобто інвестиційно-спекулятивного активу, розглянемо їх переваги та недоліки на прикладі Bitcoin.

Таблиця 1

Переваги та недоліки використання криптовалюти

№	Переваги	Недоліки
1	Відсутність інфляції. У системі Bitcoin максимально можлива грошова маса обмежена та збільшується з визначеною швидкістю. Тому, товарні ціни залишаються на однаковому рівні, що призводить до відсутності знецінення валюти	Відсутність гарантій. Власники біткойнов не мають ніяких гарантій, що вони хоча б зможуть повернути свої гроші, які в них вклали. курс біткойнів встановлюється ринком, і може навіть впасти до нуля
2	Прозорість – всі операції з електронною готівкою зберігаються в базі безстроково, а тому кожний користувач мережі має можливість перевірити баланс крипто гаманця.	Для того щоб скористатися засобами, вкладеними в систему Bitcoin, необхідно мати доступ в інтернет, програмне забезпечення і пароль від власного гаманця
3	Значна економія витрат на емісію грошей. Оскільки система Bitcoin є нематеріальною, то чеканка монет і друкування банкнот, а також пов'язані з цим витрати на обслуговування є непотрібними.	Втрата пароля до електронного криптогаманця або його непрацездатність ведуть до безповоротної втрати всього, що знаходиться в ньому.
4	Децентралізація – відсутність емісійного центру впливає на те, що валютний курс не може бути ніким продиктований і встановлюється відповідно до умов попиту і пропозиції.	Неможливість зупинки або скасування транзакцій.
5	Висока система захисту – криптовалюту не можна підробити завдяки системі захисту блокчейн.	Високі ризики волатильності, що перетворюють Bitcoin у вкрай нестійкий з економічної точки зору актив.

Розглянувши переваги та недоліки криптовалют на прикладі Bitcoin, як інвестиційно-спекулятивного активу можна зробити висновок, що така популярність криптовалют може передбачати загрозу стабільності національних валют, адже з кожним днем інтерес до криптовалют стрімко зростає, оскільки більшість людей потребують так званих “справедливих грошей”, тобто таких, що є анонімними і захищеними від підробок, і всі криптовалюти надають такі можливості. Криптовалюта на даний момент є найбільш зручним засобом як платежів так і валютою для зберігання та накопичення активів, адже стрімкі коливання в вартості приносить великий дохід власникам валют. Проте на думку світового центрального банку це є можливість заявити про небезпечність зберігання коштів і отримання можливого доходу у таких крипто валютних системах передбачає великий ризик. Стабілізація курсу валют та відсутність інфляції у криптовалют стають причиною того, що економічно активна частина населення відмовляється від національної валюти на користь саме криптовалют. І тому центральні банки та

різні фінансові установи змушені вимагати заборони використання криптовалют.

Література:

1. Молчанова Е. Глобальна сервісна природа сучасних криптовалют / Е.Молчанова, Ю.Солодковський // Міжнародна економічна політика. – 2014. – № 1. – С. 60–65.
2. Обзор цифровых валют. [Електронний ресурс] // Режим доступу до матеріалів:https://www.prostobank.ua/internet_banking/stati/obzor_tsifrovyyh_kriptovalyut

СУЧАСНІ ТЕХНОЛОГІЇ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ В ЛОГІСТИЦІ

Снурніков О.О.

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій*

Процес впровадження цифрових технологій в діяльність організацій транспортної сфери не тільки сприяє підвищенню їх конкурентоспроможності, а й веде до цифровізації економіки країни в цілому.

Завдяки появі інноваційних технологій, таких як хмарна логістика, блокчейн, великі дані і IoT, процес розвитку галузі триває. Описані нижче п'ять технологій роблять ланцюг поставок більш орієнтованими на клієнта.

1. Хмарна логістика

Використання хмарних технологій в логістиці набирає значні оберти, та стає популярною. Хмарними сервісами вже користуються понад 50% логістичних постачальників та близько 20% планують впровадження. Завдяки планомірному переносу даних в хмару, підприємці можуть зекономити на витратах IT-рішень. Це означає, що вони платять тільки за потрібну їм послугу і коли потрібно. Завдяки використанню таких сервісів як Freightly і Shipwire надається змога управління транспортом в режимі реального часу. Ці сервіси охоплюють всі процеси : закупівля, виставлення рахунків, відстеження транспорту, відстеження вантажу та інші. Саме це робить все простіше та дешевше для компанії.

2. Електронна авіанакладна (e-AWB) – була першим кроком до цифровізації галузі. Це цифрована версія існуючих паперових авіанакладних але з певними стандартами, яка супроводжує вантаж від відправника до вказаного місця доставки.

E-AWB підвищує якість відстеження та ефективність обробки даних вантажу, а також безпеку шляху проходження і прозорість. Використання e-AWB знижує затримки і витрати. На початку 2019 року IATA (міжнародна асоціація повітряного транспорту) оголосила про перехід на e-AWB. Імениті авіакомпанії: Emirates і Lufthansa, United Airlines і Delta Airlines, вже впровадили електронну авіанакладну. А на кінець 2020 року 80% авіанакладних стали електронними.

3. Великі дані і машинне навчання

Дані в нашому світі мають найцінніше знання, завдяки використанню big data відбувається стрімкий розвиток бізнес-моделей підприємств. Застосування

штучного інтелекту спростило прогнозування оптимізацію маршрутів, попиту, використовувати прогнозну аналітику і дозволило управляти ризиками. Витрати на підприємстві скоротилися, в середньому на 49%, а введення нових смарт-рішень відбувається в 44% випадків (інформація зі звіту Big Data Executive).

Великі дані замінять логістичні бізнес-моделі з реактивних на прогнозовану. Прогнозування різких стрибків продаж можна завдяки аналітиці використання даних онлайн-постачальників, це значить, що постачальник зможе відправити додаткову партію вантажу(товару), як тільки в цьому виникне необхідність.

4. Блокчейн

Блокчейн також залишив свій відтиск на ринку транспортної цифрової логістики, оскільки завдяки цій технології можна вдосконалити систему сплати рахунку. Ми отримуємо функцію яка активує списання коштів за оплату тільки після того як товар прибуде до пункту призначення.

5. Інтернет речей (IoT)

IoT (Internet of Things) - це велика мережа штучних і природних фізичних об'єктів які пов'язані з використанням датчиків і інтерфейсів прикладного програмування (API) для спільного використання даних через Інтернет.

На мою думку саме ця технологія задає значний поштовх в розвитку цифрової трансформації, завдяки їй проводиться моніторинг товарів по всьому ланцюгу. Використання сучасних GPS-стеження за автотранспортними засобами та RFID-датчиків можна використовувати для збору даних про стан, місцезнаходження активів, температурі і інших формах даних про конкретних елементах. Це допоможе менеджерам ланцюга поставок впровадити більш ефективний контроль якості, забезпечити своєчасні поставки, мінімізувати крадіжки і дати загальне уявлення про функціонування ланцюга поставок, щоб допомогти у прийнятті рішень.

Дані IoT можуть використовуватися для оптимізації планування маршрутів і їх перепланування, управління витратою палива і скорочення викидів для збільшення показників зеленої діяльності компанії. Управління запасами і прогнозування. Датчики IoT можуть використовуватися для відстеження запасів і надання даних, які допоможуть в аналізі тенденцій для прогнозування майбутніх потреб у запасах. Це допоможе уникнути ситуацій з недостатнім запасом і надлишковим запасом.

Приведено в приклад декілька основних функцій даної технології, але існує набагато більше функціональних можливостей, що може запропонувати технологія IoT для рішення задач логістичним компаніям та споживачам.

Можна впевнено сказати, що цифрова трансформація вже вдарила по індустрії, але очікується набагато більше в найближчі 2-3 роки. Технології цифрування в логістиці виступають засобом які допоможуть з вирішенням ключових завдань отримання конкурентоспроможності галузі транспорту та логістики.

Література

1. Никишов С.И. Цифровая трансформация логистики – Москва, 2019. – 25 с.
2. Интегратор digital-технологій, інноваційних програмних продуктів, інструментів і сервісів для цифрового перетворення корпоративного ринку. URL: <https://www.everest.ua/> (дата звернення: 02.04.2021)

ОСОБЛИВОСТІ ТА ІНСТРУМЕНТИ ЦИФРОВОГО МАРКЕТИНГУ

Висоцький А.Ю

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

Цифровизація є основним трендом розвитку сучасного суспільства. Всесторонньо проникаючи в економіку, державне управління і соціальну сферу цифрові технології сприяють підвищенню ефективності всіх громадських і бізнес-процесів [1-4].

Крім цього, вони відкривають принципово нові можливості для економічного і соціального зростання [5]. Однією з таких можливостей став цифровий (digital) маркетинг.

Термін «цифровий маркетинг» увійшов у вжиток наприкінці 1990-х рр. і розглядався в той період як сукупність заходів щодо просування продукції з використанням інформаційних і телекомунікаційних технологій [5]. Однак в даний час правильніше визначити цифровий маркетинг як самостійну концепцію маркетингової діяльності в цифровому просторі, що включає в себе маркетингові дослідження, ціноутворення, продаж, просування, а в окремих випадках, і створення продукту. Цифровий маркетинг має на увазі використання digital-технологій на всіх етапах взаємодії з клієнтом. У XXI столітті споживачі проводять в цифровому світі занадто багато часу, при цьому їх мислення і діяльність безпосередньо в цифровому середовищі може істотно відрізнятись від традиційної купівельної поведінки. Тому маркетингологи повинні навчитися працювати в цифровому світі настільки ж ефективно, як і в традиційному бізнес-середовищі, відійти від сформованих стереотипів вирішення маркетингових завдань і прийняти, а в ідеалі, нав'язати потенційним клієнтам нові правила гри.

Концептуально цифровий маркетинг базується на клієнтоорієнтованому підході. Використання передових цифрових технологій дозволяє компаніям охопити максимум цільових споживачів і налагодити ефективність взаємодії з ними (цілодобові послуги, оперативна обробка замовлення, швидке реагування на звернення, цілодобова підтримка і т.п.), що і забезпечує високу результативність даного підходу. Типовими завданнями цифрового маркетингу є також збір контактних даних зацікавлених користувачів, інформування

цільових аудиторій, створення бази постійних клієнтів, збір даних в ході маркетингових досліджень, підвищення охоплення і впізнаваності бренду, формування позитивного іміджу компанії або продукту, «розкрутка» інноваційного продукту, підвищення споживчої лояльності.

Розробляти ефективну маркетингову стратегію дозволяють інструменти цифрового маркетингу. Інструментами цифрового маркетингу є всі способи і засоби вирішення маркетингових завдань на основі digital-технологій. До основних інструментів можна віднести:

- SEO - оптимізацію сайту для підвищення його позицій в пошукових системах;

- SMM - роботу з групами в соціальних мережах, в тому числі створення і розміщення контенту, організацію конкурсів і інших форм взаємодії з аудиторією;

- SERM - управління репутацією компанії за рахунок створення її позитивного іміджу на майданчиках з відгуками; нативну рекламу, що представляє собою публікації на сторонніх ресурсах (відгуків, експертних думок і ін.), які підштовхують до купівлі товару / послуги;

- SMS - розсилки рекламних повідомлень абонентам стільникових мереж; вірусну рекламу, яка передбачає створення контенту (найчастіше мультимедійного) з провокаційним змістом, через що користувачі самі поширюватимуть його в глобальній мережі (на своїх блогах, з друзями і т.п.); використання QR-кодів; просування та продаж через соціальні мережі. Досягти максимального охоплення цільової аудиторії дозволяє, як правило, застосування комплексу різних інструментів.

Основними каналами цифрового маркетингу є глобальна мережа інтернет, цифрове телебачення, мобільні мережі, локальні комп'ютерні мережі. Доступ до каналів забезпечується різноманітним обладнанням: комп'ютерами, планшетами, мобільними гаджетами, різними smart-пристроями, що мають WI-FI-підключення до мережі інтернет, терміналами самообслуговування, інтерактивними екранами, POS-терміналами.

Вибір інструментів і каналів цифрового маркетингу залежить від трьох ключових факторів: характеристик цільового сегменту, особливостей продукту і фінансових можливостей підприємства. Важливим фактором забезпечення ефективності застосовуваних інструментів є аналіз результативності кожної окремо взятої кампанії або інструменту.

Винятковими можливостями у використанні цифрового маркетингу мають інфокомунікаційні компанії, які в силу специфіки свого бізнесу володіють власною техніко-технологічною базою для успішного вирішення маркетингових завдань в цифровому середовищі [2]. Цифровізація бізнес-процесів галузевих компаній є важливим фактором підвищення їх конкурентоспроможності протягом останнього десятиліття [2-3]. Можна

сказати, що інфокомунікації - одна з передових галузей з точки зору застосування методів та інструментів цифрового маркетингу, які забезпечують високу лояльність споживачів інфокомунікаційних сервісів і послуг [5].

Література

1. Андреева О.Д., Абрамова А.В. Развитие использования цифрового маркетинга в мировой экономике // Российский внешнеэкономический вестник, 2015. – Т. 2015. – №4. – С. 45-66.
2. Володіна Е.Е., Дев`яткин Е.Е., Пастух С.Ю., Дев'яткіна Е.М., Плоскій А.Ю. Ринковий потенціал інтернету речей // Т-Comm: Телекомунікації та транспорт, 2016. - № 9. - С. 28.
3. Gorodnichev M., Kukharenko A., Kukharenko E., Salutina T. Methods of developing systems based on blockchain / Conference of Open Innovation Association, FRUCT, 2019. – № 24. – С. 613-618.
4. Кухаренко Е.Г. Исследование эволюции маркетинговых концепций в инфокоммуникационном бизнесе // Т-Comm: Телекоммуникации и транспорт, 2015. – Т. 9. – № 9. – С. 72-75.
5. Нікуліна А.І., Кухаренко О.Г. Аналіз лояльності споживачів інфокомунікаційних послуг // Телекомунікації та інформаційні технології, 2014. - Т.1. - № 2. - С. 28-29.