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

IV ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«TELECOMMUNICATION: PROBLEMS AND INNOVATION»

30 травня 2023 року

Збірник тез

м. Київ

IV Всеукраїнська науково-технічна конференція «Telecommunication: problems and innovation». Збірник тез. – К.: ДУТ, 2023. – 248 с.

Збірник містить тези доповідей учасників конференції, представлених на IV Всеукраїнській науково-технічній конференції «Telecommunication: problems and innovation», яка проводилась 30 травня 2023 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

ОСНОВНІ МЕТОДИ ВДОСКОНАЛЕННЯ ВОЛЗ

Забродський Антон Ігорович
Державний університет телекомунікацій
Навчально-науковій інститут телекомунікацій

Вдосконалення лінії ВОЛЗ є одним з питань, яке повстає в телекомунікаційних мережах, які пов'язані з кабельною системою в загалом. Стосовно вдосконалення лінії ВОЛЗ повстає питання вдосконалення не тільки про прийом та передачу сигналу, скільки повстає питання живлення апаратури, яка забезпечує прийом та передачу оптичного зв'язку по оптичному кабелю. Саме електроживлення викликає масу питань, такі як: якщо ми маємо відповідну апаратуру зв'язку, від чого вона буде живитися? Якщо вона живиться від мережі, то чим можна ще живити апаратуру зв'язку, якщо мережевий струм кудись зникає?

Саме на ці питання потрібно вміти відповідати правильно, а тим паче ще й закріплювати практикою. Системи електроживлення (СЕЖ) є однією із складових будь-якого пристрою який працює від електроенергії. Окрім забезпечення живлення апаратури зв'язку, воно ще може використовуватися ще й для наступних цілей: запуск апаратури, перемикання та контроль режиму роботи та використовується ще й для захисту.

Системи живлення діляться на наступні елементи: електронна апаратура, засоби вторинного живлення, системи електроживлення апаратури, джерела вторинного електроживлення та функціональні вузли вторинного живлення електронної апаратури. Кожний з елементів, який входить в систему електроживлення є невід'ємною частиною в роботі апаратури зв'язку і не тільки.

Електронна апаратура – це сукупність радіоелементів, які конструктивно об'єднані між собою та є частиною несучих конструкцій та монтажних з'єднань. Системи електроживлення апаратури – це засоби живлення апаратури, які можуть живити електронну апаратуру, як автономно, так і за рахунок мережі. Системою електроживлення частіше називають мережу живлення 220В з частотою 60 Гц та електростанції, які виробляють електричний струм для живлення. Засоби вторинного живлення та джерела вторинного живлення апаратури – це системи живлення, які не залежать від мережі та здатні самі виробляти струм та живити ним апаратуру. До такого типу систем живлення належать виключно автономні системи живлення, такі як: акумулятори, генератори, батареї. До функціональних вузлів вторинного електроживлення апаратури належать пристрої, які виконують одну або декілька функцій, такі як: випрямлення струму, стабілізація струму, регулювання струму живлення, комутацію сигналів та систем зв'язку в цілому та ін.

Також існує такий вид систем живлення, який називається - системи аварійного живлення. Системи аварійного електроживлення – це системи живлення апаратури, які використовуються лише для того, щоб живити апаратуру, на випадок, якщо будь-які інші системи живлення або вийшли з ладу, або відсутнє живлення від мережі живлення. Як правило, вторинні системи живлення можна використовувати, як і аварійні системи живлення.

Стосовно живлення апаратури від мережі нема жодного сдова. Очевидно, що мережа полягає під собою електростанції та систему що передає струм від електростанції да абоненту.

Будь-яка апаратура працює від мережі. Але, стосовно апаратури зв'язку не тільки повстає питання живлення від мережі, але ще й повстає питання вторинного та аварійного живлення. В більшості випадків зв'язківці як раз і займаються питання стосовно живлення апаратури зв'язку від мережі, від вторинних джерел та від аварійних систем живлення. Більше уваги зв'язківці роблять саме на аварійних системах живлення апаратури. Чому так? Бо завжди є питання стосовно живлення: якщо основне живлення – мережеве живлення зникне, або воно тимчасово пропаде не відомо на який термін, які системи можуть живити апаратуру зв'язку, щоб можна було продовжити якісну передачу зв'язку? Саме тут на допомогу приходять на допомогу такі автономні системи живлення, які можуть використовуватися як і аварійні системи живлення, це: акумулятори, батареї та генератори.

Наприклад в медицині використовують аварійне живлення на випадок аварії на електростанціях або на окремій фазі живлення. Аварійне живлення в медичні використовують для операційних та для підтримки роботи: апаратури штучно дихання, апарати фільтрації крові, апарати підтримки життя пацієнта, холодильники з донорськими матеріалами та апаратура, яка допомагає моніторити стан пацієнта. В супермаркетах використовують аварійне живлення, для підтримки праці холодильників та морозильних камер, щоб продукти, яким потрібна заморока або постійний холод, пропадали та не втрачали свого товарного виду. Без систем аварійного живлення все це було б не можливим та в цілому ускладняло би життя людям, не кажучи про лікарні та лікарів, які там працюють. Також, було б не погано, якби і апаратура зв'язку теж працювала б на аварійній системі живлення на всяк випадок, якщо воно знадобиться.

Більш практичним є застосування генераторів як аварійних систем живлення. Але, навіть якщо генератори є надійними автономними приладами аварійного живлення, є маса недоліків, такі як: постійна потреба в паливі (бензин або дизель) та стрибки напругі під час запуску генератора, або після від'єднання навантаження на генератор (під навантаженням мається на увазі підключена апаратура зв'язку). Також, ще одним мінусом для генераторів є виділення чадного газу та вихлопів, які є шкідливими для організму людини та для довкілля в цілому. Шум від генератора теж є одним з недоліків. Більш безпечним, як система аварійного живлення в цьому випадку є акумулятори. Наприклад військові на випадок відмови роботи мережі та генераторів, як аварійне живлення використовують акумулятори від вантажівок, наприклад акумулятори від вантажівки КрАЗ або КамАЗ. Акумулятори не роблять шкоди людям і довкіллю так, як вони не виділяють вихлопи під час роботи, вони менші за генератори, вони безшумні та прості в монтажу. Є один мінус від акумуляторів – вони постійно потребують заряду та вони не люблять коли їх розряджають повністю. Стосовно розряду до нуля, це може спричинити до того, що електроліт, який знаходиться в акумуляторах може втратити свої властивості накопичувати та віддавати струм. Але як система аварійного живлення, вона є найбільш дешевим, та оптимальним м в використанні і його не треба так часто обслуговувати як генератори.

Література:

1. Каток В.Б., Руденко І.Е., Ранський Є.Г., Однорог П.М. Волоконно-оптичний зв'язок / Під ред. Катка В.Б. – К.: Логос, 2015. – 383 с.: іл.
2. Системи електроживлення електронної апаратури. Конспект лекцій для студентів спеціальності 171 «Електроніка», спеціалізації 8(7).050802 «Електронні системи». - К.: НТУУ "КПІ", 2016. – 180 с.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ ДЛЯ ОПТИМІЗАЦІЇ ВИКОРИСТАННЯ РЕСУРСІВ ОРГАНІЗАЦІЇ

Кошель І.С. студентка, група САДМ-51,
Державний університет телекомунікацій, м. Київ

В сучасному світі найважливішим ресурсом кожної організації є інформація. Часто так відбувається, що особа, що приймає рішення, не володіє повнотою інформації щодо наявних ресурсів навіть власного підприємства. А від своєчасності та повноти такої інформації залежить якість рішення, що приймається. Для збору, представлення, та аналізу такої інформації використовується цілий перелік інформаційних систем та технологій.

Одними з таких систем є CRM-системи, які дозволяють накопичувати та аналізувати інформацію про взаємодію з клієнтами.

Впровадження CRM-систем на підприємствах було досліджено в статті С.П. Юрченко [4], роботі Ю.Ю. Карпенко [1], але постійне вдосконалення існуючих інформаційних систем, зростаюча їх потужність та можливість інтегрування, зумовлює необхідність вивчення аспектів їх впровадження в кожній конкретній галузі.

Принципи використання CRM-систем

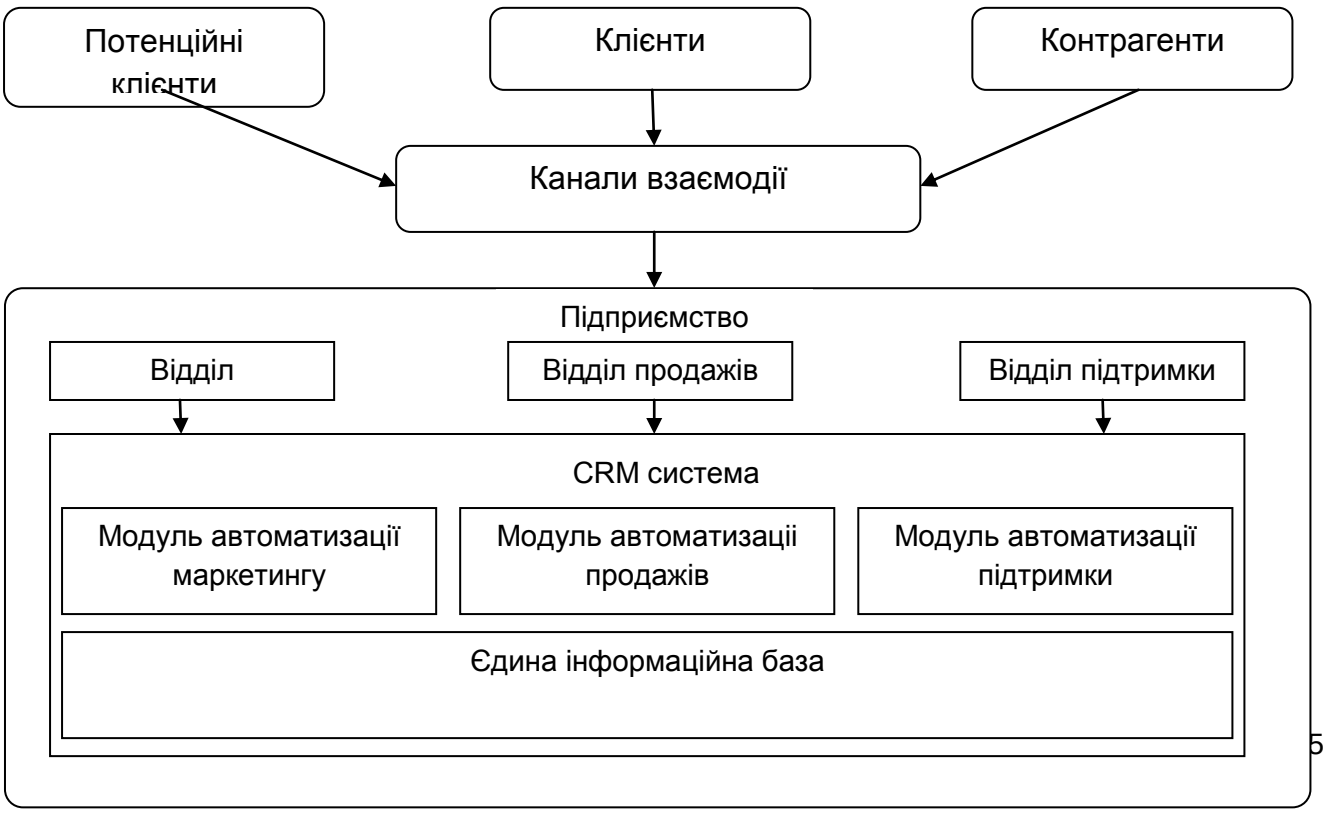
CRM-системи дозволяють автоматизувати та стандартизувати взаємовідносини з клієнтами завдяки наступним механізмам:

- створення та підтримка єдиної бази клієнтів і контрагентів;
- консолідація інформаціїі про роботу відділу продажів, що дозволяє реалізувати його ефективний контроль;
- генерація на підставі зібраної інформації статистичних та аналітичних звітів;

Завдяки отриманим звітам, а також можливості масштабувати отриману інформацію, консолідувати її по різним параметрам, керівник має змогу приймати обгрунтовані рішенння щодо задоволення й утримання клієнтів, оптимізувати діяльність фахівців компанії, скорочуючи витрати пов’язаних ресурсів.

Складові частини CRM-систем

Схему управління взаємодією організації з клієнтами за допомогою CRM-системи надано нижче:



Каналами взаємодії є e-mail, телефон, месенджери, безпосередньє спілкування, сайт компанії.

Ядром CRM-системи є база даних, яка зберігає всю власну інформацію, а також інтегрується з усіма іншими корпоративними інформаційними системами.

Крім перелічених компонентів CRM-система може містити безліч інших модулів, серед яких:

- модуль, що містить календар, управління завданнями, модулі сполучення з e-mail та іншими засобами зв'язку;
- модуль інтеграції з call-центром що веде статистику звернень, стандартні запитання та інш;
- модуль управління взаємовідносинами з партнерами;
- модуль, відповідаючий за веб-частину CRM, в нього можуть входити веб-сайт компанії, інтернет-магазин, B2B майданчик, взаємодія з клієнтами через Інтернет;
- модуль бізнес-аналітики;
- модуль інтеграції з іншими корпоративними системами.

Оператори CRM-систем

Як можна бачити з вище наведеного, CRM-система являє собою досить складну інформаційну систему, що потребує певної кваліфікації особи яка з нею працює. Найкраще, щоб це була окремо виділена людина – CRM-менеджер.

Одна з його основних функцій - це повне управління базою даних клієнтів. На основі отриманих статистичних звітів він розробляє та контролює маркетингові акції, які відповідають цілям організації.

Крім цього він працює і безпосередньо з клієнтами. Для залучення й утримання клієнта, необхідна одночасна й злагоджена робота декількох підрозділів. Не достатньо просто вигадати маркетингову акцію, важливо й правильно її провести. Після проведення необхідно оцінити ефективність, співвіднести витрати та результати, врахувати помилки.

Висновки

Розробка універсальної моделі управління організацією неможлива по причині його складності та слабої структурованості. Проте, можливе значне підвищення ефективності цих процесів завдяки застосуванню інформаційних систем та технологій збору та обробки інформації.

На прикладі використання CRM-системи взаємодії з клієнтами ми мали змогу побачити наскільки таке використання покращує отримання та обробку інформації про продажі. Якщо ж таку систему інтегрувати з іншими системами організації – фінансовою, кадровою, складською, юридичною, та інш., - керівництво отримує потужні інструменти для оптимізації власних бізнес-процесів майже з безмежними можливостями.

Список використаної літератури

1. Білоусько Т.М., Карпенко Ю.Ю. Інформаційні системи та технології як забезечення системи управління взаємовідносинами банку з клієнтами – Інститут економіки, управління та інформаційних технологій. - Полтава: ПУЕТ,2019
2. Пономаренко О. І. Системні методи в економіці, менеджменті та бізнесі – К. : Либідь, 2015. – 240 с.
3. Ушакова, Г. О. Плеханова. Інформаційні системи та технології на підприємстві : конспект лекцій – Харків : Вид. ХНЕУ, 2009. – 128 с
4. Юрченко С. П. CRM инструмент повышения эффективности работы предприятия / С. П. Юрченко // Проблемы развития территории. – 2006. – № 3. – С. 53–60.

ОСОБЛИВОСТІ IPV6 АДРЕСАЦІЇ

Миронова Т.І., здобувачка вищої освіти,
Державний університет телекомунікацій,
м. Київ

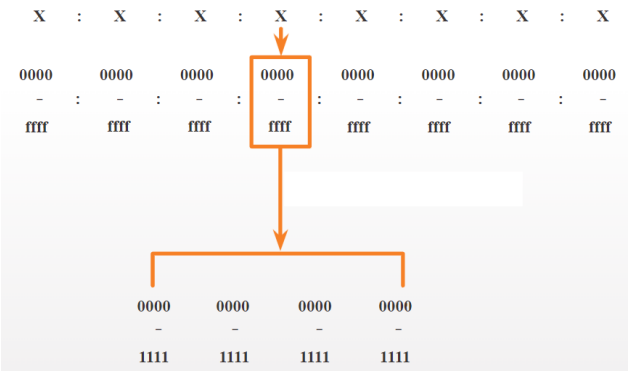
Вичерпання адресного простору IPv4 — основний стимулюючий чинник переходу до використання IPv6. З подальший збільшенням кількості користувачів Інтернет залишається все менше вільних IPv4-адрес. Протокол IPv6 було розроблено як наступник протоколу IPv4. IPv6 має більший 128-бітний адресний простір, що достатньо для 340 адрес. Однак протокол IPv6 також містить додаткові покращення. Серед таких покращень - протокол керуючих повідомлень версії 6 (ICMPv6), який включає дозвіл адрес і автоналаштування адрес.

Теоретична максимальна кількість IPv4-адрес – 4,3 мільярда. Приватні адреси разом із механізмом перетворення мережевих адрес (NAT) дозволяли якийсь час уповільнити процес виснаження адресного простору IPv4. Однак механізм перетворення мережевих адрес (NAT) має певні обмеження, що погіршують комунікації в одноранговій мережі.

Зі збільшенням числа мобільних пристроїв мобільні провайдери почали перехід на IPv6. Два найбільші провайдери мобільного зв'язку в США повідомляють, що IPv6 складає понад 90% їхнього трафіку. Більшість провідних інтернет-провайдерів та контент-провайдерів, таких як YouTube, Facebook та NetFlix, також зробили перехід.

Сучасний Інтернет суттєво відрізняється від Інтернету минулих десятиліть. Сьогодні це не просто електронна пошта, веб-сторінки та передача файлів між комп'ютерами. З розвитком Інтернет стає Інтернетом речей. Практично всі пристрої — від автомобілів та біомедичного обладнання до побутової техніки та природної екосистеми можуть бути оснащені сенсорами та підключені до Інтернету. У зв'язку з цим виросла потреба в IP-адресах і перехід на IPv6 стає більш актуальним.

Довжина IPv6-адрес становить 128 біт, написаних у вигляді рядка шістнадцяткових значень. Кожні 4 біти представлені однією шістнадцятковою цифрою, причому загальна кількість шістнадцяткових значень дорівнює 32, як показано на малюнку 1. IPv6-адреси нечутливі до регістру, їх можна записувати як малими, так і великими літерами.



Малюнок 1. Адреса IPv6

Написання IP-адрес можна спростити. Нулі на початку групи можна не писати. Декілька груп нулів можна замінити на ::, але не більше 1 разу на адресу.

Існує три категорії адрес IPv6:

Індивідуальний (або одноадресне розсилання, unicast) : служить для однозначного визначення інтерфейсу на пристрої під керуванням протоколу IPv6.

Груповий (або адреса багатоадресної розсилки): використовується для надсилання одного IPv6-пакета на кілька адрес призначення.

Довільний (або адреса довільної розсилки): будь-яка індивідуальна IPv6-адреса, яка може бути призначена кільком пристроям. Пакет, що надсилається на адресу довільної розсилки, надсилається до найближчого пристрою з цією адресою.

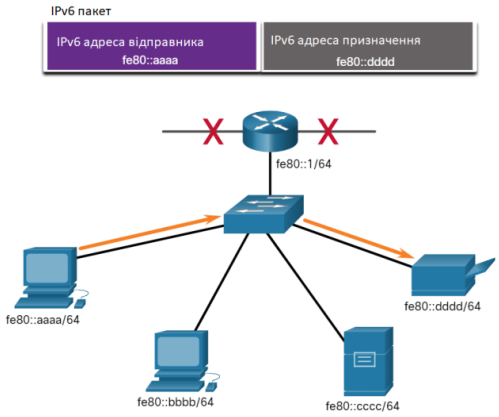
На відміну від IPv4, IPv6 не використовує широкомовну адресу. Однак є групова IPv6-адреса для всіх вузлів, яка дає аналогічний результат.

IPv6 не використовує для маски підмережі десяткове уявлення з роздільними точками. Як і IPv4, довжина префікса представлена у вигляді косої межі та використовується для вказівки мережної частини адреси IPv6. Діапазон довжини префікса може становити від 0 до 128. Звичайна довжина префікса IPv6 для локальних мереж та більшості інших типів мереж /64, як показано на малюнку 2.

Малюнок 2. Структура IPv6 адреси.

Локальна IPv6-адреса каналу дозволяє пристрою обмінюватися даними з іншими пристроями з увімкненим протоколом IPv6 в тому ж каналі (підмережі) і тільки в ньому. Пакети з локальною адресою каналу джерела або призначення не можуть бути надіслані за межі каналу, в якому створюється пакет. Кожен інтерфейс мережі з підтримкою IPv6 повинен мати LLA. Якщо локальна адреса каналу не налаштована вручну на інтерфейсі, пристрій автоматично створює її самостійно. Це дозволяє пристроям під керуванням IPv6 обмінюватися даними з іншими пристроями під керуванням IPv6 в одній підмережі, у тому числі зі стандартним шлюзом (маршрутизатором).

На малюнку 3. наводиться приклад здійснення зв'язку за допомогою групових адрес для всіх вузлів.



Малюнок 3. IPv6 LLA

IPv6 LLA знаходяться в діапазоні fe80::/10. /10 вказує, що перші 10 бітів - 1111 1110 10xx xxxx. Діапазон значень першого гекстету: від 1111 1110 1000 0000 (fe80) до 1111 1110 1011 1111 (febf).

Список використаних джерел:

1. cisco.com
2. Karen Webb. Building Cisco Multilayer Switched Networks. Cisco Systems; First Edition
3. CCNP Enterprise Advanced Routing ENARSI 300-410 official cert guide. Cisco Systems, 2020

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ МЕРЕЖІ VANET

Бацак Артем Олексійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Мережа автономних транспортних засобів (VANET) є бездротовою мережею, що з'єднує транспортні засоби та інфраструктуру на дорозі з метою обміну інформацією. VANET вирішує ряд завдань, таких як покращення безпеки на дорозі, підвищення ефективності руху транспорту та надання різноманітних послуг для водіїв і пасажирів.

Однією з основних особливостей функціонування VANET є його динамічність. Транспортні засоби постійно змінюють своє положення, швидкість та напрямок руху, що створює постійно змінну мережу. Це вимагає розробки ефективних протоколів маршрутизації та керування ресурсами для забезпечення надійного зв'язку між транспортними засобами.

Ще одною важливою особливістю VANET є його високі вимоги до затримки та надійності зв'язку. Зважаючи на безпекові аспекти, інформація про дорожні умови, аварії та інші події повинна передаватись майже в реальному часі. Тому протоколи комунікації в VANET повинні бути швидкими та надійними, здатними впоратись з високим рівнем рухомості та змінюваними умовами зв'язку.

VANET також стикається з проблемою обмежених ресурсів. Транспортні засоби можуть мати обмежену потужність передавачів та обмежену пропускну здатність каналів зв'язку. Крім того, доступ до спільного радіоспектра може бути обмеженим через конкуренцію між різними транспортними засобами та іншими бездротовими пристроями.

Безпека є ключовою складовою VANET. Мережа використовується для обміну інформацією про дорожні небезпеки, такі як аварії, перешкоди на дорозі та інші небезпеки, а також для виявлення неправильних дій та зловживань. Розробка механізмів аутентифікації,

шифрування та контролю доступу є критично важливою для забезпечення безпеки та запобігання зловживанням.

BANET використовує різноманітні технології комунікації, такі як Wi-Fi, DSRC (Dedicated Short-Range Communications), LTE (Long-Term Evolution) та інші. Ці технології дозволяють транспортним засобам та інфраструктурі на дорозі обмінюватись даними, спілкуватись та координуватись для досягнення спільних цілей, таких як запобігання зіткненням та покращення потоку транспорту.

Отже, VANET є складною інфраструктурою, яка поєднує транспортні засоби, інфраструктуру на дорозі та різноманітні сервіси. Ця мережа має великий потенціал у поліпшенні безпеки на дорозі та наданні нових послуг для автомобілістів. Проте, вона стикається з численними викликами, такими як динамічність, затримка, надійність та безпека, які потребують дальшого дослідження та розробки.

Список використаних джерел:

1. https://www.sciencedirect.com/topics/computer-science/vehicular-ad-hoc-network

НЕБЕЗПЕКА ВИКОРИСТАННЯ ХМАРНИХ МЕНЕДЖЕРІВ ПАРОЛІВ В КОМПАНІЯХ

Адаменко О.О.
Київський національний університет будівництва і архітектури
м. Київ, Україна

Все більше роботи ми виконуємо в так званій Хмарі, тобто використовуємо сервіси, що не знаходяться на нашому пристрої, ми це робимо як в персональних так і в робочих цілях. Крім того кожен з нас так чи інакше користується різними сайтами, деякі з яких вимагають від користувача наявності власного облікового запису.

Оскільки дуже велику кількість роботи користувач, або працівник виконує не локально на своєму пристрої, а, фактично, робить це віддалено, персональні або корпоративні дані постійно відправляються в мережу.

Задля захисту персональних чутливих даних в мережі застосовується багато різних методів: SSL/TLS протоколи, двофакторна аутентифікація, шифрування внутрішніх даних в місці їх тривалого зберігання, паролі та інші. Паролі, багато паролів, вони стали невід'ємною частиною нашого життя. Майже кожен сервіс вимагає від вас облікового запису, або підключення стороннього сервісу з обліковим записом як Google, або Facebook, до яких ви також маєте пам'ятати пароль.

Як більшість знає, та і кожен сервіс повідомляє вам – пароль має бути складним, не логічним, мати різноманітні символи та ні з чим не асоціюватись. Як на мене найкращий кандидат на цю роль - це ХЕШ. Унікальний та неповторний хеш як ніщо інше підходить на цю роль, але в цьому і є проблема – його дуже складно запам'ятати, тим більше коли кожен ваш пароль це хеш.

Задля вирішення цього питання вже досить давно існують менеджери паролів. Існують версії цих застосунків, що встановлюються на ваш пристрій, та взагалі не потребують виходу у мережу, але ж трапляється, що вам можуть знадобитись ваші дані поза домом. При такому сценарії використання менеджеру паролів в хмарі значно зручніше, адже ви можете працювати за ПК, а після цього змінити пристрій і не втратити доступ до свої даних. Для такого сценарію зазвичай використовується один, або декілька ключів шифрування, що і є вашими паролями, їх значно легше запам'ятати ніж всі ті дані, що вони приховують.

Але якщо, наприклад, ви працюєте в команді з групою людей та кожен з вас повинен мати доступ до певних спільних ресурсів чи облікових записів? Для сучасних менеджерів паролів – це не проблема, вони надають вам великий спектр можливостей: можливість

поділитися даними, створити спільне сховище, налаштувати групову політику та багато іншого.

Це дійсно дуже зручно, дозволяє оптимізувати роботу команди, або навіть цілої компанії. Але якщо розглянути це під іншим кутом: уявімо, що ви та ще один працівник мають облікові записи в якомусь хмарному менеджері паролів, хтось з вас створює спільне сховище, але жоден з вас не надає іншому дані для входу, всі подібні сервіси дають вам змогу використовувати власні дані для входу. З однієї сторони це добре, жоден з вас не ділиться власними даними, а отже це безпечно. З іншої сторони, тоді принаймні дані для входу у зазначене спільне сховище не є його ключами шифрування. І виникає питання – де ж вони?

В цьому питанні і полягає вся небезпека – ніхто цього не знає, або майже ніхто. Деякі з подібних сервісів дають вам змогу розгорнути таку ж систему на власному сервері, але далеко не всі. Що це означає для компаній, що користуються хмарними менеджерами паролів не розгортаючи його на власних серверах? Вони не можуть бути впевненими, що їх облікові дані та дані їх працівників, або клієнтів повністю захищені, якщо вони навіть і не шифруються.

Описана вище ситуація не є спробою когось залякати, або звинуватити, просто не завжди «зручніше» означає «краще», особливо коли мова йде про безпеку. Прикладом може бути сервіс LastPass. Певний час він був найпопулярнішим подібним сервісом, але при цьому був зламаний двічі за 6 місяців [1].

Серед шляхів вирішення цієї проблеми є наступні:

1. Використовувати сервіси, що дають змогу розгорнути свою систему локально та самостійно контролювати її.
2. Написати власний. Так, дуже очевидно, але це несе за собою велику кількість переваг. Для великої компанії буде не складно виділити ресурси на розробку подібного сервісу, враховуючи, що не обов’язково реалізовувати абсолютно весь функціонал існуючих аналогів, адже, можливо, вам вистачить базового набору функцій з урахуванням специфіки роботи саме вашої компанії. Основною перевагою цього рішення є те, що новостворена система, нехай не принципово, але буде відрізнятись від її аналогів, що ускладнить можливості її зламу. Адже зламати щось невідоме та до цього не бачене значно складніше, тим більше зловмисник навряд чи зможе навіть дізнатись, що ця система існує.

Література

1. LastPass Hacked for the Second Time in Six Months. URL: https://gizmodo.com/lastpass-hacked-again-second-time-six-months-1849841863

АКТУАЛЬНІСТЬ МЕРЕЖ 3G ТА ДОЦІЛЬНІСТЬ ЇХ ВИКОРИСТАННЯ В УКРАЇНІ

Самойленко Євген Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

3G (або третє покоління) є стандартом мобільного зв'язку, який використовується для передачі голосу та даних у бездротових мережах зв'язку. Він є наступником 2G (другого покоління) і покращує швидкість передачі даних та якість голосового зв'язку.

3G відкриває широкий спектр можливостей для мобільних користувачів, включаючи доступ до мобільного Інтернету, передачу повідомлень, відеодзвінків та інших передових послуг. Він підтримує високі швидкості передачі даних, забезпечуючи швидкий доступ до Інтернету, завантаження файлів, стрімінг відео і використання інших онлайн-сервісів.

Основні характеристики 3G включають:

1. Швидкість передачі даних: Типові швидкості в 3G мережах можуть досягати до 2 Мбіт/с для завантаження та 384 Кбіт/с для відвантаження. Однак, швидкість може варіюватися в залежності від покриття мережі та навантаження.

2. Висока якість голосового зв'язку: 3G покращує якість голосового зв'язку порівняно з попередніми поколіннями, забезпечуючи чітке та стабільне з'єднання під час голосових дзвінків.

3. Підтримка додаткових послуг: 3G дозволяє використовувати різноманітні додаткові послуги, такі як мобільний інтернет, повідомлення, відеодзвінки, відеострімінг, GPS-навігація та інші.

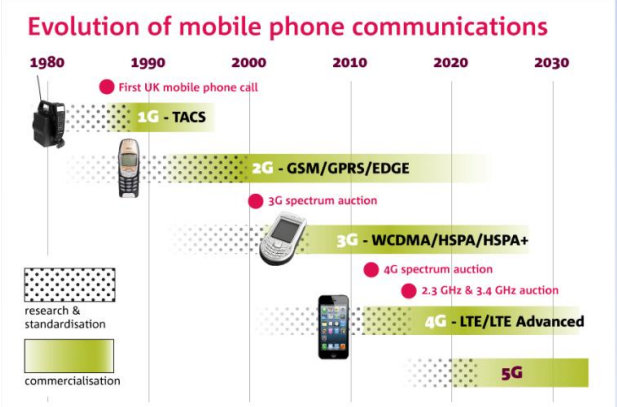
Станом на сьогодні , мережі 3G (третього покоління) використовуються в Україні, але їх актуальність знижується в контексті швидкого розвитку мереж 4G (LTE) та 5G.

У зв'язку з цим, українські оператори зв'язку активно розгортають мережі 4G (LTE) та впроваджують мережі 5G, які надають значно більшу швидкість передачі даних, покращені характеристики для мобільного Інтернету, мультимедійних послуг, Інтернету речей та інших інноваційних рішень.

		Real World (avg)		Theoretical (max)	
		Download	Upload	Download	Upload
2.5G	GPRS	32-48Kbps	15Kbps	114Kbps	20Kbps
2.75G	EDGE	175Kbps	30Kbps	384Kbps	60Kbps
3G	UMTS	226Kbps	30Kbps	384Kbps	64Kbps
	W-CDMA	800Kbps	60Kbps	2Mbps	153Kbps
	EV-DO Rev. A	1Mbps	500Kbps	3.1Mbps	1.8Mbps
	HSPA 3.6	650Kbps	260Kbps	3.6Mbps	348Kbps
	HSPA 7.2	1.4Mbps	700Kbps	7.2Mbps	2Mbps
Pre-4G	WiMAX	3-6Mbps	1Mbps	100Mbps+	56Mbps
	LTE	5-12Mbps	2-5Mbps	100Mbps+	50Mbps
	HSPA+	-	-	56Mbps	22Mbps
	HSPA 14	2Mbps	700Kbps	14Mbps	5.7Mbps
4G	WiMAX 2 (802.16m)	-	-	100Mbps mobile / 1Gbps fixed	60Mbps
	LTE Advanced	-	-	100Mbps mobile / 1Gbps fixed	-

	1G	2G	3G	4G	5G
Period	1980 – 1990	1990 – 2000	2000 – 2010	2010 – (2020)	(2020 - 2030)
Bandwidth	150/900MHz	900MHz	100MHz	100MHz	1000x BW pr unit area
Frequency	Analog signal (30 KHz)	1.8GHz (digital)	1.6 – 2.0 GHz	2 – 8 GHz	3 – 300 GHz
Data rate	2kbps	64kbps	144kbps – 2Mbps	100Mbps – 1Gbps	1Gbps <
Characteristic	First wireless communication	Digital	Digital broadband, increased speed	High speed, all IP	
Technology	Analog cellular	Digital cellular (GSM)	CDMA, UMTS, EDGE	LTE, WiFi	WWWW

На даних слайдах показано основні відмінності та порівняльні характеристики від минулих технологій до сьогодні .



На цьому слайді ми можемо побачити еволюцію підтримки різних поколінь технологій , мобільними пристроями .

Отже підсумовуючи наявні факти ми можемо підкреслити що використання технології 3G на сьогоднішній день може бути не зовсім доцільним на території України, через впровадження більш новіших та більш кращих за своїми технічними параметрами технологій підтримки мереж таких як 4G (LTE) та 5G .

МЕТОДИ ВИЯВЛЕННЯ DDOS АТАК В МЕРЕЖАХ SDN

Анніков Євген Сергійович
Державний університет телекомунікацій

Зв'язок між **DDoS-атаками** (розподілені атаки зі збоєм обслуговування) та мережами SDN (мережі з програмним керуванням) є важливою темою в сфері кібербезпеки та мережевих технологій. DDoS-атаки вважаються одними з найпоширеніших і серйозних загроз, що спрямовані на мережеву інфраструктуру. SDN - це парадигма мережевого проектування, в якій централізований контролер керує функціями комутаторів та маршрутизаторів. Ця архітектура надає гнучкість, забезпечує централізований контроль та програмну керованість мережі. Однак, вона також вносить нові виклики та вразливості з точки зору кібербезпеки, включаючи потенційну схильність до DDoS-атак. DDoS-атаки використовуються для перевантаження мережевих ресурсів, що призводить до збоїв обслуговування для легітимних користувачів та систем. У традиційних мережах це може означати перевантаження мережевих комутаторів, маршрутизаторів або серверів. Однак, у мережах SDN, де всі комутатори підконтрольовані централізованою системою, DDoS-атаки можуть мати ще більший вплив, спричиняючи проблеми зі збоєм обслуговування в самому контролері, що може призвести до відмови всієї мережі. З огляду на це, розробка ефективних методів виявлення DDoS-атак в мережах SDN стає критичною задачею.

Виявлення DDoS-атак має на меті раннє виявлення аномалій, патернів трафіку та відхилень від звичайної поведінки, що свідчать про наявність атаки. Це дозволяє операторам мережі прийняти відповідні заходи для мітигації атаки та забезпечити нормальне функціонування мережі. Методи виявлення DDoS-атак в мережах SDN можуть включати моніторинг мережевого трафіку, аналіз поведінки, виявлення змін в мережевій топології, детекцію аномальних пакетів, аналіз споживання ресурсів та застосування політик безпеки.

Використання комбінації цих методів може забезпечити більш ефективне виявлення та мітигацію DDoS-атак в мережах SDN. Розуміння особливостей та використання ефективних методів виявлення DDoS-атак в мережах SDN є важливим для забезпечення кібербезпеки мережевої інфраструктури. Належне виявлення та реагування на DDoS-атаки може допомогти зберегти доступність та надійність мережі, а також забезпечити безперебійне функціонування бізнес-систем та послуг.

Виявлення DDoS-атак в мережах SDN може включати в себе різноманітні методи та стратегії. Ось деякі з них:

1. **Моніторинг мережевого трафіку**: Важливо збирати дані про мережевий трафік, включаючи інформацію про вихідний та приймальний IP-адреси, порти, протоколи та обсяги передачі даних. Моніторинг трафіку допомагає виявити аномальну або високу активність, яка може бути ознакою DDoS-атаки.

2. **Аналіз поведінки**: Відстеження звичайних моделей поведінки мережі та виявлення відхилень може свідчити про наявність DDoS-атаки. Аналітичні методи, такі як машинне навчання або статистичні алгоритми, можуть використовуватися для ідентифікації аномальних патернів трафіку.

3. **Виявлення змін в мережевій топології**: DDoS-атаки можуть спричиняти зміни в мережевій топології, такі як збільшення або зменшення обсягу трафіку на певних сегментах

мережі. Використання систем моніторингу та аналізу топології може допомогти виявити такі зміни та спостерігати за великими змінами в мережевих параметрах.

4. **Детекція аномальних пакетів**: DDoS-атаки часто супроводжуються надмірним відправленням пакетів до цільових хостів або використанням пакетів з аномальними характеристиками. Використання алгоритмів фільтрації та аналізу пакетів може допомогти виявити ці аномалії.

5. **Аналіз споживання ресурсів**: DDoS-атаки можуть спричиняти значний спад продуктивності мережі або використовувати велику кількість ресурсів, таких як пропускна здатність або оброблювальна потужність комутаторів. Вимірювання та моніторинг споживання ресурсів можуть виявити незвичайні показники та свідчити про DDoS-атаку.

6. **Захист на основі політик**: Встановлення мережевих політик для фільтрації, перенаправлення або блокування трафіку може бути ефективним методом виявлення та мітигації DDoS-атак в мережах SDN. Застосування правил фільтрації на контролері або комутаторах може допомогти ідентифікувати та обмежувати шкідливий трафік.

Виявлення DDoS-атак в мережах SDN вимагає комбінації технологій, аналітики даних та мережевих стратегій. Ефективна система виявлення повинна бути здатна реагувати швидко та автоматично на DDoS-атаки, мінімізуючи вплив на продуктивність та надійність мережі.

РОЗРОБКА МЕТОДІВ ЗМЕНШЕННЯ ЕНЕРГОСПОЖИВАННЯ ТА ВПЛИВУ НА ДОВКІЛЛЯ В МЕРЕЖАХ 5G

Коцюба Михайло Валерійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

З розширенням використання мереж п'ятої генерації (5G) виникає потреба у зменшенні енергоспоживання та впливу на довкілля. Забезпечення енергоефективності в мережах 5G є важливим завданням, оскільки ці мережі характеризуються великим обсягом даних, високою швидкістю передачі та масштабуванням. Дослідження енергоефективності та розробка методів зменшення енергоспоживання є необхідними для забезпечення стійкого та екологічно чистого розвитку мереж 5G.

Мережі 5G потребують значної кількості енергії для забезпечення високої швидкості передачі даних, обробки великого обсягу інформації та підтримки безперервного з'єднання. Однак, це призводить до значного енергоспоживання та негативного впливу на довкілля. Проблеми, пов'язані з енергоспоживанням, включають високі витрати на енергію, недостатню тривалість роботи батарей, енергетичну неефективність та збільшення викидів парникових газів. Тому необхідно розробляти методи та стратегії для зменшення енергоспоживання та впливу на довкілля в мережах 5G.

Розробка методів зменшення енергоспоживання в мережах 5G включає в себе кілька аспектів. Перш за все, оптимізація ресурсного використання та розподілу трафіку може забезпечити більш ефективне використання доступних ресурсів та зменшення енергоспоживання. Протоколи ресурсного керування, такі як Power Saving Mode (PSM) та Discontinuous Reception (DRX), можуть використовуватися для регулювання режимів споживання енергії підключеними пристроями та зниження їх енергетичного споживання. Крім того, розробка енергоефективних алгоритмів та протоколів передачі даних, таких як Energy-Efficient Routing Protocol (EERP) та Sleep Scheduling Protocol (SSP), може забезпечити оптимальне використання ресурсів та зниження енергоспоживання в мережах 5G.

Розробка методів для зменшення енергоспоживання в мережах 5G також враховує екологічні аспекти та вплив на довкілля. Використання енергоефективних технологій та протоколів може знизити викиди парникових газів та сприяти стійкому розвитку. Додатково, розробка алгоритмів та стратегій для впровадження відновлюваних джерел енергії в мережі 5G може сприяти зменшенню використання енергії, що походить зі шкідливих джерел.

Врахування енергоефективності в процесі оптимізації ресурсного використання в мережах 5G є необхідним для забезпечення стійкого розвитку та зменшення впливу на довкілля. Розробка методів зменшення енергоспоживання та використання енергоефективних технологій та протоколів відіграють важливу роль у досягненні цієї мети. Дослідження у цій області сприятимуть розвитку стійких та екологічно чистих мереж 5G, що забезпечуватимуть ефективне використання ресурсів та мінімальний вплив на довкілля.

Список літератури:

1. Bockarjova, M., & Sokolovska, N. (2020). Energy Efficiency in 5G Networks: Challenges and Solutions. Proceedings of the International Scientific Conference on Sustainable Economy and Entrepreneurship (ICSEE).
2. Li, J., Li, J., Liang, Q., Cheng, X., & Chen, L. (2018). A Survey on Edge Computing Systems. Proceedings of the IEEE/ACM Symposium on Edge Computing (SEC).
3. Zhang, M., Wang, Q., Hu, H., Liu, J., & Xiong, N. (2019). Edge Computing for Internet of Things: A Survey. IEEE Internet of Things Journal, 6(3), 5882-5899.

МЕТОДИКА ПОБУДОВИ IPSEC VPN ТУНЕЛІВ

Бондаренко Данило Андрійович,
Державний університет телекомунікацій

Постановка задачі. Оскільки все більше людей отримують доступ до мережі Інтернет, гостро порушується питання з приводу безпеки всередині самої мережі. IP-безпека (IPSec) дозволяє забезпечувати захист внутрішніх мереж, а також створювати безпечні рішення на базі віртуальної приватної мережі для зв'язку через зовнішні мережі (Інтернет). Технологія IPSec була розроблена групою IETF (Internet Engineering Task Force) і є галузевим стандартом шифрування трафіку TCP/IP.

Мета дослідження. Увага буде зосереджена на організації захисту між мережами засобами IPsec.

Результати дослідження. Для незалежності від прикладних протоколів та додатків захищені віртуальні мережі формуються на одному з більш низьких рівнів моделі OSI - канальному, мереженому чи сеансовому. Канальному (другому) рівню відповідають такі протоколи реалізації VPN, як PPTP, L2F и L2TP, мереженому (третьому) рівню – IPSec, SKIP, а сеансовому (п’ятому) рівню – SSL/TLS та SOCKS. Отже, IPSec працює на мережному рівні стека TCP/IP і, таким чином, він є прозорим для додатків, завдяки чому безпеку за допомогою IPSec можна забезпечувати в багатьох різних середовищах без необхідності зміни додатків.

Протокол IPSec застосовується головним чином в рішеннях VPN (Virtual Privat Network) в двох областях: для організації захищених з’єднань між офісами (філіями); для захисту віддаленого доступу користувачів. У разі VPN між офісами, трафік між двома локальними мережами проходить через міжмережеві екрани (Firewall), маршрутизатори чи крипто-шлюзи з підтримкою IPSec з обох боків з’єднання. Шлюз шифрує пакети IP і відправляє їх через загальнодоступну мережу далі до шлюзу призначення, де ті розшифровуються і

аутентифікуються. У разі віддаленого доступу шифрування і подальшу передачу пакетів бере на себе клієнтська програма на віддаленій робочій станції.

Створення захищеного тунелю виконують компоненти віртуальної мережі, що функціонують на вузлах, між якими формується тунель. Ці компоненти прийнято називати ініціатором та термінатором тунелю. Ініціатор тунелю інкапсулює (вбудовує) пакети в новий пакет, що містить разом з початковими даними новий заголовок з інформацією про відправника і одержувача. Хоча всі пакети, які передаються по тунелю, є пакетами IP, пакети, що інкапсулюються, можуть належати до протоколу будь-якого типу, включаючи пакети протоколів, які не маршрутизуються, наприклад, NetBEUI. Маршрут між ініціатором і термінатором тунелю визначає звичайна мережа IP, яка може бути і мережею, відмінною від Internet. Термінатор тунелю виконує процес, зворотній інкапсуляції, - він виділяє нові заголовки і направляє кожний початковий пакет в локальний стек протоколів або адресату в локальній мережі. Сама по собі інкапсуляція ніяк не впливає на захищеність пакетів повідомлень, які передаються по тунелю VPN. Але завдяки інкапсуляції з'являється можливість повного криптографічного захисту пакетів, що інкапсулюються. Конфіденційність пакетів, що інкапсулюються, забезпечується шляхом їх криптографічного закриття, тобто шифрування, а цілісність і автентичність – шляхом формування цифрового підпису. Оскільки існує безліч методів криптозахисту даних, дуже важливе, щоб ініціатор і термінатор тунелю використовували одні і ті ж методи та могли погоджувати один з одним цю інформацію. Крім того, для можливості розшифрування даних і перевірки цифрового підпису при прийомі, ініціатор і термінатор тунелю повинні підтримувати функції безпечного обміну ключами. Щоб тунелі VPN створювалися тільки між уповноваженими користувачами, кінцеві сторони взаємодії необхідно автентифікувати. Таким чином, протокол IPSec забезпечує конфіденційність, цілісність і автентифікацію джерела даних. Для роботи IPSec повинні бути відкриті такі IP порти: порт 50 для протоколу ESP (шифрування пакетів); порт 51 для протоколу AH (цифровий підпис пакетів); порт 500 для протоколу ISAKMP/Oakley (встановлення безпечних з'єднань).

Існує два режими, в яких можна застосовувати IPSec для роботи в мережі, які називаються Транспортним режимом і Тунельним режимом. Транспортний режим дозволяє взаємодіяти двом або більше системам, використовуючи IPSec із з'єднанням на вимогу, як встановлює політика, яка була заздалегідь створена. Наприклад, можна визначити, що, коли комп'ютер із підмережі M1 намагається взаємодіяти з сервером C1, то весь трафік повинен бути зашифрований і захищений підписом. Або можна визначити, що коли комп'ютер отримує доступ до бази даних, всі взаємодії повинні бути тільки захищені підписом.

Висновки та перспективи. Таким чином, розгортання протоколу IPSec дозволяє забезпечити високий рівень безпеки усієї мережі. При використанні IPSec, на серверах та клієнтах IPSec, захист здійснюється автоматично для усіх додатків.

Список використаних джерел

1. www.juniper.net [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – [Основи IPsec]. – Режим доступа: https://www.juniper.net/documentation/ru/ru/software/junos/vpn-ipsec/topics/topic-map/security-ipsec-basics.html – Назва з екрана.
2. Bollapragada V. IPSec VPN Design / V. Bollapragada, M. Khalid, S. Wainner., 2005. – 384 c. – (Cisco Press). – (Networking Technology).

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ІНФОКОМУНІКАЦІЙНИХ СИСТЕМ НА ОСНОВІ ВИКОРИСТАННЯ МЕТОДІВ ТА ЗАСОБІВ РОЗПІЗНАВАННЯ МОВИ

Венгльовський Я. В.
Державний університет телекомунікацій

Розпізнавання мови у голосових інтерфейсах є актуальною та перспективною галуззю досліджень в сфері інформаційних технологій. Цей процес включає аналіз та інтерпретацію вимовленого мовлення з метою розуміння змісту та намірів користувача. Використання методів та засобів розпізнавання мови дозволяє покращити ефективність та зручність взаємодії між людиною та комп'ютерною системою.

Один з основних аспектів розпізнавання мови у голосових інтерфейсах - це процес перетворення звукових сигналів, що виникають під час мовлення, на текстову форму. Це досягається за допомогою ряду алгоритмів та методів, які базуються на статистичних моделях, машинному навчанні та глибинному навчанні.

- Ефективне розпізнавання мови вимагає детального дослідження та розуміння акустичних, фонетичних та синтаксичних аспектів мови. Розробка таких систем вимагає значних обсягів даних для навчання та налаштування моделей розпізнавання мови.

- Застосування розпізнавання мови у голосових інтерфейсах розширює можливості взаємодії між людиною та комп'ютерною системою. Він дозволяє користувачам взаємодіяти з пристроями та програмним забезпеченням за допомогою голосових команд та розуміти їх. Це забезпечує більш зручну форму взаємодії, особливо у випадках, коли інші методи введення даних є незручними або неможливими.

- Завдяки розпізнаванню мови у голосових інтерфейсах можлива реалізація широкого спектру систем управління, включаючи голосові помічники, системи управління та навігації автомобілем, системи домашнього автоматизування та багато інших. Використання методів та засобів розпізнавання мови сприяє покращенню ефективності, зручності та доступності інфокомунікаційних систем, роблячи їх більш інтуїтивно зрозумілими та ефективними для користувачів.

Статистичні методи розпізнавання мовлення є важливими інструментами в розпізнаванні мови і використовуються для моделювання та аналізу різних мовних характеристик і властивостей. Вони базуються на статистичних моделях та алгоритмах, які використовують імовірностні методи для визначення найбільш ймовірного розпізнаного тексту.

Один з популярних статистичних методів у розпізнаванні мови - це модель марківських ланцюгів (HMM). HMM використовується для моделювання послідовності акустичних властивостей мовлення та розпізнавання їх у текстову форму.

Інший статистичний метод - це модель на основі гаусових сум (GMM). GMM використовується для моделювання розподілу акустичних характеристик, таких як мел-частотні кепстральні коефіцієнти (MFCC), в різних фонетичних класах або звуках. GMM використовується для порівняння акустичних характеристик вхідного сигналу з моделями різних фонем або слів.

- Статистичні методи також можуть використовуватися у поєднанні з лінгвістичними моделями, що враховують граматичні та семантичні властивості мовлення, для покращення точності розпізнавання мови. Наприклад, можуть бути використані статистичні моделі, такі як модель n-грамів, яка моделює взаємозв'язки між словами у мовленні. Ці моделі допомагають знизити кількість помилок у розпізнаванні мовлення.

- Статистичні методи в розпізнаванні мови дозволяють моделювати та аналізувати мовлення з використанням ймовірнісних підходів. Це важливий напрямок досліджень, який сприяє підвищенню ефективності інфокомунікаційних систем та забезпеченню точного та надійного розпізнавання мовлення.

Методи машинного навчання грають важливу роль у досягненні високої ефективності в розпізнаванні мови. Вони базуються на алгоритмах та моделях, що використовуються для автоматичного виявлення та розпізнавання різних мовленнєвих патернів та шаблонів у вхідних аудіо- або відеозаписах.

Один з ключових методів машинного навчання - це модель глибокого навчання, відома як рекурентні нейронні мережі (RNN) та їх варіації, такі як LSTM (Long Short-Term Memory) та GRU (Gated Recurrent Unit). Вони здатні аналізувати послідовність акустичних властивостей мовлення та звуків, ураховуючи контекст та залежності між звуками в словах і реченнях.

- Популярним підходом є навчання моделей з використанням надзвичайно великих баз даних, включаючи зразки мовлення різних людей, акцентів та лексичних варіацій. Це дозволяє моделям покращувати свою здатність розпізнавати широкий спектр мовлення та адаптуватися до різних дикторів.

- Після тренування моделі можуть бути використані для розпізнавання мовлення в реальному часі, порівнюючи вхідний аудіосигнал з розпізнаними шаблонами та приймаючи рішення щодо найбільш імовірного розпізнаного тексту або команди.

- У загальному розумінні методів машинного навчання у розпізнаванні мови має значний потенціал для підвищення ефективності інфокомунікаційних систем. Ці методи дозволяють досягти високої точності та швидкості розпізнавання мовлення, забезпечуючи зручну та натуральну взаємодію між людиною та комп'ютерною системою.

ВИКОРИСТАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ДЛЯ ОЦІНКИ ТА КОМПЕНСАЦІЇ ВТРАТ УКРАЇНИ ВІД ЗБРОЙНОЇ АГРЕСІЇ НА ПРИКЛАДІ РИНКУ ПРАЦІ

Тишковець Артем Володимирович
Державний університет телекомунікацій

Російська агресія завдала серйозної шкоди українській економіці. За оцінками Міністерства економіки України, ВВП України у 2022 році знизилось на 29,2% . Очікується, що у 2023 році економіка почне відновлюватись, але ріст буде в межах статистичної похибки і коливатиметься від 0,3 до 1 % ВВП.

Суттєво постраждав і ринок праці України. Так Міжнародна організація праці оцінювала втрату робочих місць в Україні в 4,8 млн працівників [1]. Реальні показники були нижчими і за даним Пенсійного фонду України в піку, весною 2022 року досягали 2,9 млн працівників. При цьому зросло так зване «приховане безробіття». Так кількість осіб, які перебували у відпустці без збереження заробітної плати досягла 1,6 млн осіб, а кількість осіб, які працювали не повний робочий день або тиждень перевищила 1 млн.

Проте наявність цих даних у Пенсійного фонду України свідчить про побудовану систему збору даних про трудову діяльність працівників. Дійсно, у 2021 році була введена електронна трудова книжка, а інформація про трудову діяльність працівників зберігається в реєстрі застрахованих осіб Державного реєстру загальнообов’язкового державного соціального страхування (далі – Реєстр). Реєстр зберігає інформацію про період трудової діяльності, найменування роботодавця, розмір сплаченої заробітної плати працівнику (та динаміка

заробітної плати), а також періоди, коли трудові відносини зберігались, але заробітна плата не виплачувалась (відпустки без збереження заробітної плати, призупинення трудового договору) тощо.

Таким чином, Реєстр є банком даних про трудову діяльність працівника з можливостями для їх аналізу. Зазначену інформацію доцільно використати при оцінці втрат понесених працівниками через збройну агресію російської федерації.

Основним викликом, в такому випадку, буде побудова електронної системи збору та верифікації заявок від працівників. Проте Уряд України вже має релевантний досвід з виплатою грошової допомоги за вакцинацію від Covid 19, який може бути використаний для побудов такої системи. Основним цифровим рішенням виступатиме налагодження взаємодії між Єдиним портал державних послуг Дія (далі – портал Дія) та Реєстром. Виплати коштів можна проводити на вже існуючі рахунки «Є підтримки». Джерелом коштів для проведення виплат пропонується визначити кошти сплачені країною агресором як репарації та контрибуції. Типовою моделлю сплати репарацій пропонується використати адаптовану до українських реалій модель сплати репарацій Іраком Кувейту.

Накопичений Урядом України досвід впровадження цифрових рішень для адміністративних послуг, а також існуюча цифрова інфраструктура дозволить реалізувати запропоновану модель оцінки та компенсації втрат працівників від збройної агресії без залучення додаткових коштів. Налагодження взаємодії між порталом Дія та Реєстром пропонується проводити силами державного підприємства Дія та Пенсійного фонду України.

Розробка та впровадження системи оцінки та компенсації втрат працівників від збройної агресії російської федерації забезпечить компенсацію постраждалим учасникам ринку праці України, прискорить економічне відновлення країни після війни, пом’якшить соціальну шкоду завдану війною, а також створить прецедент поширення оцінки втрат від збройної агресії на соціально-трудову сферу, що збільшить ціну початку військових конфліктів в майбутньому. Використання цифрових інструментів при впровадженні такої системи дозволить забезпечити адресність та достовірність такої компенсації, а також дозволить знизити майже до нуля адміністративні витрати на реалізацію такої системи.

В подальшому, запропоновану систему пропонується поширити й на інших учасників ринку праці, зокрема роботодавців, профспілок та державу.

Список використаних джерел:

1. Report of the Director-General. Third Supplementary Report: Report on the application of the resolution concerning the Russian Federation’s aggression against Ukraine from the perspective of the mandate of the International Labour Organization. Governing Body. 345th Session, Geneva, June 2022. URL: https://www.ilo.org/gb/GBSessions/GB345/WCMS_847449/lang--en/index.htm (дата звернення: 28.05.2023).

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ SOFTWARE-DEFINED NETWORKING (SDN) У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Бабич В’ячеслав Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Програмно-конфігурована мережа (Software-Defined Networking — SDN) — це віртуалізована мережа для передавання даних, в якій шар менеджменту (контролю або управління) мережею (Management Plane) відокремлений від пристроїв передавання даних і

реалізується програмним шляхом. SDN являє собою одну з відомих форм віртуалізації обчислювальних ресурсів, зокрема мережних сервісів і додатків.

Мотивація щодо застосування SDN така.

1. Традиційні мережі занадто статичні, а отже, не відповідають динаміці, притаманній сучасному бізнесу, мережним (віртуальним) серверам, додаткам і сервісам.

2. Завдяки технологіям віртуалізації додатки розподілено сьогодні між безліччю віртуальних машин, які інтенсивно обмінюються даними. Для оптимізації завантаження серверів віртуальні машини часто мігрують, що, у свою чергу, призводить до змін точок «прив'язки» трафіку.

3. Традиційні схеми адресації, логічного поділу мереж, як і способи призначення правил обробки трафіку в сучасних динамічних середовищах втрачають ефективність.

Мережі SDN призначено для автоматизованого виконання низки завдань, серед яких:

♦ емуляція MAC-кадрів і пакетів (MPLS, IP, LAN, мобільний радіозв'язок поколінь 3G, 4G) на рівнях L2 і L3;

♦ розгортання зон, демаркація користувачів;

♦ «хмарні послуги» в договорах оренди Cloud Services;

♦ підтримка різноманітних SDN-архітектур і провайдерів

Втілення в життя концепції SDN для програмної реалізації провайдерського ядра на практиці, зокрема в мережах 5G, дасть змогу підприємствам і операторам зв'язку отримати незалежні від постачальника функції менеджменту та контролю над мережними компонентами й сервісами будь-якого типу з єдиного центру, що значно спростить їх експлуатацію. Рутинні функції реконфігурації мережі також спростяться. Адже адміністраторам не доведеться вводити сотні рядків коду конфігурації окремо для різних комутаторів або маршрутизаторів. Характеристики мережі можна буде оперативно змінювати в режимі реального часу. Відповідно, терміни впровадження нових додатків і сервісів значно скоротяться (Intelligent Web of connected things, Real-time remote control, Mobile Cloud Traffic, Immersive Experience, Lifelike media, Ubiquitous Connectivity, Telepresence тощо).

Список використаних джерел:

А. О. Лунтовський, А. І. Семенко, http://con.dut.edu.ua/index.php/communication/issue/view/63 [ст. 13-19]

ВПЛИВ ВІЙНИ НА РОЗВИТОК ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ В УКРАЇНІ

Ігнатенко Анастасія Сергіївна
Державний університет телекомунікацій
м. Київ

Телекомунікаційні системи являють собою комплекс програмного та апаратного обладнання, який з'єднаний один із одним в один ланцюг, що здійснює передачу даних з однієї точки в іншу. Така передача даних можлива завдяки чіткій структуризації телекомунікаційної мережі.

В Україні зв'язок є одним з найбільш стійких секторів економіки. Його стійка якісна робота є найважливішою умовою діяльності держави і суспільства. Однак війна суттєво впливає на розвиток телекомунікаційних систем в Україні, створюючи виклики щодо їхньої інфраструктури та функціонування. Руйнація та пошкодження інфраструктури, або навіть повне її знищення, внаслідок воєнного конфлікту обмежує доступ до зв'язку та інформації для населення та військових частин. Недостатній доступ до засобів комунікації та отримання інформації під час військових дій ускладнює координацію та оперативність дій військових підрозділів.

Слід зауважити, що вплив війни на розвиток телекомунікаційних систем спричиняє критичну необхідність невідкладних ремонтів та відновлення знищених та пошкоджених мереж аби забезпечити стійкий, якісний та безперебійний зв'язок. В умовах знищення інфраструктури важливу роль відіграє використання альтернативних технологій, таких як супутниковий зв'язок та мобільні мережі, що дозволить забезпечити зв'язок навіть у зруйнованих районах. Розвиток супутникових комунікаційних систем та їх використання дозволить забезпечити надійний та швидкий зв'язок у віддалених та обмежених доступом районах.

Розвиток резервних мереж та механізмів автоматичного переключення може забезпечити надійність телекомунікаційних систем навіть в умовах війни. Наприклад «велика трійка» українських мобільних операторів під час війни оголосила про створення національного роумінгу, це означає що кожен користувач може обрати будь якого мобільного оператора в Україні незалежно від сім-картки, яку використовує. Важливість мобільності та резервування телекомунікаційних мереж зростає в умовах війни.

Кібербезпека стає критично необхідною в таких складних умовах, оскільки загроза кібератак та кіберінцидентів зростає на телекомунікаційних системах. Необхідність розробки та впровадження стратегій захисту стає невідкладною. Також зростає необхідність використання технологій, що забезпечують анонімність та шифрування, щоб забезпечити приватність та безпеку користувачів. Запровадження ефективної системи оперативного реагування та попередження кібератак зменшить ризики пошкодження систем та забезпечить стійкість.

Використання безпілотних літальних апаратів, дронів та безпілотних технологій може бути корисним у військових операціях, але також може створювати нові виклики у забезпеченні безперебійного зв'язку та контролю над радіоспектром.

Зважаючи на вищезазначене, війна має серйозний вплив на телекомунікаційні системи в Україні, приводячи до пошкоджень та знищень інфраструктури, а також обмеження доступу до зв'язку. Ремонти та відновлення, які мають здійснюватися надзвичайно швидко та в найкоротші терміни, стають невідкладними завданнями для забезпечення стійкості, надійності та забезпечення безперебійного зв'язку в умовах війни.

З'ЄДНАННЯ ЗА ДОПОМОГОЮ ВИТОЇ ПАРИ: ОПИС ТА СТАНДАРТИ

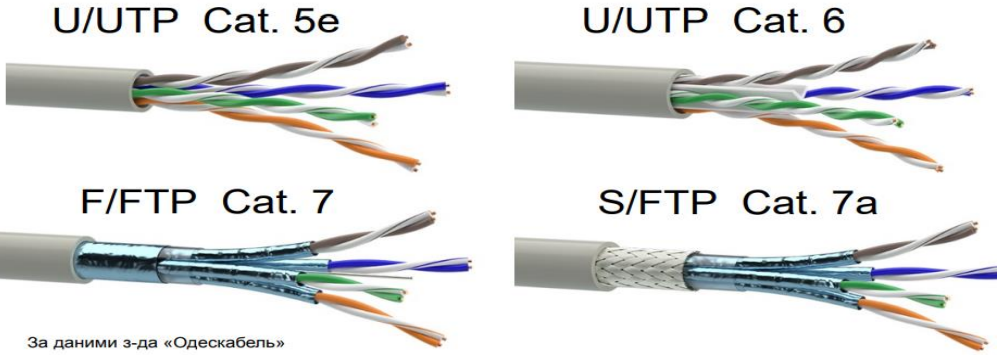
Голік Вадим Сергійович
Державний університет телекомунікацій

Встановлення підключень між мережами, та пристроями в мережі виконується за допомогою витої пари, коаксіального кабелю, оптичного волокна та бездротового з'єднання. В даній тезі буде розглянута вита пара.

Вита пара — вид мережевого кабелю, з однією або кількома парами ізольованих провідників, скручених між собою для зменшення взаємних наведень при передачі сигналу і покритих пластиковою оболонкою. Використовується для побудови мереж у багатьох технологіях. Останнім часом, завдяки своїй дешевизні й легкості установки, є найпоширенішою для побудови локальних мереж. Кабель приєднується до мережевих пристроїв за допомогою з'єднувача 8P8C, іноді інтерфейсу фізичного інтерфейсу RJ-11.

Стандарти кабелів "кручена пара" розроблені для того, щоб продукція відповідала універсальним вимогам для того, щоб гарантувати якість. Документ, в якому описані вимоги до кабелю кручена пара – ГОСТ 53246-2008. Якщо брати міжнародний рівень, то тут вже є інший стандарт – ISO 11801.

Має категорії CAT1-CAT7, CAT8 знаходиться на стадії розробки(до 40 Гбіт/с). Розповсюдження здобули кабелі CAT5e (1000 Мбіт/с), CAT6(10Гбіт/с), CAT7(10Гбіт/с,екранований) та CAT7a (10Гбіт/с, екранований) через їх низьку ціну та легкість використання в побудові LAN мереж. Нижче приведені їх характеристики:



За даними з-да «Одескабель»

Категорія	Конструкція	Ø жил, мм	Опір, Ом/км	Ємність, нФ/км	Згасання, дБ/100 м не більше на частоті				NEXT, дБ не менше на частоті			
					100	250	500	1000	100	250	500	1000
5E	U/UTP	0,51	92	56	22,0				35,3	-	-	-
6	U/UTP	0,54	87	56	19,9	33,0	-	-	45,3	39,3	-	-
7	F/FTP	0,56	75	56	19,0	31,0	45,3	-	75,5	66,4	61,9	-
7A	S/FTP	0,58	71	56	18,5	29,7	42,8	61,9	75,4	69,4	64,9	60,4

Типи захисту має: UPD-не екранований(відсутній захист);U/FTP-фольгований для кожної пари провідників; F/UTP-зовнішній екран із фольги; S/UTP-зовнішній екран із металевого обплетення; F/FTP, S/FTP-загальний екран із фольги або оплетки та індивідуальний фольгований.

Екранований дріт застосовується лише у місцях, де є джерела електромагнітного випромінювання.

Якщо брати до уваги діаметр кручений пари, то у не екранованого кабелю для монтажу всередині приміщення він становить 5-5,5 мм, а для зовнішніх робіт – 5,3-7 мм. Екранована вита пара має діаметр у межах 6-7 мм.

Конструктивно кабель складається з: мідних ізольованих провідників, поясної ізоляції, екрану, зовнішньої оболонки.

Ізоляція провідників виготовляється ПВХ, поліетиленом або поліпропіленом. У кабелі “вита пара” переріз жили маркується за американською системою калібрування і становить 22-26 AWG. В основному використовуються провідники діаметром 0,51 мм, що відповідає значенню 24AWG.

За типом жил розрізняють однодротовий та багатодротовий кабель. Перший використовується для монтажу всередині приміщень та підключення до розеток. Багатожильний провід кручена пара має гарну гнучкість і його застосовують для виготовлення комутаційних шнурів.

За призначенням кабель можна розділити на 3 види: для зовнішнього застосування, для монтажу всередині приміщення,для прокладання в пленум-областях.

Залежно від умов прокладання зовнішній кабель може мати додаткові конструктивні елементи: захисну оболонку з вологостійкого поліетилену чорного кольору, яка знижує вплив ультрафіолетових променів; гідрофобний заповнювач сердечника; броньові покриви з гофри чи дроту.

Оболонка кабелю для внутрішньої прокладки виготовляється із ПВХ зниженої горючості та має сірий колір. Помаранчева оболонка позначає використання полімерів, що не розповсюджують горіння і з низьким димовиділенням.

ДИНАМІЧНЕ УПРАВЛІННЯ ТРАФІКОМ В МЕРЕЖАХ СЕРВІС ПРОВАЙДЕРІВ

Михальчишин Т.Ю.
Державний університет телекомунікацій, м. Київ

Мережа Internet починалася як експеримент в кінці 1960-х років, який проводився агентством по передових дослідженнях (Advanced Research Project Agency – ARPA), яке знаходилося у відомстві Міністерства оборони США. Агентство ARPA проводило комплексні дослідження роботи комп'ютерів, об'єднаних у мережу. Так як результати експериментів зазнали успіху, мережа розвивалась, скоро покинула експериментальні та воєнні рамки і відносно скоро стала всесвітнім надбанням[1].

В результаті титанічних зусиль та неоцінимої роботи інженерів в 1989 році з'явилась перша версія протоколу граничного шлюзу – BGPv1. Масово використовується даний протокол 4-ї версії – BGPv4, починаючи із 1993 року, і на даний момент альтернативи йому не існує. Вперше, завдяки протоколу BGP, з'явилася можливість агрегації (об'єднання), що дозволяє реалізувати безкласову міждоменну маршрутизацію (CIDR), та забезпечити підтримку супермереж.

Все це дає підставу говорити, що даний протокол – опора всієї мережі Internet. Саме тому, в рамках розгляду питань даної роботи, протоколу BGP приділено найбільше уваги, так як саме на принципах даного протоколу побудована система автоматичного прийняття маршрутизаційних рішень, що є основним питанням досліджень[3].

BGP-community – один із атрибутів шляху згідно протоколу BGP, що дозволяє кожен із анонсованих або прийнятих префіксів (маршрутів) позначати спеціальним чином для ідентифікації маршруту та подальшої його обробки.

Один з варіантів застосування – передається сусідній AS для управління вхідним трафіком. Значення від 0x00000000 до 0x0000FFFF і від 0xFFFF0000 до 0xFFFFFFFF зарезервовані .

Як правило community (співтовариство) відображаються у форматі ASN: VALUE. У такому форматі, доступні для використання community від 1:0 до 65534:65535. У першій частині вказується номер автономної системи, а в другій значення community, яке визначає політику маршрутизації трафіку.

Деякі значення співтовариство зарезервовані. RFC1997 визначає три значення таких community. Ці значення повинні однаково розпізнаватися і оброблятися усіма реалізаціями BGP, які розпізнають атрибут community .

Якщо маршрутизатор отримує маршрут в якому зазначено зарезервоване значення communities, то він виконує специфічну, визначену дію засновану на значенні атрибута.

Зумовлені значення communities (Well- known Communities) :

- no-export (0xFFFFFF01) – всі маршрути, які передаються з таким значенням атрибута community не повинні анонсуватися за межі конфедерації (автономна система, яка не є частиною конфедерації вважається конфедерацією). Тобто, маршрути не анонсуються EBGP-сусідам, але анонсуються зовнішнім сусідам у конфедерації;
- no-advertise (0xFFFFFF02) – всі маршрути які передаються з таким значенням атрибута community не повинні анонсуватися іншим BGP-сусідам;
- no-export – subconfed (0xFFFFFF03) – всі маршрути які передаються з таким значенням атрибута community не повинні анонсуватися зовнішнім BGP-сусідам (ні зовнішнім у конфедерації, ні справжнім зовнішнім сусідам). У Cisco це значення зустрічається і під назвою local-as.

Список використаних джерел:

1. Cisco Press. Networks. – М.: «Вільямс», 2002. — 560 с. – ISBN 5-8459-0700-4, 1-5870-5043-9

2. Computer Networks: Principles, Technologies and Protocols for Network Design - Natalia Olifer, Victor Olifer, 2005. – 1000 с. – ISBN-10 0470869828, ISBN-13 978-0470869826
3. Iljitsch Van Beijnum. BGP.– «O'ReillyMedia», 2011. – 231 с.

ДОСЛІДЖЕННЯ СТАНДАРТИЗОВАНОЇ АРХІТЕКТУРИ ONEM2M IOT

Андрусенко Христина Віталіївна
Дмитренко Володимир Віталійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій

Сучасні виклики та вимоги до технології Інтернету речей стали рушійною силою для досліджень питань мережевої архітектури. В останні кілька років архітектурні норми зазнали змін, з'явилися фреймворки для вирішення проблем розробки широкомасштабних IoT мереж. Основоположною концепцією всіх цих існуючих архітектур є підтримка даних, процесів і функції, які виконують кінцеві пристрої[1].

Прагнучи стандартизувати швидко зростаючу сферу міжмашинного зв'язку (M2M) створено Європейський інститут стандартів телекомунікацій (ETSI) та технічний комітет M2M у 2008 році. Метою цих організацій було створити загальну архітектуру, яка допоможе прискорити впровадження додатків M2M. Згодом сфера застосування розширилася й охопила Інтернет речей[2]. Інші споріднені організації також почали створювати подібні архітектури M2M і спільна архітектура для стандарту M2M стала необхідністю.

Метою oneM2M було створення загального рівня послуг, який можна легко вбудувати в пристрої для забезпечення зв'язку з серверу додатків. Фреймворк oneM2M зосереджений на послугах Інтернету речей, програмах і платформах. До них належать інтелектуальні вимірювальні програми, «розумна» мережа, автоматизація «розумного» міста, електронна охорона здоров'я та підключені транспортні засоби.

Однією з найбільших проблем при розробці архітектури IoT є робота з неоднорідністю пристроїв, програмного забезпечення та методів доступу. OneM2M розробляє стандарти, які забезпечують взаємодію на всіх рівнях стеку IoT, шляхом розробки горизонтальної платформи архітектури. Наприклад, можна автоматизувати систему опалення, вентиляції та кондиціонування, підключивши її до безпроводових датчиків температури, розміщених у офісі. При цьому саме користувачеві вирішувати, які використовувати протоколи чи технології для розгортання датчиків (рис.1). Наприклад, горизонтальний фреймворк oneM2M і RESTful API дозволяють системі LoRaWAN взаємодіяти з системою управління будівлею через мережу IoT, таким чином сприяючи наскрізному зв'язку IoT узгодженим способом, незалежно від того, наскільки різнорідними є мережі.

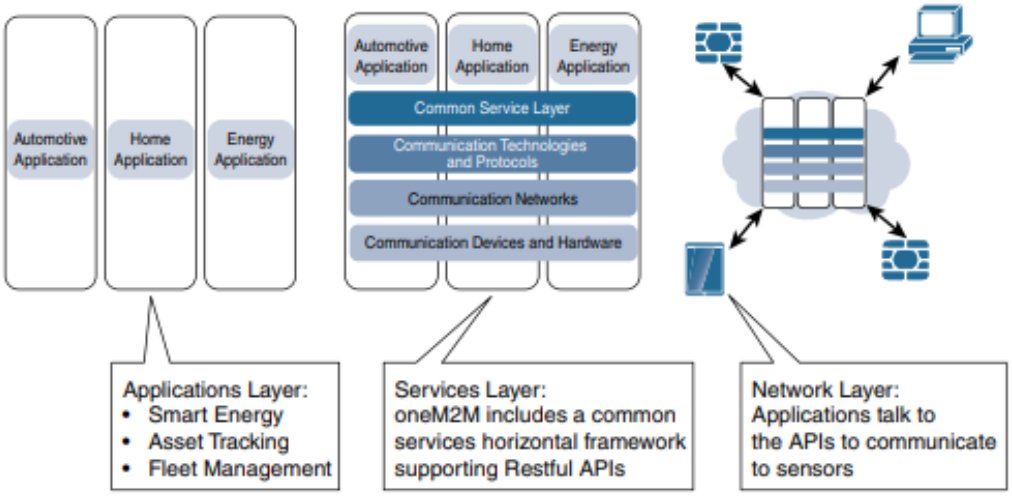


Рис.1. Основні елементи архітектури oneM2M IoT

Архітектура oneM2M поділяє функції IoT на три основні домени: рівень додатків, рівень послуг і мережевий рівень. Хоча така архітектура може здатися простою і дещо загальною на перший погляд, однак вона є насиченою і сприяє взаємодії через дружні до API та підтримує широкий спектр технологій[3].

У багатьох випадках «розумні» пристрої спілкуються з один одного. В інших випадках міжмашинний зв'язок не потрібен, і пристрої просто спілкуються через мережу (FAN) для конкретного випадку використання програми в домені програм IoT. Таким чином, домен пристрою також включає шлюзовий пристрій, який забезпечує зв’язок до базової мережі та діє як точка розмежування між пристроєм і мережевими доменами.

Перелік посилань

1. Arik Gabbai. Kevin Ashton describes the Internet of Things. [Електронний ресурс] - Режим доступу: www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749

2. Cisco. The Cisco Connected Factory: Powering a Renaissance in Manufacturin. [Електронний ресурс] - Режим доступу: www.cisco.com/c/dam/m/es_la/|internet-of-everything-ioe/industrial/assets/pdfs/cisco-connected-factory.pdf

3. OneM2M Technical Specification. [Електронний ресурс] - Режим доступу: ftp.onem2m.org/Deliverables/20140801_Candidate%20Release/TS-0002-Requirements-V-2014-08.pdf.

З'ЄДНАННЯ ЗА ДОПОМОГОЮ ОПТИЧНОГО ВОЛОКНА: ОПИС ТА СТАНДАРТИ

Голік Вадим Сергійович
Державний університет телекомунікацій

Оптичне волокно - це технічний виріб, що складається з оптичного світловоду і захисних покриттів та маркуючої кольорової оболонки. Оптичний світловод - це фізичне середовище транспортування оптичного сигналу і складається із серцевини та оболонки, що мають різні величини показників заломлення. Завдяки явищу повного внутрішнього відбиття, надається змога транспортування оптичних світлових сигналів, що генеруються та приймаються обладнанням, до якого підключено оптичне волокно.

Стандарти оптичних волокон описують розміри та характеристики оптичних волокон. Одномодове волокно має діаметр серцевини 8-10 мкм, а багатомодове - 50-62,5 мкм

Згідно режиму роботи оптичні волокна (ОВ) поділяються на два основні типи: Одномодові; Багатомодові.

Серцевина ОВ має змінну залежність величини показника заломлення по радіальній осі світловоду, котра називається профілем показника заломлення (ППЗ). Наприклад: Світловоди з градієнтним показником заломлення; Світловоди із сходинковим профілем показника заломлення.

Нижче приведеними стандартами згідно ISO/IEC 11801 та визначається специфіка використання:

Стандарт G.650 дає загальні визначення типів волокон, перелік основних характеристик і параметрів одномодових волокон, а також методів вимірювання та контролю цих параметрів.

Стандарт G.651 описує «Багатомодові оптичні волокна з градієнтним показником заломлення і діаметром світлопровідної серцевини 50 мкм» і обшивки 125 мкм і на ВОК на його основі. У ньому описані рекомендації по основним параметрам цих волокон, їх характеристикам і допустимим нормам. Цей тип волокон використовується тільки в короткохвильових лініях зв'язку з робочою довжиною хвилі 0,85 і рідко 1,31 мкм всередині приміщень. Застосовується для оптичних мереж невеликої довжини близько 1 км.

Стандарт G.652 "Характеристики одномодового оптичного волокна і кабелю" - розроблений для волокон довжиною 1,31 мкм. При такому показнику волокно G.652 має нульову хроматичну дисперсію і згасає з мінімальним значенням сигналу. У волокна G.652 діаметр сердечника дорівнює близько 9 мкм, а обшивки - 125 ± 2 мкм.

Оптичне волокно G.652 відрізняється високою надійністю і забезпечує передачу даних на швидкості до 10 Гбіт/с на дистанції 50 км. Застосування оптоволокна G.652 в лініях зв'язку, де необхідна передача даних на швидкості вище 10 Гбіт/с, вимагає встановлення більш складного обладнання, що спричиняє великі фінансові витрати.

Стандарт G.653 називається "Одномодове оптичне волокно із зсувом дисперсії" l = 1,55 мкм. Це волокно має нульову дисперсію в області мінімальних втрат волокна, таке числове значення досягається за рахунок більш складної конструкції світлопровідного сердечника, а саме спеціально заданому розподілу коефіцієнта заломлення по діаметру жили. Розмір світлопроводящього сердечника становить 8 мкм, обшивки - близько 125 мкм, захисного покриття - приблизно 250 мкм

Волокно типу G.653 використовується в протяжних магістральних широкосмугових лініях і мережах зв'язку, при побудові високошвидкісних інтернет ліній, воно забезпечує передачу інформації на кілька сотень кілометрів зі швидкостями до 40 Гбіт/с. Однак, по ньому можна передавати тільки один спектральний канал інформації, тобто воно не може бути використано в волоконно-оптичних системах і мережах, в яких застосовуються волоконно-оптичні підсилювачі і щільне оптичне спектральне мультиплексування (DWDM-технології). Причина цього полягає в високих рівнях світлової потужності в волокні після посилення і високої щільності спектрального ущільнення, тобто необхідності одночасної передачі великого числа незалежних спектральних каналів по одному волокну.

Висока концентрація світлової потужності в волокні - G.653 через особливості структури жили призводить до появи нелінійних ефектів і, зокрема, чотирьох хвильового зміщення, яке проявляється при нульовій хроматичної дисперсії і призводить в свою чергу до перехресних перешкод в лінії.

Стандарт G.654 - "Характеристики одномодового оптичного волокна і кабелю зі зміщеною дисперсією та відсічкою" з мінімальними втратами в межах 1,55 мкм. Це волокно було розроблено для передачі даних на багатокілометрові відстані в оптоволоконних лініях зв'язку під водою. За рахунок великих розмірів хвилеведучої жили, воно дозволяє передавати

більш високі рівні оптичної потужності, але в той же час має більш високу хроматичну дисперсією в діапазоні l = 1,55 мкм. Волокно типу G.654 не призначене для роботи на будь-якій іншій хвилі випромінювання крім l = 1,55 мкм. Діаметр жили 10,5 мкм. Діаметр обшивки становить 125 мкм і зовнішнього покриття 250 мкм.

Стандарт G.655 відноситься до волокна зі зміщеною ненульовою дисперсією - NZDSF (Non-Zero Dispersion Shifted Fiber) - "Характеристики одномодового оптичного волокна і кабелю з ненульовим дисперсійним зміщенням". Це волокно призначене для застосування в магістральних ВОЛЗ і системах, де широко поширене застосування технології DWDM в діапазоні довжин хвиль 1,55 мкм. Завдяки великому розміру сердечника і слабкою дисперсію може використовуватися на лініях зв'язку, де застосовуються оптоволоконні підсилювачі. Це знижує проблему чотирьох хвильового зміщення і нелінійних ефектів і відкриває можливості застосування ефективних волоконно-оптичних підсилювачів. Діаметр модового поля на довжині хвилі 1550 нм: 8,0 -11,0 мкм. Зовнішнє покриття - діаметр 250 мкм.

Стандарт G.656 - "Характеристики волокна і кабелю з ненульовою дисперсією для широкосмугової оптичної передачі" в області 1,55 мкм. В такому оптичному волокні ненульова дисперсія використовується для зменшення чотирьох хвильового змішування і перехресної фазової модуляції в більш широкому діапазоні довжин хвиль. Застосовується при побудові широкосмугових ліній зв'язку. Діаметр модового поля на довжині хвилі 1550 нм: 7,0 - 11,0 мкм ". Діаметр обшивки 125 мкм при захисному покритті 250 мкм.

Стандрат G.657 - «Характеристики одномодового оптичного волокна і кабелю, що не чутливий до втрат на макро вигині, для використання в мережах доступу». Волокна описані в рекомендації G.657 допускають дуже малі радіуси вигинів. Оптимально підходять для застосування у внутрішніх приміщеннях. По інших оптичних характеристиках цей тип оптоволокна аналогічний рекомендацій G.652.D. Діаметр модового поля на довжині хвилі 1310 нм: 6,3-9,5 мкм. покриття 125 мкм.

Типи роз’ємів для підключення оптичного волокна:

Серед великої кількості роз’ємів таких як ST, SC, FC, LC, MU, E2000, MTRJ, SMA, DIN, а також MTP і MPO, можна виділити:FC/PC (Physical Contact), FC/APC (Angled Physical Contact), SC/PC (Physical Contact), SC/APC (Angled Physical Contact), ST/PC (Physical Contact), LC/PC (Physical Contact), LC/APC (Angled Physical Contact).

Використання матеріалу для виготовлення:

Скляне оптоволокно майже завжди виробляється із діоксиду кремнію, проте деякі інші матеріали, як флуорид цирконію, алюмінію та халькогеніди, а також кристалічні матеріали на зразок сапфірів, теж використовується для довгохвильових інфрачервоних та інших специфічних застосувань. Діоксид кремнієве та флуоридне скло зазвичай мають показник заломлення десь близько 1,5, але деякі інші матеріали можуть досягати цього показника аж до 3. Типово, різниця цих величин матеріалів серцевини та оболонки волоска є меншою одного процента. Пластикове волокно береться для виготовлення сходинкових мультимодових світловодів із діаметром серцевини 0.5мм і більше,так як надає більше згасання.

ДОСЛІДЖЕННЯ ТРАНСПОРТНИХ МЕРЕЖ П’ЯТОГО ПОКОЛІННЯ З МІНІМАЛЬНИМИ ЗАТРИМКАМИ СИГНАЛІВ

Клещевніков Дмитро Олегович
Державний Університет Телекомунікацій

Дослідження транспортних мереж п'ятого покоління з мінімальними затримками сигналів є необхідним для впровадження майбутніх інноваційних технологій, таких як

автономні автомобілі, розширена реальність та Інтернет речей, і це підкріплюється дослідженнями та джерелами.

Розшифровка:

Затримки сигналів є важливою проблемою, яка впливає на продуктивність і ефективність транспортних мереж. Дослідження їх мінімізації стануть критичними для забезпечення швидкості передачі даних, зменшення відгуку та покращення загальної якості зв'язку.

Впровадження майбутніх технологій, таких як автономні автомобілі, вимагає низького рівня затримок сигналів, щоб забезпечити швидку і безперебійну передачу даних між автомобілями, інфраструктурою та центральними системами керування. Дослідження транспортних мереж п'ятого покоління в цьому контексті стануть основним кроком у забезпеченні безпеки та ефективності автономної транспортної системи.

Використання розширеної реальності та Інтернету речей вимагає низького рівня затримок, щоб забезпечити швидку передачу даних між пристроями та інтерактивність в реальному часі. Дослідження транспортних мереж п'ятого покоління, спрямовані на зниження затримок сигналів, є важливим кроком у покращенні користувацького досвіду та успішному впровадженні цих технологій.

Приклади необхідності дослідження транспортних мереж п'ятого покоління з мінімальними затримками сигналів в повсякденному житті та наукових відкриттях:

Автономні автомобілі: Дослідження транспортних мереж з мінімальними затримками сигналів є критичним для успішного впровадження автономних автомобілів. Низькі затримки сигналів дозволяють автомобілям отримувати реальні дані з датчиків, передавати інформацію між автомобілями та інфраструктурою, і приймати швидкі та безперебійні рішення на основі цих даних. Це підвищує безпеку, зменшує затори та покращує ефективність транспортної системи.

Розширена реальність: Дослідження з мінімальними затримками сигналів також є важливим для реалізації розширеної реальності (AR). AR дозволяє взаємодіяти з віртуальними об'єктами у реальному світі. Затримки сигналів можуть спричиняти несинхронізацію візуальних та звукових ефектів, що руйнує іммерсію та користувацький досвід. Дослідження мереж п'ятого покоління з фокусом на зменшення затримок допомагають забезпечити плавну та реалістичну взаємодію з віртуальними об'єктами у реальному часі.

Інтернет речей (IoT): IoT базується на взаємодії між великою кількістю підключених пристроїв, які обмінюються даними. Затримки сигналів можуть впливати на швидкість та надійність комунікації між цими пристроями. Дослідження транспортних мереж п'ятого покоління з мінімальними затримками сигналів сприяють створенню надійних та ефективних мереж IoT, що відкривають нові можливості для покращення управління будинками, містами та різними індустріальними процесами.

Наукові дослідження та інновації: Вивчення транспортних мереж п'ятого покоління з мінімальними затримками сигналів сприяє науковим відкриттям та інноваціям. Це дозволяє вирішувати складні технічні проблеми, розробляти нові алгоритми передачі даних та протоколи комунікації, і підвищує наші знання про оптимальні методи побудови ефективних транспортних мереж майбутнього.

Ці приклади показують, що дослідження транспортних мереж п'ятого покоління з мінімальними затримками сигналів мають велике значення як для покращення повсякденного життя, так і для прогресу наукових досліджень та технологічних інновацій.

ОСОБЛИВОСТІ ЗАХИСТУ WI-FI МЕРЕЖ

Журбенко Володимир Валерійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Захист Wi-Fi мережі є дуже важливим завданням. Зловмисники вміло інфікують домашні та корпоративні мережі з метою отримання прибутку. До їх схем відносяться крадіжка особистих даних, наприклад, номера банківських рахунків та шифрування файлів комп'ютера з метою викупу. Тому безпека мережі так важлива для забезпечення захисту ваших даних від зловмисників.

Даний термін асоціюється з великою корпоративною мережею, до якої належать тисячі комп'ютерів. Однак навіть кілька комп'ютерів, підключених до домашнього роутера, також вважаються мережами. Забезпечення їх безпеки не менш важливе, оскільки вони також містять Ваші файли.

Основні загрози безпеці Wi-Fi мереж можуть бути наступними:

- Несанкціонований доступ до мережі Wi-Fi;
- Перехоплення трафіку Wi-Fi;
- Атаки на точки доступу Wi-Fi;
- Використання слабких паролів.

Особливості захисту Wi-Fi мереж полягають у використанні різних методів захисту. Механізми захисту Wi-Fi мереж передбачають автентифікацію (клієнт та точка доступу представляються один одному і підтверджують права на обмін даними) та шифрування (обрання алгоритму шифрування інформації та даних, що передаються по бездротовій мережі, генерація та зміна ключів).

Існує кілька типів захисту Wi-Fi мережі, таких як:

- WEP (Wired Equivalent Privacy);
- WPA (Wi-Fi Protected Access);
- WPA2 (Wi-Fi Protected Access II).

WEP є застарілим і небезпечним методом перевірки автентичності. WPA є надійним і сучасним типом безпеки з максимальною сумісністю з усіма пристроями і операційними системами. WPA2 є новою, допрацьованою і більш надійною версією WPA з підтримкою шифрування AES CCMP.

Щоб зробити свою Wi-Fi мережу більш безпечною, можна використовувати різні методи захисту. Наприклад, створити складний пароль для точки доступу, змінювати пароль на регулярній основі та використовувати надійний антивірус.

СУТНІСТЬ ТА ОСОБЛИВОСТІ ВОЛЗ

Забродський Антон Ігорович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

ВОЛЗ (волоконно-оптична лінія зв’язку) – це система лінії зв’язку, яка складається з систем передачі та прийому оптичного зв’язку, діелектричного середовища передачі інформації

– оптичне волокно, та складається з пасивних систем оптичного зв'язку та активних систем оптичного зв'язку.

В 70-х роках минулого століття почались дослідження нового типу зв'язку, який може передати інформацію швидко, далеко та інформація може містити великий об'єм даних. Цим новим видом зв'язку став оптичний зв'язок. Після декількох досліджень різних варіантів передачі оптичного зв'язку було виявлено, що для того, щоб передати інформацію без втрат та щоб на нього не впливали зовнішні чинники, було вирішено використовувати скло (SiO_2) як носій інформації, який можна передати за рахунок світла та законів оптики. Як виявилося, після проведення декількох досліджень, скло є ідеальним матеріалом для оптичного волокна (ОВ). В ті ж самі роки минулого століття вдалося створити оптичне волокно з затуханням 16 дБ/км. Після цього, виготовлення та використання волоконно-оптичних кабелів зв'язку (ВОК) зростала та набирала популярність.

Потім у 80-ті роки минулого століття оптична система передача зв'язку знайшла своє застосування і навіть змогла ще далі розкинутися, як нова система зв'язку. Перший побудова волоконно-оптичної лінії зв'язку та застосування оптичного зв'язку в Україні починається у 1986 році, які використовувалися на міських мережах. В ті рокі встановлювалася система передачі «Соната-2», та воно було з'єднувальною міжстанційною лінією. Система тих років дозволяла використовувати та організовувати 120 цифрових каналів ОЦК (64 кбіт/с) зі швидкістю 8,448 Мбіт/с по двох волокнах з градієнтним профілем показника заломлення.

В кінці 80-х років минулого століття на зонових мережах почало використовуватися обладнання «Сопка 2/3» (кількість каналів – 120 або 480 ОЦК). У 90-х роках минулого століття та на початку 21-го століття – 2000-ні роки почалося будівництво магістральних ліній оптичного зв'язку. Першим магістральним оптичним зв'язком став: «Захід», а потім стала ціла низка: «ІТУР», «Таврія», «Північ», «Дніпро-Донбас», «Схід» та ін. Далі, магістральні оптичні лінії зв'язку, за ними – зонові, будувалися за схемою кінцевої топології.

Потребами волоконно-оптичного зв'язку є: використання невидимої частоти оптичного спектру інфрачервоного діапазону довжини хвиль (800-1675 нм). Електромагнітні хвилі розповсюджуються у вакуумі зі швидкістю $3*10^8$ м/с. В оптичному волокні, якщо спиратися на закони оптики, коли проміно падає на границю розділу двох середовищ, у яких є різні оптичні характеристики, певна його частина відбивається. Відношення оптичної хвилі у вакуумі до швидкості оптичної хвилі у середовищі називають показником заломлення. Показник заломлення показує та доказує – у скільки разів фазова швидкість електромагнітної хвилі в середовищі є меншою від швидкості розповсюдження оптичної хвилі у вакуумі. Відношення синуса кута падіння до синуса кута заломлення дорівнює зворотному відношенню показників заломлення середовищ розповсюдження оптичних хвиль, що розглядаються.

Оптичні кабелі діляться на два види: одномодові а багатомодові. Одномодові оптичні кабелі – це вид кабелів, у яких оптичні волокна, по яким в робочому діапазоні частот розповсюджується лише основна мода. Багатомодові оптичні кабелі – це вид оптичних кабелів, у яких оптичні волокна, по яким в робочому діапазоні частот розповсюджується більше однієї моди.

Одне волокно оптичного кабелю може передати інформацію зі швидкістю 40 Гбіт/с. Зростання рівня потужності передавання сигналу в оптичному волокні та зростання його швидкості передавання даних потребує створення нового покоління оптичних волокон та оптичних кабелів. В такому разі, оптичні волокна мають мати великі діаметри серцевин для одномодового режиму. На основі таких питань, було вирішено цю проблему за рахунок розроблення ряду оптичних волокон – мікроструктуроване волокно та волокно на основі

фотонних кристалів. Вони відрізняються від звичайних оптичних волокон тим, що вони виготовлюються з однорідного скла.

В волокні з фотонним кристалом локалізація світла в центрі волокна виходить за рахунок інтерференції на періодичній структурі, яка має розмір, що дорівнює довжині оптичній хвилі, яка створюється циліндричними порожнинами. Фотонний кристал полягає у періодичній структурі, де промені світла, що відбиті від областей з різним показником заломлення, можуть інтерферувати один одного, посилюючись або послаблюючи, що може від співвідношення довжин хвиль та періоду структур.

Література:

1. Високошвидкісні волоконно-оптичні лінії зв'язку: навч. посіб. / Г.М. Розорінов, Д.О. Соловйов. – 2-е вид., перероб. і допов. – К.: Кафедра, 2012. – 344 с.
2. Каток В.Б., Руденко І.Е., Ранський Є.Г., Однорог П.М. Волоконно-оптичний зв'язок / Під ред. Катка В.Б. – К.: Логос, 2015. – 383 с.: іл.

ЗАГАЛЬНА АРХІТЕКТУРА СЕНСОРНИХ МЕРЕЖ

Брезіцький Сергій Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій

Сенсорні мережі є важливою складовою частиною сучасних систем збірних даних. Вони дозволяють збирати, обробляти та аналізувати інформацію з навколишнього середовища за допомогою різноманітних датчиків.

Архітектура бездротової сенсорної мережі у відповідності до моделі OSI (рис. 1) складається з п'яти рівнів: рівня додатків, транспортного рівня, мережевого рівня, канального рівня і фізичного рівня. Також додаються три додаткові площини: площина керування живленням, площина управління мобільністю, площина управління завданнями.

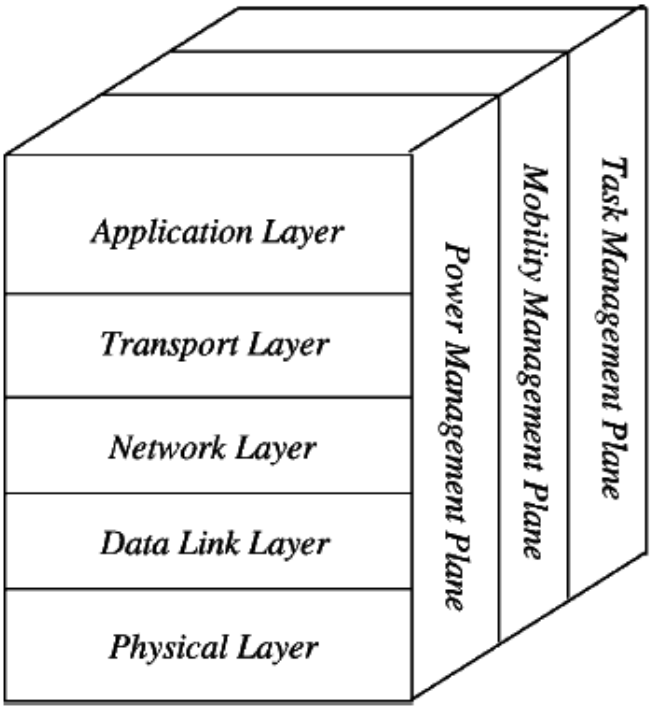


Рисунок 1. Архітектура бездротової сенсорної мережі

Рівень додатків (Application Layer). Прикладний рівень відповідає за управління трафіком і пропонує програмне забезпечення для різних додатків, які перетворюють дані в зрозумілу форму для пошуку відповідної інформації. Сенсорні мережі організовані в численних додатках у різних галузях, таких як сільське господарство, військова промисловість, охорона навколишнього середовища, медицина тощо.

Транспортний рівень (Transport Layer). Функція транспортного рівня полягає в тому, щоб забезпечити уникнення перевантажень і забезпечити надійність там, де багато протоколів, призначених для надання цієї функції, є практичними у висхідній частині. Ці протоколи використовують різні механізми для розпізнавання та відновлення втрат. Транспортний рівень якраз і потрібен, коли планується зв'язок системи з іншими мережами. Забезпечення надійного відновлення втрат є більш енергоефективним, і це одна з головних причин, чому TCP не підходить для бездротових сенсорних мереж. Загалом, транспортний рівень можна розділити на пакетний та подієвий. Існує декілька популярних протоколів транспортного рівня, а саме STCP ((Sensor Transmission Control Protocol), PORT (Price-Oriented Reliable Transport Protocol) і PSFQ (pump slow fetch quick).

Мережевий рівень (Network Layer). Основна функція мережевого рівня - маршрутизація, він має багато завдань, що залежать від додатку, але насправді основні завдання полягають в енергозбереженні, обмеженій кількості пам'ять, буфери та датчики не мають універсального ідентифікатора і повинні бути самоорганізованими. Проста ідея протоколу маршрутизації полягає в тому, щоб пояснити надійні та надлишкові смуги відповідно до вибіркової шкали, яка називається метрикою, що варіюється від протоколу до протоколу. Існує багато протоколів для цього мережевого рівня, їх можна розділити на пласку маршрутизацію та ієрархічну маршрутизацію, або ж розділити на керовану часом, керовану запитами та керовану подіями.

Канальний рівень (Data Link Layer). Канальний рівень відповідає за мультиплексування, виявлення кадрів даних, потоків даних, MAC і контролю помилок, підтверджує надійність з'єднання "точка-точка" (або "точка-багатоточка").

Фізичний рівень (Physical Layer). Фізичний рівень забезпечує передачу потоку бітів через фізичне середовище. Цей рівень відповідає за вибір частоти, генерацію несучої частоти, виявлення сигналу, модуляцію та шифрування даних. IEEE 802.15.4 пропонується як типовий для низькошвидкісних окремих районів та бездротових сенсорних мереж з низькою вартістю, енергоспоживанням, щільністю, дальністю зв'язку для збільшення часу автономної роботи. CSMA/CA використовується для підтримки топології зірка та однорангової топології. Існує декілька версій стандарту IEEE 802.15.4.V.

Додаткові міжрівневі площини в основному використовуються для управління мережею, а також для того, щоб датчики працювали як єдине ціле, щоб підвищити загальну ефективність мережі.

Площина керування живленням (Power Management Plane) відповідає за керування рівнем потужності сенсорних вузлів для обробки, зондування та зв’язку

Площина управління мобільністю (Mobility Management Plane) відповідає за конфігурацію або реконфігурацію вузлів датчиків при встановленні і підтримуванні підключення до мережі.

Площина управління завданнями (Task Management Plane) відповідає за розподіл завдань між сенсорними вузлами для продовження терміну служби мережі та підвищення енергоефективності.

Список використаних джерел

1. Ahmad Abed Alhameed Alkhatib, Gurvinder Singh Baicher. Wireless Sensor Network Architecture, 2012 International Conference on Computer Networks and Communication Systems(CNCS 2012) IPCSIT vol.12 (2011)© (2011)IACSIT Press, Singapore. Режим доступу: // https://www.researchgate.net/profile/Ahmad-

Alkhatib/publication/227352986_Wireless_Sensor_Network_Architecture/links/0fcfd4fe1f8216be00000000/Wireless-Sensor-Network-Architecture.pdf

2. Kamaldeep Kaur, Parneet Kaur, Er. Sharanjit Singh. Wireless Sensor Network: Architecture, Design Issues and Applications. International Journal of Scientific Engineering and Research (IJSER) www.ijser.in ISSN (Online): 2347-3878 Volume 2 Issue 11, November 2014. Режим доступу: // https://www.ijser.in/archives/v2i11/MTMxMTE0MDE=.pdf

УДОСКОНАЛЕНИЙ МЕТОД РОЗПОДІЛУ ПРОПУСКНОЇ СПРОМОЖНОСТІ В БЕЗДРОТОВИХ МЕРЕЖАХ НА ОСНОВІ НЕЙРО-НЕЧІТКИХ МЕРЕЖ

Здоренко Юрій Миколайович,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»,
к.т.н., доцент кафедри комп'ютерних та інформаційних технологій та систем
Селеменов Юрій Іванович,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»,
студент
Здоренко Марина Сергіївна,
Європейський університет

Сучасні бездротові мережі мають ряд особливостей функціонування, які впливають на показники якості обслуговування кінцевих користувачів. Необхідна пропускна спроможність для обслуговування користувачів забезпечується використанням відповідного виду модуляції сигналу. Одним з найбільш поширених цифрових видів модуляції є квадратурна амплітудна модуляція QAM-M. Порядок M модуляції QAM визначає пропускну спроможність тракту. Більша пропускна спроможність тракту забезпечується вищим порядком QAM модуляції. Сучасні радіозасоби передбачають адаптивну зміну порядку M модуляції QAM в залежності від співвідношення потужності сигнал/шум на вході приймача. Для цього бездротові засоби мають режими адаптації потужності передавача, що також дозволяє забезпечити кращу електромагнітну сумісність та скритність лінії в порівнянні з режимом постійної потужності. Однак, в існуючих системах не враховується потреба на забезпечення мінімально необхідної пропускної спроможності тракту, виходячи з інтенсивності очікуваного трафіку [1]. Тому, при виборі рівня потужності сигналу меншого за пороговий, можуть зрости втрати пакетів. В роботі [1] запропонований метод розподілу пропускної спроможності на основі використання нейро-нечітких мереж для прогнозування очікуваного навантаження в найближчий часовий період. Однак в даному підході не враховано вищезазначених можливостей бездротових мереж по адаптації своїх параметрів. Тому пропонується поєднати можливості двох вищезазначених підходів для забезпечення оптимального рішення. В умовах динамічої зміни пропускної спроможності тракту та наявності прогнозних даних про вхідне навантаження, перерозподіл пропускної спроможності запропоновано здійснювався на основі рішення задачі лінійного програмування [1]. Однак в умовах значних навантажень уникнути втрат пакетів стає неможливим. Тому, для їх зменшення, запропонований в [1] метод, пропонується удосконалити шляхом використання адаптивних підходів при виборі виду модуляції. Так, для адаптації потужності випромінювання пропонується завчасно визначати значення загасання на радіонапрямку протягом найближчого проміжку часу. Рівень сигналу в точці прийому в загальному випадку може бути описаний основним рівнянням радіопередачі:

$$P_{rec} = \frac{P_{tr}\gamma_{tr}G_{tr}G_{rec}\gamma_{rec}}{L_o L_{add}} \quad (1)$$

де P_{tr} - потужність сигналу на виході передавача, γ_{tr}, γ_{rec} - коефіцієнти передачі трактів, що зв'язують відповідно вихід передавача з передавальною антеною і вихід прийомної антени з приймачем, G_{tr}, G_{rec} - коефіцієнти підсилення передавальної і приймальні антен відповідно, L_o, L_{add} - основні і додаткові втрати енергії сигналу в просторі між станціями.

Компенсацію очікуваного (прогнозного) загасання сигналу пропонується здійснювати шляхом завчасної адаптації потужності випромінювання радіозасобів з врахуванням очікуваної потреби в пропускній спроможності. Задачу лінійного програмування для перерозподілу пропускної спроможності пропонується вирішувати на основі значення пропускної спроможності, яку можна забезпечити з врахуванням компенсації очікуваного загасання сигналу.

Список використаних джерел

1. Polcshikov K., Masesov M., Zdorenko Y. Method of telecommunications channel throughput distribution based on linear programming and neuro fuzzy predicting, Elixir International Journal, Network Engineering, 2014. – Vol. 75 – pp.27327–27334.

ПЕРСПЕКТИВНІ МЕТОДИ ПЕРЕДАВАННЯ ДЛЯ ЗАСТОСУВАННЯ В МЕРЕЖАХ 6G

Іващенко Петро Васильович,
Орябінська Олеся Олександрівна,
Кудряшов Андрій Сергійович,
Державний університет інтелектуальних технологій і зв’язку, м. Одеса

На сьогодні існує безліч стандартів для побудови IoT-пристроїв, які реалізують фізичний рівень мережі. Рішення про вибір стандартів для розгортання мережі IoT залежить від багатьох факторів, передусім, це необхідні характеристики фізичного рівня. В цілому, при виборі стандартів надають перевагу пристроям з низьким споживанням енергії. Технології LPWA (Low Power Wide Area) призначені для M2M (Machine-to-Machine)-додатків, які вимагають низькошвидкісної передачі даних по радіоканалу та роботи без нагляду протягом тривалого часу, можливо у віддалених або важкодоступних місцях. Вимоги IoT-додатків настільки різноманітні, що всі випадки використання LPWA єдиною технологією не охоплюються. Для безпроводового підключення IoT-пристроїв існує низка можливостей і одна з них – це перспективні мережі 6G. На сьогодні основним напрямком досліджень застосувань IoT в мережах 6G є розроблення систем з новими алгоритмами демодуляції та низькою обчислювальною складністю. Для цього виконується пошук нових сигналів, прийом яких можливий з мінімальними втратами завадостійкості за допомогою простих алгоритмів [1]. Необхідність застосування саме простих алгоритмів демодуляції обумовлена підвищеними вимогами до швидкості передавання в системах IoT та енергоефективності прикінцевих пристроїв. Оцінити кожен з критеріїв перспективних методів передавання – досить складна задача, тому розглянуті основні критерії з точки зору використання ресурсів каналу – це позасмугове випромінювання та частотно-часова ефективність; енергоспоживання та обчислювальна складність. Частотно-часова ефективність залежить від методу передавання і є важливим параметром для порівняння характеристик використовуваних сигналів. Порівняння показує, що перерахованим критеріям в найбільшій мірі відповідають методи передавання UFMC і GFDM (фільтровані OFDM сигнали). Ставиться задача – порівняти складність IoT-пристроїв та частотно-часову ефективність вказаних методів передавання. Порівняння складності проведено шляхом підрахунку кількості обчислень при виконанні швидкого перетворення Фур’є та фільтрації.

Частотно-часова ефективність усіх методів передавання крім GFDM та FBMC не залежить від розміру пакета. Частотно-часова ефективність методу FBMC наближається до ефективності методу OFDM, коли розмір пакета наближається до 5, і він показує більшу ефективність за розмірів пакета, що перевищують 5 символів. Найнижчий рівень позасмугового випромінювання за FBMC і швидко спадає поза виділеною смугою частот. В порівнянні з OFDM, W-OFDM має найнижчу складність. F-OFDM і FBMC приблизно в п'ять і шість разів складніші за OFDM, а GFDM в 12 разів складніше в порівнянні з OFDM. Найвища складність властива UFMC (у десятки – сотні разів вища порівняно з OFDM). Складність UFMC прямо пропорційна кількості піддіапазонів. Слід зазначити, що більш ефективні способи реалізації, наприклад багатофазна, можуть знизити складність UFMC в 5 – 10 разів. Методи передавання UFMC і GFDM більше підходять для передачі короткими пакетами в порівнянні з іншими сигнальними конструкціями, але мають досить високу складність порівняно з іншими методами передавання. Метод FBMC більше підходить для передачі довгих пакетів і неефективний для передачі коротких пакетів. Враховуючи, що для IoT характерні короткі пакети та бажана низька складність обладнання, оптимальними методами можуть бути F-OFDM або W-OFDM. Для об’єктивного кінцевого вибору необхідно порівняти завадостійкість обох методів.

Література:

1. Вэнь Тонг, Пейин Чжу (редакторы). Сети 6G. Путь от 5G к 6G глазами разработчиков. От подключенных людей и вещей к подключенному интеллекту. / Пер. с англ. В.С. Яценкова. – М.: ДМК Пресс, 2022. – 624 с.: ил.

РОЛЬ ШИФРУВАННЯ В ЗАБЕЗПЕЧЕННІ КОНФІДЕНЦІЙНОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Іщенко Ілля
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Телекомунікаційні мережі забезпечують передачу і обмін інформацією між вузлами, але в цифровому світі збільшується загроза несанкціонованого доступу до цих даних. Одним із ключових методів захисту є шифрування, яке забезпечує конфіденційність даних та приватність комунікацій.

Шифрування - це процес перетворення зрозумілого тексту (криптографічного ключа) в незрозумілий формат (шифрованого тексту) за допомогою спеціального алгоритму шифрування. Шифрування забезпечує захист даних, оскільки лише особа з правильним ключем може розшифрувати зашифровану інформацію.

Конфіденційність є одним з основних принципів безпеки телекомунікаційних мереж. Вона означає забезпечення та збереження конфіденційності передаваних даних, що включає особисту інформацію, комерційні дані, банківські транзакції тощо. Шифрування відіграє ключову роль у забезпеченні цієї конфіденційності.

Шифрування дозволяє зробити передані дані незрозумілими для сторонніх осіб, які не мають права доступу до цих даних. За допомогою шифрування, дані перетворюються на шифрований формат, що неможливо розібрати без відповідного ключа. Це забезпечує високий рівень конфіденційності переданих даних і унеможливлює їх несанкціонований доступ.

Існує багато видів шифрування, таких як симетричне шифрування, асиметричне шифрування та хеш-функції. Симетричне шифрування використовує один ключ для

шифрування та розшифрування даних, тоді як асиметричне шифрування використовує пару ключів: публічний і приватний. Хеш-функції використовуються для перетворення даних в унікальний хеш-код, який не може бути розшифрований.

Шифрування застосовується в різних аспектах телекомунікацій, таких як бездротові мережі, віртуальні приватні мережі (VPN), електронна пошта, месенджери та інші комунікаційні канали. Шифрування забезпечує захист від перехоплення інформації, підробки та несанкціонованого доступу до даних.

У зв'язку з постійним розвитком технологій та загроз кібербезпеці, шифрування стає складнішим завданням. Кіберзлочинці намагаються зламати шифри, а тому постійне вдосконалення алгоритмів шифрування та використання сильних ключів є важливими викликами. Проте, розвиток квантового шифрування може відкрити нові перспективи для ще більш безпечної телекомунікаційної інфраструктури.

Шифрування відіграє невід'ємну роль у забезпеченні конфіденційності телекомунікаційних мереж. Воно забезпечує захист передаваних даних, перешкоджаючи несанкціонованому доступу та забезпечуючи приватність комунікаційних процесів. Розуміння ролі шифрування та використання сучасних шифрувальних методів є ключовим для створення безпечного телекомунікаційного середовища.

ПРОТОКОЛИ IP - ТЕЛЕФОНІЇ

Карпенко Сергій Анатолійович
Державний університет телекомунікацій

При здійсненні дзвінка голосовий сигнал перетворюється на стислий пакет даних (докладніше цей процес буде розглянуто у розділах “Імпульсно кодова модуляція” та “Кодеки”). Далі відбувається пересилання даних пакетів поверх мереж з комутацією пакетів, зокрема IP мереж. При досягненні пакетів одержувача вони декодуються в оригінальні голосові сигнали. Ці процеси можливі завдяки великій кількості допоміжних протоколів, частина яких буде розглянута далі.

У цьому контексті протокол передачі даних — певна мова, яка дозволяє двом абонентам зрозуміти один одного та забезпечити якісне пересилання даних між двома пунктами.

Протоколи IP-телефонії - мережеві протоколи, що використовуються для організації телефонних розмов та іншої мультимедійної взаємодії поверх IP-мережі.

На сьогоднішній момент немає чіткого стандарту протоколу IP-телефонії. Умовно протоколи IP телефонії можна розділити на дві групи: сигнальні та передачі даних. Постараємося розглянути найпоширеніші їх і використовувані, нині, з практичного боку питання.

Сигнальні протоколи:

SIP (Session Initiation Protocol)

Протокол встановлення сеансу зв'язку перша версія протоколу SIP 1.0 вийшла в 1999 році і була описана в рекомендаціях RFC 2543 організацією IETF. У 2002 році вийшла остаточна рекомендація протоколу SIP 2.0 описана в рекомендації IETF RFC 3261. З того часу SIP обростав безліччю доповнень і розширень. SIP, будучи клієнт-серверним протоколом, подібно до HTTP і SMTP працює на основі послідовних запитів-відповідей. Як і HTTP, SIP реалізований за допомогою текстових тегів – усі SIP-заголовки передаються у вигляді ASCII-тексту, що спрощує його використання у додатках. На даний момент SIP протокол став основним в обладнанні IP-телефонії, в першу чергу за його лаконічність та простоту.

Додатково існують різновиди даного протоколу для використання його в традиційних мережах загального користування SIP-T (Session Initiation Protocol for Telephones), описаного в

RFC3372 та SIP-I (Session Initiation Protocol Internetworking), основне завдання яких є прозора передача ОКС7 (ISUP) повідомлень по IP -Мережі.

Протокол H.323

Історично перший протокол для IP телефонії, розроблений Міжнародним союзом електрозв'язку (ITU) в 1996 році. У свою чергу, H.323 охоплює питання передачі голосу, відеоданих через ір-мережі. На сьогоднішній день цей протокол використовується все рідше і рідше, в основному у старих аналогових АТС. Недоліком даного протоколу стала його складність і прихильність до медіа даних на відміну від SIP.

Skinny (SCCP)

Пропрієтарний протокол для IP телефонії використовуваний компанією Cisco у своєму телекомунікаційному обладнанні. Якоюсь мірою стороннє обладнання Symbol Technologies, IPBlue, SocketIP і Asterisk вміє працювати з цим протоколом.

H.248 (MEGACO)

Цей протокол використовується між елементами телекомунікаційних мереж: шлюзом (Media Gateway) та контролером шлюзів (Media Gateway Controller). Підтримує різні системи сигналізації мереж із комутацією каналів, включаючи тонову сигналізацію, ISDN, ISUP, QSIG та GSM. Закріплений як стандартний протокол IMS, поряд із SIP та Diameter. Є спадкоємцем протоколу MGCP та використовується в основному мережах провайдера IMS платформ.

IAX2 (Inter-Asterisk eXchange protocol)

Протокол розроблений для роботи IP-АТС Asterisk. Особливістю даного протоколу є пристосованість до трансляції мережевих адрес та подолання NAT голосових пакетів. На відміну від SIP та H.323 використовує лише один порт 4569 протоколу UDP для сигналізації та медіаданих. Протокол використовується в мережах із слабкою пропускною здатністю і більше практично не розвивається.

Протоколи передачі:

RTP (Real-time Transport Protocol)

Протокол, призначений передачі аудіо і відеопотоків через мережу Інтернет. Описаний в RFC3550 (до цього в RFC 1889). Цим же стандартом описується протокол RTCP (Real-time Control Protocol), призначений для узгодження параметрів QoS між учасниками обміну.

SRTP (Secure Real-time Transport Protocol)

Розширення до протоколу RTP, що забезпечує шифрування, автентифікацію, цілісність та захист від повторів. Опубліковано як RFC 3711і використовує порт 5004.

ВАРІАНТ СТРУКТУРИ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ NGN В УКРАЇНІ

Кононов Андрій
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

NGN (англ. Next Generation Network — мережа наступного покоління) — це мультисервісна мережа зв'язку, яка підтримує інтеграцію послуг передавання мови, даних та мультимедіа та базується на IP-мережі (на відміну від ISDN). Основна відмінність мереж наступного покоління від традиційних мереж в тому, що вся інформація, яка циркулює в мережі, розбита на дві складові. Це сигнальна інформація, що забезпечує комутацію абонентів та надання послуг, і безпосередньо дані користувача, що містять корисну інформацію, призначену абоненту (голос, відео, дані). Шляхи проходження сигнальних повідомлень і даних користувача можуть не збігатися. Функціональна архітектура NGN поділяється на три

функціональні площини та чотири функціональні шари. Функціональними площинами NGN є: площина транспорту, площина доступу та прикладна площина. У цій градації втілено основний принцип NGN — впровадження послуг, що не залежать від систем доступу до них, і відокремлення транспорту від систем доступу й обслуговування.

Площина транспорту забезпечує зв'язок між двома іншими площинами. Вона відповідає за доставку інформації (як медіапотоків, так і сигналізації виклику та команд управління пристроями). Відповідно, технологія транспорту, що використовується, має підтримувати всі види трафіка, для обслуговування якого призначається NGN.

У площині доступу здійснюється адаптація різноманітних технологій перенесення інформації для передавання через транспортну площину. У цій площині, зокрема, здійснюється конвертація потоків з часовим розподілом сигналів у пакетний формат і перетворення сигналізації ТфЗК у сигналізацію транспортної мережі.

Прикладна площина відповідає за надання користувачам послуг шляхом маніпулювання інформаційними та сигнальними потоками у мережі. За типом інформації, що передається, функціональні об'єкти NGN поділяються на чотири рівні: сигналізації, послуг/управління, інформації та мережевого управління. Компонентами функціональних рівнів є функції, основними з яких є: функція медіашлюзу, функція контролера медіашлюзів, функція сервера прикладних програм, функція медіасервера, функція перетворення сигналізації та функція тарифікації. Ці функції можуть бути фізично реалізовані як окремі пристрої, або ж один пристрій може поєднувати декілька функцій. Рівень послуг/управління здійснює управління послугами та виконанням сервісної логіки, забезпечуючи обробку викликів та надання різних за складністю послуг. До пристроїв цього рівня належать так званий софтсвіч — Softswitch (або контролер медіашлюзів — MGC) та сервер прикладних програм AS. Для реалізації послуг ці пристрої взаємодіють з пристроями рівнів інформації та сигналізації. Взаємодія між шлюзом і контролером здійснюється через протокол MEGACO (H.248) або MGCP. Контролер медіашлюзів управляє роботою одного або кількох медіашлюзів, що забезпечують взаємодію мереж на нижчих рівнях, і зосереджує у собі інтелект пари «шлюз — контролер», яка виконує функції місцевої або міжміської АТС.

Література:

1. ITU-T Recommendation. NGN JRG/13 – Lucent Technologies. Management and Control for NGN, 2004. - 9 p.

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА ПІДПРИЄМСТВА ЯК ЗАСІБ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ

Жмака С.В. *студент, група САДМ-51,*
Державний університет телекомунікацій, м. Київ

Необхідною умовою підвищення ефективності діяльності будь-якого сучасного підприємства є використання інформаційно-телекомунікаційних систем. Без цього сьогодні неможливе швидке і якісне приймання рішення на всіх рівнях управління. Саме використання інформаційно-телекомунікаційних систем забезпечує управлінський персонал підприємства якісною та своєчасною інформацією, що дозволяє вчасно аналізувати параметри господарської діяльності підприємства та всебічно оцінювати та прогнозувати результати його роботи.

Різні аспекти використання інформаційних систем в діяльності підприємств досліджували Сухоцька С. М. [2], Пацай Б.Д. [3], та інші.

Використання інформаційно-телекомунікаційних систем.

Інформація є сьогодні одним з найголовніших ресурсів, без вчасного володіння інформацією неможливе ефективне використання людських, матеріальних та інших ресурсів підприємства. Накопичення та зберігання такої інформації на підприємстві відбувається саме за допомогою інформаційно-телекомунікаційних систем, тому вдосконалення інформаційно-телекомунікаційної системи є засобом здешевлення то оптимізації апарату управління [1].

Найважливішим аспектом формування ефективної інформаційної системи є створення єдиної інформаційної мережі, що забезпечує накопичення, обробку та обмін інформацією як по вертикалі, так і по горизонталі. Така мережа стане базою для управлінської діяльності підприємства. Це, в свою чергу дозволить вирішити низку проблем:

- складність вибору оптимального рішення в умовах невизначеності;
- складність обробки великих обсягів інформації;
- необхідність прийняття рішення в обмежений проміжок часу;
- складності координації рішення з іншими підрозділами;
- необхідність накопичення та збереження досвіду.

Апаратна частина інформаційно-телекомунікаційних систем.

З вищевикладеного випливає, що інформаційно-телекомунікаційна система – це програмно-апаратний комплекс. І саме від правильно побудованої та налагодженої апаратної частини залежить працездатність та ефективність всієї системи в цілому. Апаратна частина - це мережа яка містить стандартне устаткування – маршрутизатори, концентратори, роутери, точки доступу, різноманітні термінальні пристрої.

Основна задача, що постає в процесі побудови такої мережі – це її здатність забезпечувати стійкий канал зв'язку і своєчасний доступ до необхідної інформації між всіма її учасниками. Для реалізації цієї задачі мережа повинна надавати можливість оперативного моніторингу пристроїв передачі даних та динамічного їх коригування. Тому при побудові та модернізації інформаційних мереж навіть невеликих підприємств все частіше використовується кероване обладнання замість некерованого, а виробниками втілюються нові мережеві протоколи та архітектури.

Тенденції розвитку інформаційно-телекомунікаційних мереж

Одним з напрямків розвитку телекомунікаційних мереж є втілення архітектури програмно-керованих мереж (Software-Defined-Networking, SDN) [4]. Ця архітектура є кроссплатформеною, завдяки чому автоматично знімається проблема залежності від конкретного виробника обладнання. Ця архітектура передбачає відокремлення функцій управління від функцій передачі даних, реалізоване програмним шляхом, в той час як в класичних комутаторах ці процеси пов‘язані.

В архітектурі SDN контролери можуть бути як фізичними так і віртуальними пристроями. Управління здійснюється по протоколам Open-Flow. Згідно логіки SDN частина мережі, що складається з пристроїв різних виробників, розглядається як один логічний комутатор. Це дозволяє адміністраторам налаштовувати мережу як єдине ціле, а не займатися безліччю окремих комутаторів. Така концепція значно спрощує конфігурування та експлуатацію мережі. Комутатори, в свою чергу, можуть бути простими та дешевими. Настроювання мережі можна змінювати в режимі реального часу, скорочуючи таким чином терміни впровадження нових сервісів.

ПО управління використовує API виробника комутатора, тому для виконання найрізноманітніших функцій розробнику не потрібно знати особливості роботи конкретного мережевого пристрою.

Висновки.

Проаналізувавши важливість використання інформаційно-телекомунікаційної системи на підприємстві, можна зауважити, що в підготовці та прийнятті управлінських рішень таке використання займає в сучасних умовах чи не найголовнішу роль. Від обґрунтованості та ефективності прийнятого рішення залежить сьогодні вся діяльність підприємства, в тому числі

досягнення поставлених цілей. І, зважаючи на величезні об’єми інформації, що треба проаналізувати, без використання інформаційно-телекомунікаційних систем неможливе прийняття рішення, що буде достатньо ефективне.

Але крім самого факту використання системи, багато залежить ще і від того, як ця система побудована та налаштована. Наскільки повний об’єм інформації вона здатна накопити й переробити, наскільки швидко та своєчасно вона надасть необхідну інформацію. Навіть те, на якому обладнанні побудований фізичний рівень інформаційно-телекомунікаційної системи – теж впливає на те, наскільки своєчасне та ефективне рішення буде прийняте в той чи інший час.

Список використаної літератури

1. Годін В.В.Інформаційне забезпечення управлінської діяльності: підручник. / В.В. Годін, І.К. Корнєєв. -М.: Майстерність, 2001.-240с.
2. Зелінська О. В., Сухоцька С. М. Використання сучасних інформаційних технологій в агропромисловому комплексі // Галицький економічний вісник. – 2016. – №2. – С. 148–152.
3. Пацай Б.Д. Роль інформаційних технологій в управлінні фінансовими ресурсами підприємств.// Фінанси України. - № 8 – 2008. – с.82-84.
4. Смелянский Руслан. Программно-конфигурируемые сети. Открытые системы. СУБД, №9. Открытые системы (20 ноября 2012).

ТЕХНОЛОГІЯ FTTx: ПЕРЕВАГИ ТА НЕДОЛІКИ

Ленда Євгеній Олександрович,
Державний університет телекомунікацій, м. Київ

Fiber To The X або FTTx (англ. fiber to the x - оптичне волокно до точки X) - це загальний термін для будь-якої комп'ютерної мережі, в якій від вузла зв'язку до певного місця (точка X) доходить волоконно-оптичний кабель, а далі, до абонента, - мідний кабель (розглядається варіант в якому оптоволокно прокладається безпосередньо до абонента.

Переваги:

- Мале загасання сигналу (0,15 дБ/км в третьому вікні прозорості) дозволяє передавати інформацію на значно більшу відстань без використання підсилювачів. Підсилювачі у технології можуть ставитися через 40, 80 і 120 кілометрів, залежно від класу кінцевого устаткування.
- Висока пропускна здатність оптичного волокна дозволяє передавати інформацію на високій швидкості, недосяжною для інших систем зв'язку.
- Висока надійність оптичного середовища: оптичні волокна не окислюються, не намокають, не схильні до слабкого електромагнітного впливу.
- Висока захищеність від міжволоконних впливів - рівень захисту, випромінювання понад 100 дБ. Випромінювання в одному волокні не впливає на сигнал в сусідньому волокні.
- Пожежо- та вибухобезпечність при вимірюванні фізичних і хімічних параметрів.
- Малі габарити і маса.

Недоліки:

- Відносна крихкість оптичного волокна. При сильному вигинанні кабелю (присутнє явище якщо силовий елемент використовується склопластиковий пруток) можлива поломка волокон або їх помутніння через виникнення мікротріщин.
- Проблематичність з’єднання у випадку розриву.
- Складна технологія виготовлення як самого волокна, так і компонентів системи.
- Складність перетворення сигналу.

- Висока вартість кінцевого рішення. Устаткування є дорогим у абсолютних цифрах. Співвідношення ціни і пропускної спроможності для ВОЛП краще, ніж для інших систем.
- Втрата прозорості волокна з часом, внаслідок старіння.

Розглянувши види архітектур, які входять до технології **FTTx** хотілося б відмітити самі розповсюдженні і дати їм короткий опис:

FTTB (Fiber to the Building) – оптичне волокно до будівлі. В цій архітектурі оптичне волокно доходить до комутаційного обладнання оператора, який розміщений переважно на границі території будівель або підприємств. **FTTH (Fiber to the Home) -** оптичне волокно до приватного будинку або квартири. Кабель прокладається до границі площі користувача, це може бути коммунікаційна коробка. **FTTC (Fiber to the Curb) –** оптичне волокно прокладене до мікрорайону, кварталу, певної кількості будинків.

FTTN (Fiber to the Node) – волокно до вузла мережі. Оптоволокно закінчується у вуличній шафі, за пару кілометрів від кінцевого споживача.

МЕТОДИ ДОСЛІДЖЕННЯ АЛЬТЕРНАТИВНИХ ДЖЕРЕЛ ЖИВЛЕННЯ В ТЕЛЕКОМУНІКАЦІЯХ

Романенко Валентин
Державний університет телекомунікацій

Розвиток альтернативних джерел живлення в телекомунікаціях є важливим кроком у напрямку сталого розвитку та зменшення негативного впливу на довкілля. Дослідження різних методів використання альтернативних джерел живлення у телекомунікаціях дозволяють знайти оптимальні технологічні рішення для ефективного використання цих джерел. У даному творі розглянемо деякі методи дослідження альтернативних джерел живлення в телекомунікаціях та їх значення для розвитку сучасної інфраструктури зв'язку.

Один з методів дослідження альтернативних джерел живлення - аналіз потужності та продуктивності. Для визначення придатності альтернативних джерел живлення необхідно провести ретельний аналіз їх потужності та продуктивності. Це означає вивчення виробництва енергії, стабільності живлення та ефективності використання ресурсів. Наприклад, дослідження сонячних панелей для живлення телекомунікаційних веж дозволяє визначити потужність, яку вони можуть забезпечувати, а також оцінити, як вони працюють в умовах різних погодних умов.

Ще одним методом дослідження є економічний аналіз. Дослідження альтернативних джерел живлення також включає оцінку економічної доцільності їх використання. Необхідно порівняти вартість встановлення та експлуатації альтернативних джерел з традиційними джерелами живлення. Такий аналіз дозволяє визначити, наскільки вигідним є використання альтернативних джерел живлення для телекомунікаційних систем.

Також важливим методом дослідження є оцінка впливу на довкілля. Альтернативні джерела живлення повинні бути не тільки ефективними та економічно вигідними, але й мінімізувати негативний вплив на навколишнє середовище. Дослідження повинні включати аналіз екологічних показників, таких як викиди шкідливих речовин, споживання води та земельні ресурси. Наприклад, дослідження використання біогазу для живлення телекомунікаційних систем дозволяє оцінити його екологічні переваги порівняно з традиційними джерелами енергії.

Одним із найважливіших методів дослідження є пілотні проекти та експерименти. Перед впровадженням альтернативних джерел живлення в широкому масштабі необхідно провести пілотні проекти, під час яких будуть випробовуватися нові технології та методи. Такі проекти дозволяють виявити потенційні проблеми та знайти оптимальні рішення. Наприклад, пілотний проект з використання вітрової енергії для живлення телекомунікаційних веж дозволяє встановити ефективність та надійність таких систем у реальних умовах.

Отже, дослідження альтернативних джерел живлення у телекомунікаціях вимагають комплексного підходу та використання різних методів. Аналіз потужності, економічний аналіз, оцінка впливу на довкілля та пілотні проекти допомагають визначити ефективність та доцільність використання альтернативних джерел живлення в телекомунікаціях. Ці дослідження сприяють розвитку сталої та екологічно чистої інфраструктури зв'язку, що є важливим кроком у напрямку сталого розвитку суспільства.

Джерела:

1. Tiwari, G. N., & Singh, H. N. (2012). Sustainable energy development: The present (2011) scenario and future (2025) projections. Renewable and Sustainable Energy Reviews, 16(4), 244-284.
2. Bakshi, B. R., & Lepech, M. D. (2013). Sustainability science and engineering: The emergence of a new metadiscipline. Environmental Science & Technology, 47(18), 10165-10175.
3. Zhang, X., Zhao, C., Chen, H., Li, X., & Dai, Y. (2020). Comparative analysis of renewable energy and fossil fuel based mobile base station. Applied Energy, 263, 114635.
4. Dincer, I., & Rosen, M. A. (2012). Thermal energy storage: Systems and applications (2nd ed.). John Wiley & Sons.
5. Hosseini, S. E., & Wahid, M. A. (2016). Renewable energies for sustainable development in developing countries: A review. Renewable and Sustainable Energy Reviews, 60, 599-620.

МЕТОДИ ЗБІЛЬШЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ LTE В НЕЛІЦЕНЗІЙНОМУ РАДІОЧАСТОТНОМУ СПЕКТРІ

Кондратенко Владислав Андрійович
Державний університет телекомунікацій

Очікуване зростання мобільного трафіку даних пов'язано із впровадженням трафіку нових широкосмугових послуг та запуском бездротового зв'язку. Передача через мобільні мережі величезна і буде продовжувати зростати швидко. Очікується, що в 2021 році рух даних мобільного зв'язку по всьому світу, як очікується, досягне 587 екзабайт на рік, тобто в сім разів більше, ніж був трафік мобільного трафіку по всьому світу в 2016 році. Трафік від бездротових та мобільних пристроїв складатиме дві третини загального обсягу трафіку IP до 2020 року, оскільки річні абоненти потребують більшої пропускної здатності для передачі великих обсягів даних. З метою збільшення ємності мережі мобільного зв'язку було
визначено низку технологічних рішень для використання неліцензованого спектра, що дозволило створити додатковий радіочастотний ресурс.

Технологія LTE (Long-Term Evolution) є одним з ключових стандартів мобільного зв'язку, яка надає швидку передачу даних та високу якість зв'язку. З ростом популярності мобільних пристроїв та збільшення обсягів передачі даних, забезпечення ефективного

використання технології LTE в неліцензійному радіочастотному спектрі стає надзвичайно важливим завданням для операторів зв'язку.

Методи збільшення ефективності використання технології LTE в неліцензійному радіочастотному спектрі відіграють ключову роль у забезпеченні якісного та стабільного мобільного зв'язку. Для досягнення цієї мети можна використовувати ряд методів та підходів, які описані нижче:

1. Керування ресурсами: Ефективне керування ресурсами є одним із основних методів збільшення ефективності використання неліцензійного радіочастотного спектру. Це включає оптимізацію розподілу доступних ресурсів для різних користувачів, використання алгоритмів, що враховують їх потреби в швидкості передачі даних та якості зв'язку. Такі алгоритми дозволяють ефективно розподіляти ресурси та запобігати перевантаженням мережі.

2. Використання кооперативного спектру: Для підвищення ефективності використання неліцензійного спектру можна використовувати кооперативні підходи. Оператори мобільного зв'язку можуть спільно використовувати спектр та ділитися ним, забезпечуючи більшу пропускну здатність та покриття. Це може бути досягнуто шляхом встановлення спільних угод та взаємодії між операторами.

3. Використання розумних антен та антенних систем: Вдосконалені антенні системи, такі як масивні антени, можуть значно покращити ефективність використання неліцензійного спектру. Ці системи забезпечують кращу просторову керованість та можуть працювати в режимі більшої направленості, зменшуючи взаємний вплив сусідніх базових станцій та покращуючи якість зв'язку.

4. Використання мультиносійкових технологій: Використання технологій мультиносійкового введення-виведення (MIMO) є ще одним ефективним методом збільшення ефективності використання неліцензійного спектру. MIMO використовує кілька антен для передачі та прийому даних, що дозволяє збільшити пропускну здатність та покриття. Застосування MIMO технології в неліцензійному спектрі може покращити продуктивність мережі LTE та забезпечити кращу якість зв'язку.

5. Використання технологій когнітивного радіо: Технології когнітивного радіо можуть використовуватися для ефективного використання незайнятих частотних діапазонів та спектральних ресурсів, які не використовуються в даний момент. Це дозволяє оптимізувати використання неліцензійного спектру та покращити ефективність мережі LTE. Когнітивне радіо може автоматично виявляти доступні ресурси та переключатися між ними, що забезпечує оптимальне використання спектру.

Методи збільшення ефективності використання технології LTE в неліцензійному радіочастотному спектрі є важливими для забезпечення надійного та швидкого мобільного зв'язку. Керування ресурсами, використання кооперативного спектру, вдосконалені антенні системи, мультиносійкові технології та когнітивне радіо - це лише деякі з методів, які можуть підвищити ефективність використання технології LTE в неліцензійному спектрі.

Подальше дослідження та вдосконалення цих методів допоможуть розширити можливості мобільного зв'язку та задовольнити зростаючі потреби користувачів. Забезпечення ефективного використання неліцензійного радіочастотного спектру є важливим завданням для операторів зв'язку та сприятиме розвитку мобільних технологій.

Очікується, що LTE продовжить розвиватися до моделі 11, 12 покоління і так далі, з кожним новим поколінням, що привнесе додаткові можливості та покращить продуктивність системи в технологію радіодоступу LTE. Додаткові можливості забезпечать кращу продуктивність існуючих програм. Вони також можуть відкривати нові сфери застосування або навіть бути мотивованими ними. Домашня автоматизація, інтелектуальний транспорт, безпека та електронні книги є одними із сфер застосування технології LTE-радіодоступу, але список постійно розширюється, оскільки з’являються додаткові програми, які використовують переваги мобільного зв’язку.

МОДЕЛЬ ЗБОРУ ДАНИХ IOT В «РОЗУМНОМУ» МІСТІ

Дяченко Владислава Анатоліївна
Дмитренко Володимир Віталійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій

Концепція «Інтернет речей» (IoT) основана на підключені об’єктів, що мають IP-адреси до мережі, та можуть бути об’єднанні в такі програми, як: «розумне» здоров’я, «розумні» міста, «розумна» енергія, «розумна» транспортна система тощо.

Дозволяючи підключати унікальні об’єкти до мережі, яка віддалено може ділитися даними, створеними цими об'єктами і взаємодіяти один з одним, концепція IoT представляє значну кількість переваг щодо покращення більшості аспектів людського життя.

«Розумні» об’єкти, присутні в просторі IoT, є самосвідомими та здатними для віддаленої передачі пакетів даних, згенерованих один одному через мережу зв’язку. Концептуалізація IoT полягає в тому, щоб зробити Інтернет більш поширеним для «розумних» речей, дозволяючи різнорідні пристрої, такі як датчики, сенсори, RFID, ZigBee, 6LowPAN, підключатися та взаємодіяти один з одним.

Будівництво «розумного» міста здається трудомістким і дорогим на перший момент, але важливі ресурси можна заощадити, інвестуючи в додаткові технології. «Розумне» місто має шість ключових характеристик.

Усі характеристики надають Smart City дані, як показано на рис.1.

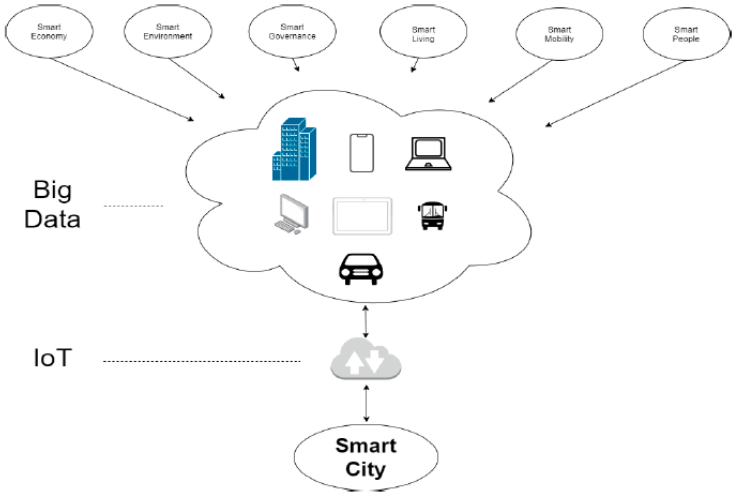


Рис.1. Блок-схема «розумного» міста

Шість пунктів у верхній частині рис.1 представляють ключові характеристики «розумного» міста. Усі характеристики разом мають одну важливу особливість: вони передають і отримують дані через смартфони, планшети, комп’ютери, ноутбуки або навіть будівлі (реалізація «розумний» дім) і транспортні засоби. Ці дані називаються Big Data.

Інтернет речей – це технологічна частина передачі даних. Таким чином, усі зібрані дані передаються до відділів «розумного» міста, які потім аналізуються та обробляються для здійснення подальшого контролю над суб’єктами IoT або надавання інформації мешканцям.

Представлена блок-схема (рис.1) ілюструє різні залежності в межах «розумного» міста і демонструє, як місто збирає дані для опрацювання. Саме компоненти «розумного» міста спілкуються із використанням Інтернету речей з різними «розумними» пристроями, які належать мешканцям.

Сучасні міста вже мають інтелектуальну реалізацію, наприклад анімовані рекламні плакати, інформаційні дисплеї на автобусних зупинках, однак більшість із них не пов’язані

одне з одним і не підключені між собою за допомогою безпроводового зв'язку. Крім того, вони не мають реалізованих шести ключових характеристик.

Необхідною умовою для розгортання IoT є здатність інфраструктури ІКТ бути здатною пропонувати швидкі та надійні послуги передачі даних.

Можна виокремити чотири ефективні підходи для впровадження «розумних» міст:

- Сприяння фундаментальним дослідженням та розробці/переходу з теоретичних інновацій на практичну реалізацію «розумних» міст;
- Сприяння дослідженням та упровадженням безпечної та стійкої інфраструктури, систем і послуг для «розумних» міст;
- Сприяння прогресу «розумних» міст шляхом обміну даними та знаннями з іншими «розумними» містами;
- Увімкнення оцінки прогресу та перспектив щодо довгострокового зростання «розумних» міст та громад.

Важливо підкреслити, що інфраструктура ІКТ включає в себе всі пристрої, мережі, протоколи та процедури, які використовуються в галузі телекомунікацій та інформаційних технологій. ІКТ-інфраструктури мають вирішальне значення для пропозиції різноманітних цифрових рішень для розгортання «розумних» міст.

Перелік посилань

4. Internet of Things architecture. [Електронний ресурс] –Режим доступу: https://www.ibm.com/cloud/architecture/architectures/iotArchitecture

5. Young-Mo Kang, Mi-Ran Han, Kyeong-Seok Han and Jong-Bae Kim. A Study on the Internet of Things (IoT) Applications. International Journal of Software Engineering and Its Applications. Vol.9. 2015. Pp. 117-126.

6. Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, Michele Zorzi. Internet of Things for Smart Cities. IEEE Internet of things journal. Vol.1. 2014.

7. Pike research on smart cities. [Електронний ресурс] –Режим доступу: http://www.pikeresearch.com/research/smart-cities.

АНАЛІЗ ПРОТОКОЛІВ ПОТОКОВОЇ ПЕРЕДАЧІ ВІДЕО

Мороз Юрій Анатолійович
Державний Університет телекомунікацій
Навчально-науковий інститут телекомунікацій

У сучасному світі відео контент займає дедалі більше місце в житті кожної людини. Відео-стрімінг стає одним з основних методів отримання інформації, розваг та спілкування. Якість передачі відео по мережі інтернет відіграє важливу роль у задоволенні потреб користувачів. Враховуючи вище сказане, аналіз протоколів потокової передачі відео є актуальною та важливою темою дослідження.

Протоколи потокової передачі відео можуть бути розділені на три основні типи: протоколи, засновані на HTTP, протоколи на основі RTMP, та протоколи, що використовують реальний час. Серед них, HTTP Live Streaming (HLS) та Dynamic Adaptive Streaming over HTTP (DASH) є найпопулярнішими для передачі відео через інтернет, тоді як Real-Time Messaging Protocol (RTMP) використовується для передачі потокового відео у реальному часі. Варто звернути увагу на WebRTC як перспективну технологію для передачі відео з мінімальною затримкою.

Якість передачі відео залежить від ряду параметрів, таких як бітрейт, кадрова частота, роздільна здатність та кодеки, які використовуються для стиснення відео. Більш високі

значення бітрейту, кадрової частоти та роздільної здатності забезпечують кращу якість зображення, але потребують більшої пропускної здатності. Адаптивні протоколи потокової передачі, такі як HLS та DASH, дозволяють автоматично налаштовувати якість відео залежно від швидкості інтернет-з'єднання користувача.

Адаптивний бітрейт - ключова технологія для оптимізації якості передачі відео. Він дозволяє пристосовувати якість відео до швидкості інтернет-з'єднання користувача, щоб забезпечити неперервне відео без буферизації. Різні алгоритми адаптивного бітрейту, такі як BOLA, MPC та Pensieve, мають свої особливості.

Передача відео в режимі реального часу стикається з декількома проблемами, такими як затримка, синхронізація аудіо та відео, а також втрати пакетів. Затримка, яка виникає при передачі відео через мережу, може погіршити користувацький досвід, особливо в ситуаціях, коли відео вимагається відтворювати синхронно для кількох користувачів, наприклад, під час спільного перегляду. Протоколи, які спеціально розроблені для передачі відео в режимі реального часу, такі як WebRTC, можуть забезпечити мінімальну затримку та ефективну синхронізацію.

Для забезпечення стабільної роботи протоколів потокової передачі відео важливо мати можливість моніторингу та діагностики проблем, що виникають під час передачі. Інструменти моніторингу, такі як QoE-метрики (Quality of Experience), дозволяють виявляти проблеми з профілем передачі, затримкою, втратами пакетів та іншими параметрами. Використовуючи ці дані, інженери можуть оптимізувати протоколи та налаштування мережі для покращення якості передачі відео.

З розвитком нових технологій, таких як 5G та WebRTC, можливості передачі відео продовжують розширюватись. 5G забезпечує збільшення пропускної здатності мережі, нижчу затримку та більш надійне з'єднання, що дає можливість передавати відео високої якості з мінімальними перебоями. WebRTC, засноване на відкритих стандартах, забезпечує просте та ефективне з'єднання для передачі відео в режимі реального часу без необхідності встановлення додаткових плагінів або програм.

Відкриті стандарти та ініціативи від організацій, таких як IETF (Internet Engineering Task Force) та W3C (World Wide Web Consortium), сприяють розвитку та стандартизації протоколів потокової передачі відео. Зокрема, робота над стандартизацією DASH та WebRTC, а також співпраця з приватним сектором, дозволяє впроваджувати нові рішення, що покращують якість передачі відео та сприяють широкому їх використанню.

Аналіз протоколів потокової передачі відео демонструє, що вибір протоколу, параметрів якості та алгоритмів адаптивного бітрейту впливає на користувацький досвід. Враховуючи швидкий розвиток інтернет-технологій, особливо 5G та WebRTC, важливо продовжувати дослідження протоколів передачі відео, їх оптимізацію та стандартизацію, щоб забезпечити найкращий користувацький досвід та відповідність сучасним вимогам. Застосування відкритих стандартів та ініціатив сприяє інноваціям у галузі потокової передачі відео, а також розвитку інтеграції з іншими системами і сервісами.

Моніторинг та діагностика проблем у протоколах потокової передачі відео є важливим аспектом забезпечення стабільної роботи сервісів та задоволення потреб користувачів. Використання передових інструментів моніторингу та вивчення QoE-метрик допомагає виявляти проблеми та оптимізувати роботу систем.

НЕДОЛІКИ ТЕХНОЛОГІЙ PDH ТА ПЕРЕВАГИ SDH

Бабич В’ячеслав Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

В даний час широкого поширення набули дві технології глобальних мереж зв'язку, що використовують оптичне волокно як середовище передачі: PDH - цифрова ієрархія, SDH / SONET - синхронна цифрова ієрархія. Ці технології (PDH і SDH) найбільш широко використовуються на вітчизняній мережі ВСС.

Загальна схема каналу передачі з використанням технології PDH навіть для простої топології мережі "точка - точка", але при швидкості 140 Мбіт / с повинна включати три рівні мультиплексування на передавальній стороні і три рівня демультиплексирования на приймальній стороні, що призводить до досить складною апаратурної реалізації таких систем. Однак суттєве здешевлення цифрової апаратури за останні двадцять років і використання волоконно-оптичного кабелю (ВОК) як середовище передачі привели до того, що PDH набула значного поширення вже у вісімдесяті роки. Ці системи дозволяли здійснити передачу великої кількості каналів високоякісної цифрового телефонного зв'язку

Однак передача даних на швидкості 64 кбіт / с на основі протоколу пакетної комутації X.25 виявила низку недоліків PDH технології. Їх суть в тому, що додавання вирівнюючих біт унеможливлює ідентифікацію і висновок (або введення), наприклад, потоку 64 кбіт / с, або навіть 2 Мбіт / с, "зашитого" в потік 140 Мбіт / с, без повного демультиплексування цього потоку і видалення вирівнюючих біт. Здійснюючи, і досить часто, таке введення / виведення, доводиться проводити відносно складну операцію трирівневого демультиплексирования PDH сигналу з видаленням / додаванням вирівнюють (на всіх трьох рівнях) біт і його подальшого трирівневого мультиплексування з додаванням нових вирівнюють біт.
Інша вузьке місце технології PDH - слабкі можливості в організації службових каналів для цілей контролю і управління потоком в мережі і практично повна відсутність коштів маршрутизації мультиплексованих потоків нижніх рівнів, що вкрай важливо для використання систем PDH в мережах передачі даних.

Недоліки плезіохронних систем передачі і прогрес в технологіях волоконно-оптичних систем, що мають в порівнянні з електричними кабельними системами практично необмежену смугу пропускання і інші переваги ВОСП, стимулювали розробку і впровадження нових цифрових систем передачі інформації.

SDH (Synchronous Digital Hierarchy - синхронна цифрова ієрархія) - сучасна телекомунікаційна технологія, яка призначена для тимчасового мультиплексування і транспортування різних цифрових потоків. Ця синхронна цифрова система дозволяє забезпечити просту, економічну і гнучку інфраструктуру мережі зв'язку.

Принцип роботи SDH заснований на упаковці входять цифрових потоків в віртуальні контейнери, які потім синхронно мультиплексируются і передаються в потрібну точку мережі.

Переваги технології SDH:

1. Висока швидкість передачі інформації
2. Наявність процедури введення-виведення
3. Висока надійність і повний програмний контроль
4. Технологія, розрахована на майбутнє
5. Сумісність

Система управління SDH дає найширші можливості в області моніторингу, адміністрування і оперативної перемаршрутізаціі каналів, забезпечуючи повну автоматизацію процесу експлуатації мережі, дозволяючи часто вирішувати проблеми замовників без виїзду на кінцеві точки каналу. Простота переходу на інші, більш високі рівні ієрархії робить можливим

здійснення розвитку мережі з мінімальними витратами. Стандартизація оптичного інтерфейсу дозволяє з'єднувати обладнання SDH різних виробників.

МЕХАНІЗМИ АВТОМАТИЗОВАНОГО МОНІТОРИНГУ ТА АНАЛІЗУ СТАНУ МЕРЕЖІ

Кузьменко Максим Юрійович
Державний університет телекомунікацій

Механізми автоматизованого моніторингу та аналізу стану мережі - це засоби, які дозволяють виявляти та усувати проблеми в роботі мережевих пристроїв, трафіку та продуктивності. Ці засоби можуть бути розділені на кілька класів, таких як:

Системи управління мережею (Network Management Systems) - централізовані програмні системи, які збирають дані про стан вузлів і комунікаційних пристроїв мережі, а також дані про трафік в мережі. Ці системи не тільки здійснюють моніторинг і аналіз, а й виконують в автоматичному чи напівавтоматичному режимі управління мережею.

Вбудовані засоби моніторингу і аналізу мереж - це програмні або апаратні компоненти, які інтегровані в комунікаційні пристрої мережі, такі як комутатори, маршрутизатори, концентратори тощо. Ці засоби забезпечують збір і надання статистичної інформації про роботу пристроїв та їх портів. Найпоширенішими вбудованими засобами є агенти SNMP (Simple Network Management Protocol) та RMON (Remote Monitoring).

Аналізатори протоколів - це програмні або апаратні засоби, які дозволяють перехоплювати, декодувати і аналізувати кадри і пакети, що передаються по мережевих каналах. Це допомагає виявити помилки в налаштуванні протоколів, конфлікти адрес, несправності обладнання тощо.

Обладнання для діагностики та сертифікації кабельних систем - це апаратні засоби, які дозволяють вимірювати електромагнітним характеристикам кабельних ланок і перевиряти їх на виконання стандартних норм. Таке обладнання включає мережевих аналогових тестеров і кабельних сканерів.

Системи управління мережею (NMS) - це централізовані програмні системи, які збирають дані про стан вузлів і комунікаційних пристроїв мережі, а також дані про трафік в мережі. Ці системи не тільки здійснюють моніторинг і аналіз, а й виконують в автоматичному чи напівавтоматичному режимі управління мережею - включення і відключення портів пристроїв, зміна параметрів мостів адресних таблиць мостів, комутаторів і маршрутизаторів і т.п..

NMS виконує управління мережею за допомогою надсилання команд на мережеві пристрої для зміни їх параметрів або режимів роботи. Наприклад, NMS може автоматично перезавантажити пристрой у разі несправності або переключити трафік на запасний канал у разі перевантаження. NMS також може сповіщати адміністраторів або користувачів про події в мережі за допомогою електронної пошти, SMS або інших способів.

Вбудовані засоби моніторингу і аналізу мереж - це програмні або апаратні компоненти, які інтегровані в комунікаційні пристрої мережі, такі як комутатори, маршрутизатори, концентратори тощо. Ці засоби забезпечують збір і надання статистичної інформації про роботу пристроїв та їх портів.

Аналізатори протоколів - це програмні або апаратно-програмні системи, які перехоплюють і декодують пакети даних, що циркулюють в мережі. Ці системи дозволяють

вивчати вміст пакетів різних протоколів, їх вкладеність, напрямки, джерела і призначення тощо.

Аналізатори протоколів можуть бути самостійним спеціалізованим пристроєм або персональним комп'ютером з спеціалізованою мережевою картою і відповідним програмним забезпеченням. Аналізатори підключаються до мережі точно також як і звичайний вузол. Відмінність полягає в тому що аналізатор може приймати всі пакети даних передавання по мережі тоді як звичайна станція - тільки адресована їй.

Обладнання для діагностики та сертифікації кабельних систем - це спеціалізовані прилади, які дозволяють вимірювати і оцінювати електромагнітні характеристики кабельних ліній, таких як опір, ємність, індуктивність, затухання, перехідне опору тощо. Ці прилади також дозволяють виявляти і локалізувати різні дефекти кабелю, такі як перерви, замикання, пошкодження ізоляції тощо.

Обладнання для діагностики та сертифікації кабельних систем можуть бути самостійним спеціалізованим пристроєм або персональним комп'ютером з спеціалізованою мережевою картою і відповідним програмним забезпеченням. Обладнання підключаються до кабельної мережи точно також як і звичайний вузол. Відмінність полягає в тому що обладнання може генерувати тестові сигнали на вході дроту і аналізувати відбиті сигнали на виході.

Специфіка використання кожного механізму залежить від типу і розміру мережі, що керується, а також від функціональних можливостей самої системи. Загальною метою є покращення продуктивності, надійності і безпеки мережевого середовища. Для цього уже визначені засоби використовують такі дані:

Дані про конфігурацію мережевих пристроїв, їх типи, адреси, версії програмного забезпечення тощо.

Дані про статус мережевих пристроїв, їх доступність, навантаження, температуру тощо.

Дані про трафік в мережі, його обсяг, напрямки, протоколи, джерела і призначення тощо.

Дані про події в мережі, їх час, причини, наслідки тощо.

Збирають цю інформацію за допомогою різних протоколів і методик, таких як SNMP (Simple Network Management Protocol), RMON (Remote Monitoring), NetFlow (Network Flow Analysis), Syslog (System Logging Protocol) тощо. Також можуть використовуватися спеціальними агентами на мережевих пристроях для надсилання даних на сервер NMS.

NMS ,обладнання, аналізатор, вбудовані засоби моніторингу аналізують отриману інформацію за допомогою розумних алгоритмів і правил для виявлення аномалій, помилок, загроз та можливостей для оптимізації мережевого функціонування.Також можуть генерувати звичайні та графічні звіти про стан мережі для адміністратора та користувача.

АНАЛІЗ ПРОТОКОЛІВ ПОТОКОВОЇ ПЕРЕДАЧІ ВІДЕО

Мороз Юрій Анатолійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Аналіз існуючих протоколів для побудови мереж VPN (Віртуальних Приватних Мереж) є центральною темою в галузі кібербезпеки, враховуючи постійно зростаючу потребу в безпечному і приватному доступі до інтернет-ресурсів. Віртуальні приватні мережі дають змогу користувачам створювати зашифровані віртуальні тунелі в мережі Інтернет, що забезпечують конфіденційність, інтегральність та доступність обміну інформацією. Для

встановлення такого безпечного з'єднання використовуються різні протоколи, зокрема PPTP, L2TP/IPsec, SSTP, OpenVPN та WireGuard, кожний з яких має свої особливості, переваги та недоліки.

PPTP (Point-to-Point Tunneling Protocol) був одним з перших протоколів, що були розроблені для підтримки VPN. Його головна перевага полягає в простоті налаштування та широкій сумісності, оскільки він підтримується більшістю операційних систем і мережевого обладнання. Однак PPTP вже не вважається достатньо безпечним для сучасних стандартів, оскільки його алгоритми шифрування можуть бути зламані за допомогою відомих атак.

L2TP (Layer 2 Tunneling Protocol) часто використовується в поєднанні з IPsec для надання вищого рівня безпеки. Протокол L2TP створює тунель, а IPsec забезпечує зашифроване з'єднання всередині цього тунелю. Хоча L2TP/IPsec надає високий рівень безпеки, він може бути повільнішим через складність двократного шифрування.

SSTP (Secure Socket Tunneling Protocol) був розроблений Microsoft і є вбудованим в систему Windows. SSTP використовує технологію SSL/TLS для шифрування трафіку, що забезпечує високий рівень безпеки. Однак він має обмежену сумісність з платформами, що не є Windows, що може бути обмежувальним фактором для деяких користувачів.

OpenVPN - це відкритий протокол VPN, що використовує бібліотеку OpenSSL для шифрування. Він підтримує широкий спектр алгоритмів шифрування і підтримує різні методи аутентифікації. Завдяки своїй гнучкості і високому рівню безпеки OpenVPN вважається одним з найбільш надійних протоколів VPN.

WireGuard - це відносно новий протокол VPN, що має на меті простоту, швидкість, ефективність і безпеку. Він використовує сучасні криптографічні протоколи, такі як:

- ChaCha20 для шифрування: це потоковий шифр, розроблений Деніелем Бернштейном. Він відомий своєю швидкістю та безпекою.
- Poly1305 для автентифікації: це алгоритм MAC (Message Authentication Code), який також був розроблений Бернштейном. Він використовується для перевірки цілісності даних.
- Curve25519 для криптографії з відкритим ключем: це еліптична крива, яка використовується для обміну ключів Діффі-Хеллмана.
- BLAKE2 для хешування: це криптографічний хеш-функція, який надає вищу продуктивність, ніж MD5 та SHA-3.

Ці криптографічні протоколи і алгоритми були обрані через їхню безпеку, швидкість та ефективність і є дуже ефективним з точки зору продуктивності.

На основі проведеного аналізу, протокол OpenVPN видається найбільш привабливим варіантом для більшості сценаріїв використання VPN. OpenVPN забезпечує високий рівень безпеки, включаючи підтримку сучасних алгоритмів шифрування та методів аутентифікації. Крім того, він пропонує високу гнучкість і широку сумісність з різними платформами і обладнанням. Незважаючи на те, що WireGuard може пропонувати кращу продуктивність, OpenVPN вже багато років є стандартом промисловості, і його надійність та стабільність були перевірені часом. Однак, варто зауважити, що кращий вибір протоколу VPN завжди залежить від конкретних вимог та обставин кожного конкретного випадку.

НАПРАВЛЯЮЧІ СИСТЕМИ ВИСОКОШВИДКІСНОГО ОПТОВОЛОКОННОГО ЗВ'ЯЗКУ

Даль І.О.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Направляючі системи високошвидкісного оптоволоконного зв'язку використовуються для забезпечення прямого і точного поширення оптичних сигналів у волоконних кабелях. Вони дозволяють знизити втрати сигналу, забезпечуючи надійну передачу даних на великі відстані.

Також для управління та керування шляхом поширення оптичних сигналів. Вони забезпечують ефективне розподілення сигналів між різними вихідними та приймаючими пристроями, що дозволяє підтримувати високу пропускну здатність та якість передачі даних.

Зачасту для керування положенням та напрямом оптичних волокон. Це дозволяє підтримувати оптимальне зв'язування між волокном та приймачем сигналу, забезпечуючи мінімальні втрати та інтерференцію, що покращує якість передачі сигналу.

Направляючі системи високошвидкісного оптоволоконного зв'язку включають в себе різні компоненти та пристрої, які забезпечують ефективну передачу оптичних сигналів у волоконних мережах. Основні типи направляючих систем включають:

Волоконні розподільні панелі (Fiber Distribution Panels) - Це механічні пристрої, які використовуються для організації та розподілу оптичних з'єднань у волоконних мережах. Вони забезпечують зручний доступ до волоконних кабелів та роз'ємів для підключення та управління.

Оптичні спліттери (Optical Splitters) - Спліттери використовуються для розділення оптичного сигналу на кілька шляхів передачі безпосередньо на волоконних кабелях. Вони забезпечують розподіл сигналу між різними пристроями або волоконними лініями, що дозволяє ефективно використовувати пропускну здатність волоконних кабелів.

Оптичні комутатори (Optical Switches) - Комутатори використовуються для перемикання оптичних шляхів та управління напрямком поширення сигналу. Вони дозволяють змінювати маршрутизацію сигналу, переключаючи його між різними вихідними пристроями або волоконними лініями.

Оптичні фільтри (Optical Filters) - Фільтри використовуються для селективної передачі або блокування певного діапазону хвильових довжин у волоконних системах. Вони дозволяють контролювати спектральні характеристики оптичних сигналів, фільтруючи небажані шуми або сигнали з інших каналів.

Мультиплексори/демультиплексори (MUX/DEMUX) - Ці пристрої використовуються для комбінування (мультиплексування) декількох оптичних сигналів на одному волокні для передачі одночасно, а також розбивання (демультиплексування) сигналу на окремі канали. Вони дозволяють передавати багатоканальні сигнали по одному волокну.

ОПТИМІЗАЦІЯ УПРАВЛІННЯ ТРАФІКОМ В МЕРЕЖАХ СЕРВІС ПРОВАЙДЕРІВ

Михальчишин Т.Ю.
Державний університет телекомунікацій, м. Київ

Сучасні комп'ютерні мережі, запропонувавши дешевий трафік, високу продуктивність, суперстабільні і хорошу конвергентність, позбулися таких привабливих якостей старих технологій, як можливість визначати шлях трафіку і забезпечити якість каналу від початку до

кінця. Навіщо взагалі може знадобитися інжиніринг трафіку? Конвергенція телекомунікаційної мережі, розділення трафіку за допомогою такої технології як MPLS Traffic Engineering. Інжиніринг трафіку є моніторинг та моделювання потоків трафіку, а також управління трафіком для забезпечення потрібної якості його обслуговування шляхом раціонального використання мережевих ресурсів за рахунок збалансованої їх завантаження.

Крім того, для послуг, які вимагають виконання заданих норм якості обслуговування QoS, наприклад, заданого коефіцієнта втрат пакетів і / або затримки / джиттера, інжиніринг трафіку дозволяє забезпечувати належне QoS шляхом призначення явно певних маршрутів.

Можна сказати, що інжиніринг трафіку в MPLS заснований на управлінні наборами атрибутів, значення яких враховуються при виборі маршрутів для створюваних в MPLS мережі LSP і LSP тунелів. Тепер спробуємо описати загальну картину роботи програми TE в MPLS, не заглиблюючись, однак, в подробиці, розгляд яких міг би скласти окрему книгу[1]. Основними компонентами підсистеми TE є:

- призначений для користувача інтерфейс, через який адміністратор може керувати політикою TE;
- IGP компонент, поширює інформацію про топології мережі і відомості про стан мережевих ресурсів;
- маршрутизація на основі обмежень - модуль, який проводить розрахунок маршруту в мережі MPLS на основі інформації, одержуваної від призначеного для користувача інтерфейсу і IGP компонента;
- компонент сигналізації для створення і підтримки LSP (або LSP тунелю), для управління LSP (LSP тунелем) та для бронювання системних ресурсів.
- компонент передачі даних, в якості якого виступає сама мережа MPLS.

Примітивні MPLS TE можна досягти вручну, встановивши тунелі, що відповідають необхідним напрямкам руху. Однак весь спектр заходів MPLS TE виглядає дещо складніше і умовно поділяється на наступні етапи [2].

1. Організація домену MPLS.

Існує конкретна мережева топологія, що складається з набору маршрутизаторів і каналів з певними властивостями між ними.

2. Введення обмежень.

У домені MPLS увімкнено механізм TE та описано мінімальні вимоги до мережі: початкові та кінцеві точки потоку трафіку, графіки маршрутів між ними та методи обчислення маршрутів уздовж них (статичні або динамічні), необхідну пропускну здатність.

3. Вивчення параметрів мережевого середовища.

Для розповсюдження інформації про канали (атрибути посилань) використовується механізм розширення протоколів маршрутизації (протоколи стану зв'язку: IS-IS, OSPF).

4. Розрахунок шляхів трафіку відповідно до адміністративних вимог та можливостей мережі.

5. Встановлення шляхів.

Обчислені шляхи встановлюються в мережі за допомогою спеціального протоколу сигналізації, який може поширювати інформацію про явний маршрут. Сьогодні відомі два такі протоколи: RSVP-ext та CR-LDP.

6. Створення маршрутів з урахуванням тунелів TE.

IGP встановлює маршрут на основі наявності тунелів (як інтерфейси тунелю). Як результат, процес маршрутизації на вхідному маршрутизаторі (head-end) просто управляє тунелями LSP як інтерфейсами. А в таблиці прямих маршрутів буде маршрут до головного хоста з наступним тунелем - TE-тунель.

7. Просування пакетів.

За допомогою механізму MPLS (Label Stacking) забезпечується необхідне тунелювання та розповсюдження пакетів.

Список використаних джерел:

1. How MPLS Traffic Engineering works [Електронний ресурс] – https://community.cisco.com/t5/networkingdocuments/how-mpls-traffic-engineering-works/ta-p/3128593

2. RFC 3945 Generalized Multi-Protocol Label Switching (GMPLS) Architecture [Електронний ресурс] –https://www.protocols.ru/WP/rfc3945/

ОСНОВНІ МЕТОДИ ДОСЛІДЖЕННЯ БЕЗДРОТОВИХ МЕРЕЖ.

Топорков Є.О.
Державний університет телекомунікацій, м. Київ

Бездротові мережі стали невід'ємною частиною сучасного суспільства, забезпечуючи зручну та швидку передачу даних у бездротовому середовищі. Однак це складне завдання, яке вимагає використання різних методів для аналізу, вимірювання та оцінки характеристик бездротових мереж.

Основними методами дослідження бездротових мереж є математичне моделювання, імітаційне моделювання, експериментальні вимірювання та аналіз реальних даних.

Математичне моделювання: Цей метод використовує математичні моделі та алгоритми для вивчення та аналізу різних аспектів бездротових мереж. Математичні моделі дозволяють прогнозувати роботу мережі, оцінювати продуктивність і розраховувати такі параметри, як пропускна здатність і стійкість до перешкод.

Виконання симуляцій: цей метод використовує комп'ютерну програму, яка імітує поведінку бездротової мережі на основі заданих параметрів. Моделювання може відтворювати різні сценарії та умови роботи мережі для оцінки продуктивності, відмовостійкості та ефективності різних протоколів.

Експериментальні вимірювання: Цей метод передбачає фізичне вимірювання і тестування бездротової мережі в реальних умовах. Збираючи дані про продуктивність, пропускну здатність, затримки та інші показники, дослідники можуть оцінити реальну продуктивність бездротових мереж і виявити потенційні проблеми.

Аналіз реальних даних: Це метод обробки та аналізу даних, зібраних з реальних бездротових мереж. Статистичні методи можна використовувати для виявлення тенденцій, встановлення залежностей і висновків про продуктивність мережі та якість обслуговування.

Висновок.

Дослідження бездротових мереж вимагає використання різних методів, включаючи математичне моделювання, імітацію, експериментальні вимірювання та аналіз реальних даних. Ці методи дозволяють аналізувати і оцінювати продуктивність, гнучкість і ефективність бездротових мереж, сприяючи подальшому вдосконаленню і розвитку цієї технології.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛЕТАЛЬНИХ АПАРАТІВ ДЛЯ ВИКОНАННЯ СТРАТЕГІЧНИХ ЦІЛЕЙ

Муравчик Кирило Станіславович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Безпілотний літальний апарат в подальшому (БПЛА). На сьогоднішній день ми маємо широкий спектр використання цього пристрою починаючи від аграрної промисловості , зйомки відео, наукових досліджень , простих розваг закінчуючи військовою сферою діяльності . Вдаючись у конкретику дій даного пристрою в аграрній промисловості він допомагає людині обробити певні ділянки землі поливаючи хімічними домішками усю площину та довжину поля , проводити розвідку по всій лінії розмежування поля, допомагаючи тим самим слідкувати за ростом поливанням та доглядом продукції. У військовій же сфері діяльність БПЛА в полягає у розвідці, транспортуванні певних засобів та ураженню живої сили противника.

Варіанти виготовлення БПЛА залежать від дій та сфери використання в якій він буде безпосередньо використовуватись . Основними складовими для виготовлення БПЛА є:

1. Корпус це основна частина конструкції , яка утримує всі компоненти разом . Вона може бути виготовлена з легких композитних матеріалів або металу.
2. Електронне керування здійснюється шляхом так би мовити комп’ютерною системою яка включає в себе наявність мікроконтроллерів , сенсори , гіроскопи , акселерометри та інші пристрої для збору і обробки даних , також для керування польотом.
3. Автопілот це пристрій або програмне забезпечення , яке використовується для автоматичного керування польотом БПЛА . Воно приймає дані з сенсорів та прийомника GPS і видає команди для керування повітряними керувальними пристроями.
4. Бортові системи служать для комунікації які дають змогу користувачу передавати дані між БПЛА та наземними станціями керуванням або іншими платформами.
5. Енергозабезпечення БПЛА може бути реалізовано шляхом паливних мастил або електричних джерел живлень (батарейки, акумулятори).
6. Двигуни, багато БПЛА оснащені електричними двигунами , хоча у деяких моделях можуть використовуватись турбінні двигуни або інші типи . Двигуни забезпечують тягу для польоту та маневреності.
7. Пристрої спостереження , це можуть бути камери , теплові чи інші сенсори , які використовуються для збору інформації та спостереження з повітря.

Данні БПЛА на сьогоднішній день використовуються безпосередньо для виконання бойових завдань у зоні бойових дій. Прийнятий на озброєння Збройними Силами України а також Службою Зовнішньої Розвідки.

На даному фото ми можемо бачити як інженер розробив та сам сконструював БПЛА.

У підсумку можна сказати що на сьогоднішній день сфера діяльності БПЛА набирає шалених обертів та сфер використання. Щодня мільйони спеціалістів вдосконалюють та модернізують пристрій вигадуючи все нові та нові ідеї . Тому я особисто вважаю це дуже гарною перспективою на майбутнє та сподіваюсь що на сьогодні світ, вже має певні технічні документації для транспортування необмеженої кількості фізичної ваги а також ще більш значних успіхів у військовій сфері.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ВОЛОКОННО-ОПТИЧНИХ СИСТЕМ ЗВ'ЯЗКУ

Самойленко Євген Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

На сьогоднішній день Україна все більше і більше розвиває свою інфраструктуру волоконно-оптичних ліній зв'язку. Волоконно-оптичні лінії систем зв'язку зазвичай розташовані під землею або морським дном, щоб захистити їх від зовнішніх впливів і забезпечити надійність передачі даних. Тому фізичний доступ до волоконно-оптичних ліній обмежений і контролюється операторами зв'язку. Якщо вам потрібен доступ до волоконно-

оптичних ліній для цілей управління або обслуговування, вам потрібно зв'язатися з оператором зв'язку або провайдером послуг Інтернету в вашому регіоні. Вони зможуть надати вам інформацію про наявні місця доступу або організувати зустріч для обговорення вашого запиту. Волоконно-оптичні системи зв'язку (ВОСЗ) мають декілька особливостей, які роблять їх привабливими для передачі даних на великі відстані. Ось деякі з них:

1. Висока пропускна здатність: ВОСЗ забезпечують велику пропускну здатність, що дозволяє передавати великі обсяги даних з високою швидкістю. Вони здатні передавати сотні гігабітів або навіть терабітів даних за секунду.

2. Висока якість сигналу: ВОСЗ дозволяють передавати сигнали на великі відстані з дуже малою втратою сигналу. Фіброву структуру легко ізолювати від електромагнітних перешкод, що дозволяє зменшити спотворення сигналу і забезпечити стабільну якість передачі.

3. Великі відстані передачі: Волоконно-оптичні лінії дозволяють передавати сигнали на великі відстані без необхідності в посилюванні сигналу посередині. Це дозволяє покрити значні території без втрати якості сигналу.

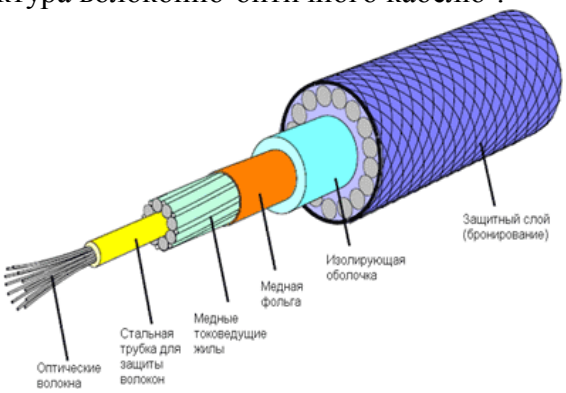
4. Малі розміри та вага: Волоконно-оптичні кабелі мають значно меншу вагу та розміри порівняно з традиційними мідними кабелями. Це спрощує їх установку та розгортання, а також зменшує необхідний простір для монтажу.

5. Висока стійкість: Волоконно-оптичні кабелі відносно стійкі до зовнішніх впливів, таких як електромагнітні перешкоди, радіочастоти, інтерференція та вологість. Вони також відносно стійкі до впливу механічних пошкоджень, таких як розриви кабелю.

6. Безпека: Волоконно-оптичні системи зв'язку не випромінюють електромагнітні сигнали, що робить їх відносно безпечними для здоров'я і нечутними для перехоплення зовнішніми пристроями.

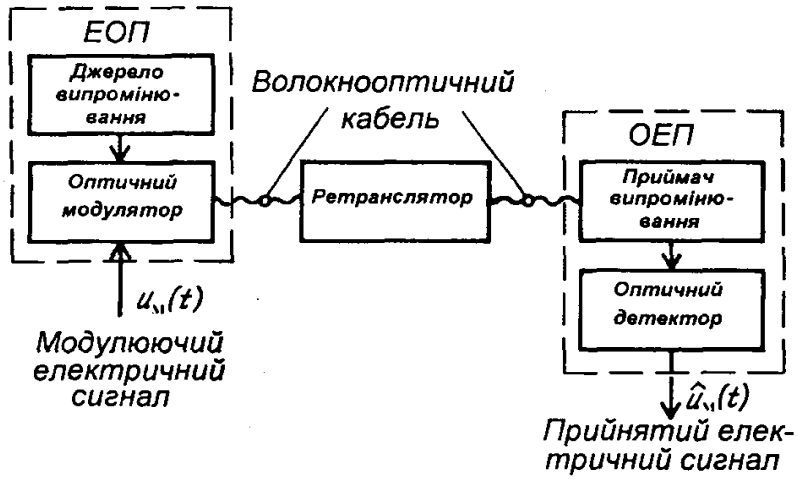
Ці особливості роблять волоконно-оптичні системи зв'язку привабливими для широкого спектру застосувань, включаючи телекомунікації, Інтернет, кабельне телебачення, мережі зв'язку даних, медичні дослідження та багато іншого.

З чого складається структура волоконно-оптичного кабелю ?



1. Захисний шар (бронювання)
2. Ізолююча оболонка
3. Мідна фольга
4. Мідні струмопровідні жили
5. Стальна трубка для захисту волокон
6. Оптичні волокна

Також в Інтернеті є маса структурних схем з’єднань завдяки волоконно-оптичному кабелю



Волоконно-оптичні системи зв'язку (ВОСЗ) використовуються широко по всьому світу і застосовуються у багатьох галузях. Ось деякі з них:

1. Телекомунікації: ВОСЗ є основним засобом передачі голосу, даних і відео в телефонних мережах, мобільних мережах, широкосмуговому інтернеті та інших телекомунікаційних системах.

2. Інтернет: Більшість міжнародного мережевого трафіку передається через волоконно-оптичні лінії, що забезпечує високу швидкість та надійність передачі даних.

3. Кабельне телебачення: ВОСЗ використовуються для передачі каналів телебачення високої якості з великим обсягом даних.

4. Мережі зв'язку даних: ВОСЗ використовуються для побудови приватних мереж зв'язку даних у бізнес-секторі та установах, що потребують великої швидкості передачі даних і високої надійності.

5. Медичні дослідження: ВОСЗ використовуються для передачі медичних даних, зображень, відео та інших важливих інформаційних потоків у медичних установах і дослідницьких центрах.

6. Банківські та фінансові послуги: Волоконно-оптичні мережі забезпечують безпечну і швидку передачу фінансових даних між банками, фінансовими установами та трейдерськими платформами.

7. Індустріальні застосування: ВОСЗ використовуються у промислових системах контролю та автоматизації, таких як системи моніторингу, керування та дистанційного управління.

Це лише кілька прикладів галузей, де використовуються волоконно-оптичні системи зв'язку. ВОСЗ продовжують розширюватись і знаходити нові застосування в різних сферах життя і бізнесу.

Тому підсумовуючи усі аспекти волоконно-оптичних систем зв’язку можна зробити наступний висновок. ВОСЗ є ефективним і надійним засобом передачі даних на великі відстані, що допомагає підтримувати зв'язок і обмін інформацією у сучасному світі. Постійний розвиток технологій волоконно-оптичних систем зв'язку сприяє подальшій їхній інтеграції в різні сфери, покращенню швидкості передачі даних і розширенню можливостей комунікаційних мереж.

ОСОБЛИВОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ В XXI СТОЛІТТІ

Поддубний Ярослав
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Зростання швидкості передачі даних - у 21 столітті спостерігається стрімкий розвиток технологій передачі даних, що призводить до значного збільшення швидкості передачі. Високошвидкісні мережі забезпечують ефективне спілкування та передачу великих обсягів інформації.

Безпроводові технології - запровадження безпроводових технологій, таких як Wi-Fi, Bluetooth, мобільні мережі, дозволяє людям підключатись до інтернету та комунікувати між собою з будь-якого місця. Це сприяє мобільності та гнучкості спілкування.

Розвиток інтернету речей (IoT) - у 21 столітті телекомунікаційні системи використовуються для підключення мільярдів різних пристроїв, що становлять Інтернет речей. Це дозволяє збирати, обробляти та обмінюватися даними між пристроями, що відкриває нові можливості в автоматизації, збереженні енергії та покращенні якості життя.

Висока надійність і кібербезпека - у зв'язку зі зростанням кількості підключених пристроїв і обсягів передачі даних, надійність та кібербезпека стають важливими аспектами телекомунікаційних систем. Інженери займаються розробкою та впровадженням заходів для забезпечення безпеки мереж та захисту від кібератак.

Розширення мережової інфраструктури - розвиток телекомунікаційних систем вимагає постійного розширення мережової інфраструктури, включаючи побудову нових базових станцій, супутникових систем, оптоволоконних мереж та інших засобів передачі сигналу. Це дозволяє забезпечити швидкий та надійний доступ до комунікаційних послуг.

Використання хмарних технологій - хмарні технології стають все більш поширеними в телекомунікаційних системах, дозволяючи зберігати та обробляти великі обсяги даних в розподіленому середовищі. Інженери розробляють та впроваджують інфраструктуру хмарних обчислень для забезпечення доступу до даних та послуг з будь-якого місця.

Вплив 5G технологій - впровадження технології 5G в сучасні телекомунікаційні системи дозволяє забезпечити вищу швидкість передачі даних, низьку затримку і велику масштабованість. Це створює передумови для розвитку інноваційних послуг, таких як розширена реальність, автономні транспортні системи та інші.

Віртуалізація та програмне забезпечення - застосування віртуалізації та програмного забезпечення в телекомунікаційних системах дозволяє забезпечити гнучкість, швидкість розгортання та ефективне управління ресурсами. Інженери працюють над впровадженням концепцій софтверної мережі (SDN) та мережі функцій віртуалізації (NFV).

Розвиток мереж Інтернету нового покоління (NGN) - NGN є еволюційним кроком у розвитку телекомунікаційних мереж, який об'єднує голосові, даних та відео комунікації в єдину IP-мережу. Це забезпечує інтеграцію різних сервісів та високу якість зв'язку для користувачів.

Розширення мобільних додатків та послуг - розробка мобільних додатків та послуг стала невід'ємною частиною телекомунікаційного сектору. Інженери створюють нові платформи та інфраструктуру для розробки та розгортання мобільних додатків, таких як мобільний банкінг, медичні послуги на відстані та інші.

Кіберфізичні системи - взаємодія між фізичними та кібернетичними системами стає все більш значущою. Інженери працюють над розробкою інтегрованих систем, які поєднують сенсори, актуатори та зв'язок, що відкриває нові можливості в сферах таких як автономні автомобілі, розумні міста та індустрія 4.0.

Ці тези надають загальний огляд основних особливостей телекомунікаційних систем та мереж у 21 столітті. Розробка та впровадження нових технологій інженерами допомагають забезпечити ефективну комунікацію та передачу даних у сучасному світі.

РОЗВИТОК ТЕЛЕКОМУНІКАЦІЙНОЇ ГАЛУЗІ В УМОВАХ ВІЙНИ

Пелепей М.М.
Навчально-науковий інститут телекомунікацій
Державний університет телекомунікацій

Телекомунікаційна галузь відіграє важливу роль у сучасному світі, забезпечуючи швидкий та надійний обмін інформацією. Умови війни поставляють певні виклики перед розвитком телекомунікаційної інфраструктури, але водночас стимулюють її подальше вдосконалення. У даному рефераті розглянемо вплив війни на розвиток телекомунікаційної галузі, основні тенденції та важливі аспекти, які необхідно враховувати в умовах конфлікту.

1. Роль телекомунікаційної галузі в умовах війни

Телекомунікаційна галузь має велике значення для забезпечення ефективного зв'язку під час військових дій. Вона дозволяє оперативно обмінюватися інформацією між військовими підрозділами, координувати дії та приймати стратегічні рішення. Також важливою функцією телекомунікаційного зв'язку є забезпечення зв'язку з цивільними структурами, що дозволяє ефективно організовувати гуманітарну допомогу та координацію дій під час кризових ситуацій.

2. Виклики для телекомунікаційної галузі в умовах війни

Умови війни поставляють перед телекомунікаційною галуззю низку викликів, з якими необхідно ефективно впоратися. Один з основних викликів - це збереження надійності та стійкості мережі зв'язку. Воєнні дії можуть призвести до пошкодження комунікаційних ліній, обладнання та інфраструктури. Тому необхідно приділити особливу увагу резервним системам зв'язку, розташуванню об'єктів у безпечних місцях та швидкому відновленню зв'язку після пошкоджень.

Також важливим викликом є захист інформації від несанкціонованого доступу. Умови війни характеризуються підвищеним рівнем кібератак та розвідки. Тому телекомунікаційна галузь повинна розвивати та впроваджувати сучасні методи захисту даних, шифрування та системи виявлення вторгнень.

3. Розвиток телекомунікаційної галузі в умовах війни

Умови війни спонукають до активного розвитку телекомунікаційної галузі та вдосконалення існуючих технологій. Воєнні конфлікти стимулюють виникнення нових інновацій та технологічних рішень, оскільки постійна потреба у швидкому та безперебійному зв'язку вимагає нових рішень.

Одним з напрямків розвитку є вдосконалення бездротових комунікаційних технологій. Воєнні операції часто відбуваються в рухомих умовах, тому мобільність та швидкість передачі даних мають вирішальне значення. Розвиток бездротових технологій дозволить підвищити мобільність військових підрозділів та забезпечити швидку передачу інформації на полі бою.

Крім того, значну роль грають супутникові комунікації. Супутникові системи забезпечують глобальний охоплення та надійний зв'язок, що особливо важливо в умовах війни, коли існує ризик знищення земних комунікаційних ліній. Постійний розвиток супутникових технологій дозволяє покращувати якість та пропускну здатність сигналу, а також зменшувати затримки в передачі даних.

Висновок

Умови війни поставляють перед телекомунікаційною галуззю великі виклики, проте вони також стимулюють розвиток нових технологій та покращення існуючої інфраструктури. Забезпечення ефективного та безперебійного зв'язку військових та цивільних структур є критично важливим для успішного ведення військових операцій та координації дій. Розвиток бездротових технологій, супутникового зв'язку та забезпечення кібербезпеки є основними напрямками розвитку телекомунікаційної галузі в умовах війни.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МЕТОДУ КОВЗАЮЧОГО СЕРЕДНЬОГО ДЛЯ ПРОГНОЗУВАННЯ СЕЗОННОСТІ ЗА ДОПОМОГОЮ ARMA-МОДЕЛЕЙ

Цибенко М.Ю.,
Державний університет телекомунікацій,
Навчально-науковий інститут телекомунікацій

Питання прогнозування для більшості компаній та бізнесів – є їх основою, адже потрібно планувати поставки, оренду приміщень та залучення додаткових ресурсів. Основними показниками продуктивності компаній, на які покладаються аналітики та бізнес, мають суттєву залежність від сезонності. Методів прогнозування з урахуванням сезонності є досить багато, але одними з найпопулярніших є метод ковзаючого середнього та експотенційного згладжування [1].

Прогнозування з урахуванням сезонності методом ковзаючого середнього є популярним підходом у аналізі часових рядів. Цей метод дозволяє виявити та врахувати повторювані сезонні залежності у даних для отримання більш точних прогнозів [2, с.11].

Метод ковзаючого середнього (англ. Moving Average) полягає у використанні середнього значення попередніх спостережень для прогнозування майбутніх значень. При цьому враховується сезонність, шляхом зміщення та обчислення середнього значення в межах певного діапазону, який охоплює певний період сезонності. Існує велика кількість модифікацій цього методу, але основним недоліком є однакова вага, як нових даних, так і старих, хоча більш нові дані, особливо, коли мова про продажі, мають мати більшу вагу [2, с. 12].

Одним з методів підвищення ефективності є моделі авторегресійного ковзаючого середнього (ARMA). Підхід передбачає забезпечення обробки більш ніж однієї вхідної серії через багатовимірну модель [3, с. 84].

Для використання даного методу необхідно обрати модель ARMA, де AR – авторегресійна частина, а MA – ковзаюче середнє.

Розглянемо ARMA (p, q), де p – порядок авторегресії, а q – порядок ковзаючого середнього, для визначення цих параметрів використовують автокореляційну функцію (ACF) та часткову автокореляційну функцію (PACF), що допомагають визначити лаги в часовому ряду, де p визначається за кількістю значущих лагів в PACF, q – за значущими лагами в ACF [3, с. 84].

Перевагами даного методу є те, що ARMA модель враховує як попередні значення ряду, так і ковзаюче середнє, що враховує попередні похибки, окрім того, ця модель надає кращу апроксимацію часового ряду для даних зі складними структурами та залежностями.

Висновки

У підсумку, для підвищення ефективності методу ковзаючого середнього можна використовувати ARMA моделі, що дають більш точніші результати та дають змогу врахувати додаткові фактори, які впливають на сезонність.

Список використаних джерел

1. James D. Hamilton, Time Series Analysis, 1994, pp.15.
2. Rob J. Hyndman, George Athanasopoulos Forecasting: Principles and Practice, 2013, pp. 11-13.
3. Robert H. Shumway, David S. Stoffer Time Series Analysis and Its Applications: With R Examples, 2000, pp. 84-86.

ПРИНЦИП ПОБУДОВИ IT МОНІТОРИНГУ КОРПОРАТИВНИХ СЕРВІСІВ КОМПАНІЇ

Денік Павло Олексійович
Державний університет телекомунікацій

Успіх і розвиток сучасних компаній багато в чому залежить від стабільності та захищеності IT-інфраструктури. Чим частіше в компанії відбуваються збої, простої після атак, тим більшою є вірогідність, що це призведе до проблем в бізнес-процесах.

Моніторинг IT-інфраструктури – важливий процес, який допомагає організаціям відстежувати зміни в їх IT-інфраструктури. Мета моніторингу – збір та аналіз даних по IT-сервісах і компонентах інформаційної інфраструктури та використання цих даних для контролю всіх її елементів, а також запобігання збоїв і поломок.

Щоб зменшувати вірогідність простою сервісів, компаніям необхідно відмовлятися від старих бізнес-процесів, оцифровувати їх, впроваджувати нові регламенти бізнес-процесів та системи моніторингу обладнання, на зразок Service Manager, CRM, Solarwinds Orion. Без особливої підготовки і захисту корпоративної мережі, всі збої в її роботі несуть за собою проблеми репутаційного та фінансового плану. Саме це і потребує від власників компанії впровадження сучасних методів регулювання та усунення технічних проблем у роботі корпоративного IT сегменту компанії, завданням якого є забезпечення прибутку компанії своєю безперебійною роботу в її клієнтів.

Service Manager - продукт для автоматизації процесів експлуатації IT сервісів на підприємствах. Використовується для створення, опрацювання та контролювання виконання інцидентів та звернень користувачів сервісів компанії з боку відповідальних за виконання бізнес-процесу.

SolarWinds Orion - це потужна масштабована платформа моніторингу та управління інфраструктурою, призначена для спрощення IT-адміністрування для локальних, гібридних середовищ і середовищ програмного забезпечення як послуги (SaaS) в одній панелі.

Система управління взаємовідносинами з клієнтами (Customer Relationship Management) — прикладне програмне забезпечення для організацій, призначене для автоматизації стратегій взаємодії із замовниками (клієнтами), зокрема, для підвищення рівня продажів, оптимізації маркетингу та покращення обслуговування клієнтів шляхом збереження інформації про

клієнтів та історії взаємовідносин з ними, встановлення та покращення бізнес-процесів та подальшого аналізу результатів.

Використання однієї з вказаних системи регулювання бізнес-процесів та сучасної системи моніторингу IT інфраструктури дозволяє побудувати чіткий та безперебійний процес моніторингу, контролю та опрацювання стану всього обладання IT мережі компанії з його подальшою ескалацією на відповідальних осіб, з використанням платформи управління процесами есплуатації IT сервісів Service Manager.

Головним елементом цього процесу є підрозділи зміни моніторингу та регулювання бізнес-процесів. Перші – виконують приймання та опрацювання звернень від користувачів (CRM) і даних з системи моніторингу (SolarWinds) з подальшою ескалацією отриманих даних про проблеми в роботі інфраструктури на обслуговуючих технічних спеціалістів через Service Manager. Другі – контролюють виконання вказаних звернень в системі Service Manager згідно затверджених регламентом термінів та виконують подальшу їх ескалацію у разі порушення цих термінів.

ПРОЄКТУВАННЯ МЕРЕЖ 5G З ІНТЕГРАЦІЄЮ БЛОКЧЕЙН

Гирба Олеся Федорівна
Дмитренко Володимир Віталійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Можливість інтеграції 5G з технологією блокчейн призведе до появи самопідтримуваної, самообслуговуваної та самокерованої мережі, яка може здійснювати транзакції, обробляти автоматично запити та безпечно підзавантажувати оновлення без необхідності підключення до центрального елемента[1].

Структура блокчейн допомогая новому поколінню розподілених безпроводових мереж забезпечити безперебійне надання доступу між різнорідними вузлами. З блокчейн, положення та угоди між вузлами доступу, мережами, і абоненти узгоджуються на льоту, як digital smart контракти. Блокчейн дозволяє пристроям у мережі обирати найкращу послугу з оператором мережі, який потім буде виконувати доступ до неї за допомогою смарт-контракту. Ця модель дозволяє надавати індивідуальні послуги окремим елементам (вузлам) в мережі, що призводить до появи нових моделей тарифікації та бізнес-моделей у мережі 5G. Крім того, інтеграція різних технологій призводить до розгортання нової базової архітектури, яка поступово замінює функції поточного ядра Evolved Packet Core (EPC) [2].

Оскільки архітектура 5G все ще перебуває на стадії розгортання, важливо інтегрувати основний функціонал блокчейн вже, до повної реалізації потенціалу мереж 5G (рис.1). Окрім переваг інтегрування технології блокчейн у мережі 5G, варто підкреслити, що сама технологія 5G дозволяє широко використовувати нові та абсолютно оновлені телекомунікаційні рішення. Наприклад, 5G прискорює впровадження IoT, забезпечуючи повсюдне підключення датчиків та сенсорів за рахунок низьких витрат енергії та низької вартості елементів[3].

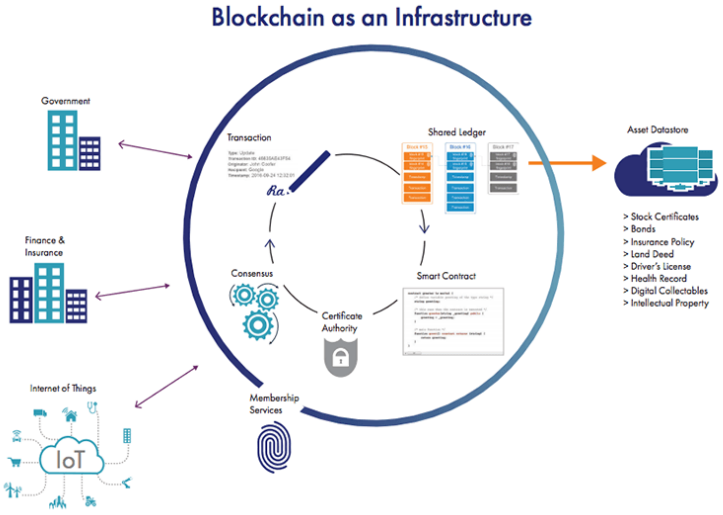


Рис.1. Приклад інтеграції блокчейн в телекомунікаційну інфраструктуру

Крім того, інтегрування блокчейн з 5G та з додаванням штучного інтелекту (AI, або ШІ), формується новий набір технологій, які здатні прискорити впровадження новітніх IT та ТК рішень. 5G має на меті забезпечити високу швидкість передачі даних, покриття, підключення та пропускну здатність із значним зменшенням затримки та енергії споживання.

Перелік посилань

1. B.Mafakheri, T.Subramanya, L.Goratti, R.Riggio. Blockchainbased infrastructure sharing in 5G small cell networks. 14th Int. Conf. Netw. Service Manage. (CNSM). Pp.313–317. 2019.

2. Blockchain in Telecoms. [Електронний ресурс] –Режим доступу: https://www.omdia.com/resources/product-content/blockchain-intelecoms-spt001-000029

3. D. T. Hoang, D. Niyato, D. N. Nguyen, E. Dutkiewicz, P. Wang, Z. Han. A dynamic edge caching framework for mobile 5G networks. IEEE Wireless Commun. Vol. 25. Pp. 95–103. 2018.

4. Cedric Dib. Blockchain technology in the telecom industry. [Електронний ресурс] – Режим доступу: https://www.rcrwireless.com/20180910/opinion/readerforum/blockchain-telecom-part1-reader-forum

ГОЛОВНИЙ ЧАТ-БОТ В TELEGRAM

Прокопець Дана Сергіївна
Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій
м. Київ

Месенджер Telegram був створений Павлом Дуровим у 2013 році. З тих пір соціальна мережа завоювала велику аудиторію, яка на сьогоднішній день сягає більше, ніж 700 млн

активних користувачів на місяць. Сама платформа входить в різноманітні ТОПи та рейтинги за популярністю, кількістю скачувань з Play Market та AppStore.

До 2015 року це був звичайний месенджер, в якому не було нічого особливого та унікального, що відрізняло б його з-поміж інших аналогічних додатків. Але в 2015 році влітку відбувся справжній прорив: світ побачив перший Telegram-бот. Навряд чи хтось зараз згадає, як називався той самий перший чат-бот у Telegram, яким функціоналом був наділений та чи був по-справжньому популярним. Але сьогодні ми поговоримо не про нього, а про того бота, який вже не перший рік допомагає системі створювати нових самобутніх чат-ботів. Ім'я йому - @BotFather (по аналогії з «GodFather» – «Хрещений батько», фільм 1971-го року). На Рисунку 1.1 показано інтерфейс чату з даним ботом та частину команд, на які він вміє реагувати.

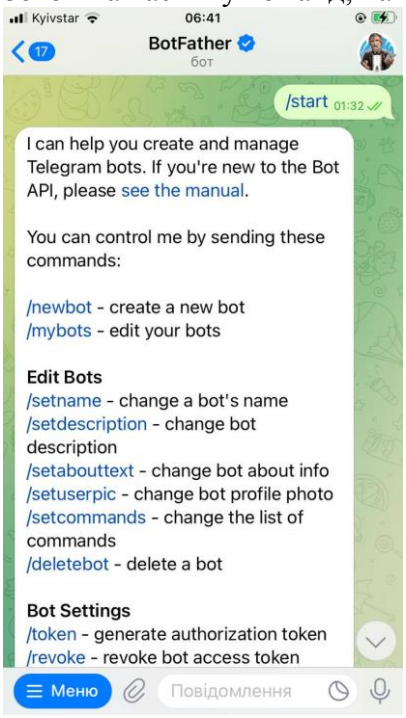


Рисунок 1.1 – Telegram-бот @BotFather

Основне призначення даного боту полягає в тому, що коли користувач хоче створити свій Telegram-бот, він звертається до @BotFather, аби той створив йому каркас для даного чат-боту, дав можливість записати назву, змінити опис створюваного каналу або поставити нове фото на аватарку боту. Але найкрутіша з його функцій в тому, що він надає унікальний набір символів (так званий токен) кожному окремо взятому каналу. Цей токен не лише дозволяє ідентифікувати бот в системі, але й за його допомогою захищає людей від шахраїв та хакерів, унеможливлюючи будь-які спроби проникнути всередину бота. Павло Дуров на стільки впевнений в безпеці своєї технології, що пообіцяв тому, хто зможе хакнути його розробку, отримаю грошову винагороду. За 8 років досі нікому це не вдалось.

Незважаючи на те, яким способом створюється бот – за допомогою конструктора чат-ботів або шляхом написання коду в програмному середовищі – в обох випадках розробник звертається до бота, аби створити оболонку для нього. В деяких випадках за допомогою @BotFather можна здійснювати повний контроль над роботою чат-боту, але за умови, що той бот, який розробляється, був задуманий для виконання простих функцій.

Розглядаючи @BotFather як частину однієї комплексної технології по розробці чат-ботів, в майбутньому ця технологія здатна вирішити багато проблем. Зокрема, це допоможе зекономити людям багато робочого часу, оскільки боти братимуть на себе виконання рутинних процесів. Це допоможе автоматизувати та/або оптимізувати різні процеси на виробництві, в бізнесі, в сфері надання послуг, в комерції тощо.

Список використаних джерел
1. https://botcreators.ru/blog/botfather-instrukciya/
2. https://sendpulse.com/ru/knowledge-base/chatbot/telegram/create-telegram-chatbot

РОЛЬ ХМАРНИХ ТЕХНОЛОГІЙ У ТЕЛЕКОМУНІКАЦІЯХ: ВИКЛИКИ ТА МОЖЛИВОСТІ

Тур О. І.
Державний університет телекомунікацій, м. Київ

В умовах швидко розвитку ринку ІТ-підприємств, існує великий попит на гнучкі інфраструктурні рішення. Впровадження нових послуг та сервісів потребує швидкого маштабування. Тому рух до агільної та гнучкої інфраструктури все частіше охоплює процес трансформації телекомунікаційних компаній, які рухаються від традиційних статичних інфраструктур до більш адаптивних, агільних та гнучких моделей, заснованих на хмарних технологіях. Розгортання хмарних рішень у телекомунікаційному секторі відкриває нові можливості та приводить до значних змін у підходах до проектування, будівництва та управління інфраструктурою.

Однією з головних переваг хмарних технологій є їх здатність забезпечувати гнучкість та агільність. Замість традиційних фізичних серверів та обладнання, хмарні рішення базуються на віртуалізації, де ресурси можуть бути швидко масштабовані в залежності від потреб користувачів. Це дозволяє телекомунікаційним компаніям пристосовуватись до змінних вимог ринку та ефективно використовувати ресурси.

Хмарні технології також сприяють збільшенню швидкості впровадження нових послуг та інновацій. За допомогою хмарних рішень, телекомунікаційні компанії можуть легко розгортати та масштабувати нові сервіси, прискорюючи час до введення їх на ринок. Це дозволяє отримувати перевагу над конкурентами і задовольняти зростаючі потреби користувачів швидше та ефективніше.

Однак, існують виклики, пов'язані з розгортанням хмарних технологій у телекомунікаціях. Забезпечення безпеки та конфіденційності даних є однією з найважливіших проблем. Телекомунікаційні компанії повинні приділяти увагу захисту інформації, особливо при використанні публічних хмарних сервісів. Крім того, інтеграція хмарних рішень з наявною інфраструктурою та системами може вимагати додаткових зусиль та розробки стандартів та протоколів для забезпечення сумісності та безперебійної роботи.

У майбутньому, розвиток хмарних технологій у телекомунікаціях буде спрямований на дослідження та вдосконалення моделей безпеки для хмарних телекомунікаційних сервісів. Також буде акцентовано на використання штучного інтелекту та машинного навчання для оптимізації та автоматизації управління хмарними інфраструктурами.

Розгортання хмарних технологій у телекомунікаціях відкриває широкі перспективи для розвитку сектору, надаючи більшу гнучкість, агільність та можливість швидкого впровадження нових послуг. Проте, успішна реалізація цих технологій вимагає вирішення викликів, пов'язаних з безпекою та інтеграцією. Подальші дослідження та розвиток хмарних технологій у телекомунікаціях будуть спрямовані на забезпечення надійності, ефективності та інноваційного росту в цій галузі.

Розвиток телекомунікаційного сектору через хмарні технології відкриває широкий спектр можливостей для трансформації та просування телекомунікаційної галузі за допомогою використання хмарних технологій. Впровадження хмарних рішень дозволяє

телекомунікаційним компаніям не лише оптимізувати існуючі процеси, але й розширити свої можливості та надати нові інноваційні послуги. Ось кілька аспектів, які можуть бути розглянуті при розкритті цієї теми:

Розширення послугового портфоліо:

Хмарні технології відкривають нові можливості для телекомунікаційних компаній щодо надання додаткових послуг. Наприклад, вони можуть розгорнути хмарні обчислення та забезпечити віртуальну приватну мережу (VPN) для підприємств, що дозволить їм зберігати та обробляти дані в безпечному хмарному середовищі.

Масштабування та еластичність:

Хмарні технології дозволяють телекомунікаційним компаніям масштабувати свою інфраструктуру залежно від потреб користувачів. Це забезпечує гнучкість та еластичність у використанні ресурсів, дозволяючи збільшувати або зменшувати обсяги обчислювальних потужностей та мережевих ресурсів в залежності від попиту.

Підвищення ефективності та оптимізація витрат:

Впровадження хмарних технологій дозволяє телекомунікаційним компаніям оптимізувати використання ресурсів, що призводить до підвищення ефективності та зниження витрат. Вони можуть спільно використовувати ресурси та інфраструктуру, що дозволяє економити кошти на обладнанні та управлінні.

Розвиток 5G та IoT:

Хмарні технології є ключовим фактором для розвитку 5G та Інтернету речей (IoT). Вони забезпечують інтеграцію та управління великим обсягом даних, що генеруються пристроями IoT, а також забезпечують швидку передачу даних у високошвидкісних 5G мережах.

Хмарні обчислення стали перспективним підходом до оренди великої IT-інфраструктури на короткостроковій основі. Оператори хмарних сервісів "Інфраструктура як послуга" (IaaS), таких як Amazon EC2, дозволяють своїм клієнтам розподіляти, отримувати доступ і контролювати набір віртуальних машин (ВМ), які працюють у їхніх центрах обробки даних, і стягувати плату лише за той період часу, протягом якого ці машини працюють лише за період часу, на який виділені машини.

Віртуалізована природа хмари допомагає створювати нові перспективні сценарії використання для ефективної паралельної обробки даних. Однак це також створює нові виклики.[1] Розвиток хмарних технологій в телекомунікаціях не здійснюється без певних проблем і викликів, які потрібно вирішувати. Ось кілька ключових проблем, пов'язаних з розвитком хмарних технологій:

Безпека даних: Забезпечення безпеки даних є однією з найбільших проблем у хмарних технологіях. Передача та зберігання конфіденційної інформації у хмарному середовищі може бути піддаються ризикам, таким як несанкціонований доступ до даних, атаки зламу та витоки інформації. Розробники хмарних рішень та користувачі повинні зосередитися на використанні потужних механізмів шифрування, аутентифікації та контролю доступу для захисту даних у хмарному середовищі.

Надійність та доступність: Відмова у роботі хмарних сервісів або перебої в роботі можуть призвести до серйозних наслідків для користувачів. Телекомунікаційні компанії повинні забезпечувати високий рівень надійності та доступності своїх хмарних інфраструктур шляхом використання резервування ресурсів, географічної реплікації та механізмів відновлення.

Масштабованість та продуктивність: Хмарні технології повинні бути здатні масштабуватися відповідно до зростаючих потреб користувачів. Високе навантаження на хмарну інфраструктуру, обмежені ресурси або недостатня продуктивність можуть стати перешкодою для задоволення потреб користувачів. Розробники хмарних рішень повинні вдосконалювати механізми масштабування та оптимізації продуктивності, щоб забезпечити ефективне використання ресурсів.

Відповідність правовим нормам: Хмарні технології залучають увагу стосовно відповідності до правових норм, таких як захист персональних даних, регулювання конфіденційності та відповідальність за порушення безпеки даних. Телекомунікаційні компанії повинні бути відповідальними щодо забезпечення дотримання цих норм та стандартів у своїх хмарних рішеннях.

Вендор-локінг: Використання певних хмарних платформ може призвести до залежності від конкретного вендора, що ускладнює перехід до інших рішень або зміну постачальника послуг. Телекомунікаційні компанії повинні зважати на цю проблему й розробляти стратегії, які дозволяють забезпечити гнучкість та можливість перенесення даних та додатків до інших хмарних платформ.

Ці проблеми потрібно вирішувати для подальшого розвитку та успішного використання хмарних технологій у телекомунікаціях.

Список використаних джерел

1. Silas Sargunam; Cloud Computing-System Implementation for Business Applications; University of Technology Tirunelveli; ст. 2 ;URL: https://www.researchgate.net/publication/303354984_Cloud_Computing-System_Implementation_for_Business_Applications; (дата звернення: 27.05.2023)

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В РОЗВИТКУ ІНФОРМАЦІЙНИХ СИСТЕМ.

Пашков С. І
Державний університет телекомунікацій, м. Київ

В сучасному світі штучний інтелект (ШІ) стає все більш впливовим інструментом, який змінює підхід до розвитку та функціонування інформаційних систем. ШІ володіє здатністю аналізувати великі обсяги даних, виконувати складні завдання, приймати рішення та навіть навчатися самостійно. У цьому тексті ми розглянемо роль штучного інтелекту в розвитку інформаційних систем та його вплив на різні сфери діяльності.

Однією з основних ролей штучного інтелекту є автоматизація та оптимізація процесів в інформаційних системах. Завдяки своїм аналітичним та когнітивним можливостям, ШІ може швидко обробляти та аналізувати великі обсяги даних [3], що дозволяє зробити точні прогнози, здійснювати швидке прийняття рішень та вдосконалювати роботу інформаційних систем. Наприклад, в банківській галузі ШІ може використовуватися для автоматизації процесу кредитного схвалення, аналізу клієнтських платежів та виявлення шахрайства.

Штучний інтелект також має значний вплив на покращення взаємодії між користувачами та інформаційними системами. Завдяки технологіям розпізнавання мови та обробки природної мови, ШІ може взаємодіяти з людьми на більш природному рівні, розуміючи їхні запити та надаючи зрозумілі відповіді. Наприклад, голос асистенти, як Siri або Google Assistant, використовують штучний інтелект для розпізнавання голосу користувача та надання відповідей на запити [2]. Це зробило взаємодію з інформаційними системами більш зручною та ефективною, особливо для людей, які мають обмеження у використанні клавіатури або екрану.

Штучний інтелект також використовується для покращення безпеки інформаційних систем. Він може аналізувати великі обсяги даних для виявлення потенційних загроз інформаційній безпеці, а також розробляти та впроваджувати ефективні заходи захисту. Наприклад, системи штучного інтелекту можуть виявляти аномальну активність у мережі, розпізнавати зловмисні програми та шифрування даних.

Ще однією важливою роллю штучного інтелекту в розвитку інформаційних систем є здатність до навчання та самозміни. Застосування алгоритмів машинного навчання та

глибинного навчання дозволяє інформаційним системам самостійно вдосконалюватися, виявляти нові патерни та робити прогнози на основі отриманої інформації. Це може бути корисним у таких сферах, як медицина, фінанси, маркетинг, де швидке та точне прийняття рішень є критично важливим.

Однак, разом з потужними можливостями штучного інтелекту виникають його етичні та соціальні виклики. Наприклад, питання конфіденційності та приватності даних, впливу на зайнятість та розподіл робочих місць, впливу на прийняття рішень людьми. Важливо розробляти відповідні етичні стандарти та правила [1], щоб забезпечити використання штучного інтелекту відповідно до принципів справедливості, прозорості та забезпечення довіри користувачів.

Крім того, розробка та впровадження штучного інтелекту вимагає співпраці між різними секторами суспільства. Необхідно залучати учасників з галузей технологій, права, економіки та соціології для обговорення та вирішення ключових питань, пов'язаних з використанням штучного інтелекту.

У підсумку, роль штучного інтелекту в розвитку інформаційних систем є надзвичайно важливою та перспективною. Він впливає на автоматизацію та оптимізацію процесів, поліпшення взаємодії з користувачами, забезпечення безпеки та розширення можливостей інформаційних систем. Однак, разом з цим виникають етичні, соціальні та правові виклики, які потребують уваги та обговорення. Забезпечення етичного використання та розуміння потенціалу штучного інтелекту є ключовими факторами для його успішного впровадження та розвитку у майбутньому.

Список використаних джерел

1. Курцвейл, Р. The Age of Intelligent Machines.
2. Мерфі, К. Machine Learning: A Probabilistic Perspective.
3. Рассел, С., Норвіг, П. Artificial Intelligence: A Modern Approach.

РОЗВИТОК СИСТЕМНОГО АНАЛІЗУ В СУЧАСНОМУ СВІТІ

Рукомеда Вадим Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Системний аналіз належить до тих напрямів сучасної науки, які виникли в період загострення соціально-економічних і політичних проблем XX століття та обґрунтували необхідність у пошуку принципово важливих рішень у різних сферах економічної діяльності. Саме це зумовило актуальність розроблення нових методів, що дозволяють ефективно аналізувати складні проблеми як ціле і що забезпечують розгляд багатьох альтернатив, кожну з яких описують великою кількістю змінних. У результаті цього пошуку сформувалася широка й універсальна методологія розв'язання проблем, яка була названа системним аналізом [1].

Системний аналіз - це науково - методологічна дисципліна, яка вивчає принципи, методи та засоби дослідження складних об'єктів за допомогою представлення їх як системи і аналізу цих систем. Таким чином, у системному аналізі будь-який об'єкт розглядається з урахуванням його системного характеру, тобто не як єдине ціле, а як комплекс взаємопов'язаних складових елементів, їх властивостей та процесів [2].

Найбільш широкого поширення системний аналіз набув у теорії та практиці управління - при виробленні, прийнятті та обґрунтуванні рішень, пов'язаних з проектування, створенням та

управлінням складними, багаторівневими та багатокомпонентними штучними системами. Передумови розвитку системного аналізу склалися у першій половині XX століття, будучи зумовлені переходом до нового типу наукових та технічних завдань: у цілій низці галузі науки та техніки центральне місце починають займати проблеми організації та функціонування складних об'єктів: пізнання та практика починає оперувати системами, межі та склад яких далеко не очевидні та вимагають спеціального дослідження в кожному окремому випадку [3]. Саме тому, розвиток системного аналізу є ключовим фактором для досягнення успіху в сучасному світі та розв'язання складних проблем у різних галузях за допомогою використання інформаційних технологій та методологічних засад аналізу.

За сучасних умов системний аналіз застосовується на етапі узагальнень при дослідженні законів динаміки різних систем (в тому числі суспільних) і абстрактного виділення з реальних систем окремих характеристик, що є спільними для всіх або хоча б для одного класу систем. Це стимулює зацікавленість до кібернетичних систем, що піддаються управлінню, і, разом з тим, підвищує інтерес до математичних моделей, які можна використовувати для отримання додаткової інформації про реальні системи. Всі методи, які передбачені таким підходом, об'єднуються під однією загальною назвою.

Розвиток системного аналізу в сучасному світі є надзвичайно важливим і ключовим для досягнення успіху в різних галузях. Системний аналіз є інструментом, що дозволяє досліджувати та аналізувати складні системи та процеси з метою вирішення проблем та покращення результатів. Застосування системного аналізу охоплює методологічні засади аналізу та використання інформаційних технологій, що дозволяє зробити процес аналізу більш ефективним та швидким. Він може бути застосований в бізнесі, науці, технологіях, соціальній сфері, медицині та багатьох інших галузях [4].

В бізнесі системний аналіз допомагає приймати рішення щодо стратегії розвитку, оптимізації процесів та використання ресурсів. У науці та технологіях системний аналіз допомагає в розробці нових продуктів та технологій, а також у вдосконаленні існуючих. В соціальній сфері системний аналіз допомагає управляти різноманітністю та забезпечити сталість соціальних систем. У медицині системний аналіз застосовується для оптимізації лікувальних процесів та поліпшення якості надання медичних послуг.

Висновки: Системний аналіз є важливою та необхідною дисципліною для розв'язання складних проблем у сучасному світі. Розвиток системного аналізу охоплює не тільки методологічні засади аналізу, але і використання інформаційних технологій, що дозволяє зробити процес аналізу більш ефективним та швидким. Застосування системного аналізу може бути корисним для багатьох галузей, таких як бізнес, наука, технології, соціальна сфера, медицина та багато інших. Одним із головних напрямків розвитку системного аналізу є зростання ролі штучного інтелекту та машинного навчання, що дозволяє зробити аналіз більш точним та автоматизованим. В цілому, системний аналіз є важливим інструментом для досягнення успіху в різних галузях та забезпечення ефективного вирішення проблем в сучасному світі.

Список використаних джерел:

1. Перегудов Ф. І., Тарасенко Ф. П. Введення у системний аналіз. - М., 2016.
2. Кліланд Д., Кінг В. Системний аналіз та цільове управління. - М., 2019.
3. Лямець В. І. Системний аналіз. Вступний курс / В. І. Лямець, А. Д. Тевяшев. – 2-ге вид., переробл. та допов. – Харків : ХНУРЕ, 2015. – 448 с.
4. Сурмин Ю. П. Теорія систем і системний аналіз : пособ. / Ю. П. Сурмин. – Київ : МАУП, 2018. – 368 с.

ТЕХНОЛОГІЯ WCDMA:ПЕРЕВАГИ ТА НЕДОЛІКИ

Саяпін Андрій Сергійович
Державний університет телекомунікацій, м. Київ

Технологія WCDMA (Wideband Code Division Multiple Access) є одним із стандартів мобільного зв'язку, який використовується для передачі даних у 3G та 4G мережах. Ось деякі переваги та недоліки технології WCDMA:

Переваги WCDMA:

1.Висока швидкість передачі даних: WCDMA забезпечує високу швидкість передачі даних, що дозволяє користувачам швидко завантажувати великі файли, стрімінгове відео та використовувати інші послуги зв'язку, які вимагають великої пропускної здатності.

2.Підтримка багатьох користувачів: Технологія WCDMA використовує CDMA (Code Division Multiple Access), що дозволяє одночасно підключати багато користувачів до одного базового станції. Це покращує ефективність мережі та дозволяє обслуговувати більше абонентів.

3.Покриття та проникнення: WCDMA має кращу здатність проникати через перешкоди, такі як стіни та будівлі, порівняно з іншими технологіями. Вона також забезпечує широке покриття сигналом, що дозволяє зберігати стабільне з'єднання в різних місцях.

4.Голосові та передача даних одночасно: WCDMA дозволяє одночасно передавати голос та дані. Це означає, що користувач може розмовляти по телефону та використовувати інтернет або інші послуги передачі даних без переривання зв'язку.

Недоліки WCDMA:

1.Висока енергоспоживання: Технологія WCDMA вимагає відносно більшої потужності передавача порівняно з іншими технологіями, такими як GSM. Це може призвести до більш швидкого розряджання батареї мобільного пристрою.

2.Спектральна ефективність: WCDMA вимагає більш широкого спектру для передачі даних порівняно з іншими технологіями. Це може створити обмеження на кількість одночасних користувачів та загальну пропускну здатність мережі.

3.Інтерференція: В умовах високої щільності користувачів або в областях зі значною кількістю сигналів може виникати проблема взаємної інтерференції, що може погіршити якість зв'язку та знизити швидкість передачі даних.

В цілому, WCDMA є важливим стандартом мобільного зв'язку, який надає високу швидкість передачі даних та підтримку багатьох користувачів. Однак, вона також має свої недоліки, такі як високе енергоспоживання та спектральна ефективність. З розвитком нових технологій, таких як 5G, WCDMA буде замінена більш ефективними та прогресивними системами передачі даних.

ПРОЦЕДУРА IDLE MODE В ТЕХНОЛОГІЇ LTE

Фадєєв Микита Олексійович
Державний університет телекомунікацій
Навчально науковий інститут телекомунікацій

Чи замислювалися ви колись над питанням, що відбувається з вашим телефоном після того як він вмикається, або виходить з авіа режиму?

1) По-перше, у тому місці на екрані, де зазвичай написано LTE/H+ або інша назва технології, ви побачите значок завантаження, або фразу “Searching for network” (пошук мережі);

2) Після цього, ви побачите як починають з’являтися рівні зв’язку: зазвичай це чотири палички з правого верхнього кута дисплею -  ;

3) Потім, ви побачите, до якої технології підключається пристрій – зазвичай це LTE, LTE+, 3G, H+, H або ж EDGE.

4) І останнє – це відображення назви оператору біля рівня сигналу.

До того моменту, поки ви не подзвоните комусь, або хтось не подзвонить вам, або ж ви не почнете користуватися інтернетом, ваш пристрій буде знаходитися в так званому “Idle Mode” (укр. – “режим очікування”).

Через назву, може здатися, що в цей час термінал не робить майже нічого, але це не так. Більше того, у цьому стані пристрій виконує дуже багато різних вимірювань та обчислень. Повна процедура дій телефону в режимі очікування описана в документі 3GPP TS 36.304 і налічує велику кількість статей. Ми ж розберемо тільки основні та найважливіші з них [1, 2].

У цілому, Idle Mode Procedure описує всі дії, які виконує пристрій від його ввімкнення та до того, як увійде в Connected Mode. А саме:

1) Cell Measurement (укр. – “Вимірювання стільника”). Термінал вимірює якість сигналу всіх сусідніх стільників;

2) Cell Search/PLMN Search (укр. – “Пошук стільника/Пошук PLMN”, де PLMN – Public Land Mobile Network, зона покриття). Пристрій виявляє PLMN стільників, та визначає, на який стільник він може підключитися; (укр. – “Вибір стільника”). Пристрій обирає стільник та проводить процедуру реєстрації;

3) Cell Reselection (укр. – “Повторний вибір стільника”). Термінал від’єднується від теперішньої соти, та підключається до іншої, сусідньої.

Далі коротко розглянемо кожен пункт окремо.

1) Cell Measurement

Типовий алгоритм дій терміналу для цього процесу:

1. Термінал настроюється на кожний частотний канал, який він підтримує та вимірює якість сигналу.

2. Після цього, термінал зі списку виміряних каналів обирає найкращий за рівнем сигналу.

3. Термінал декодує PCPICH та знаходить Physical Cell ID для кожного кандидату зі списку з пункту 1.

4. Для списку з пункту 3, термінал декодує MIB кожного кандидату.

5. Після цього, термінал може порахувати який кандидат є найкращим, декодувати SIB та розпочати процедуру реєстрації.

2) Cell Search/PLMN Search

Після процедури Cell Search, пристрій проводить вимірювання , синхронізується з Broadcast channel та ідентифікує знайдені PLMN. Пріорітетно, термінал буде намагатися знайти так званий HPLMN (Home PLMN), але якщо він не може його знайти, то підключиться до VPLMN (Visited PLMN). Після того, як термінал знову зайде в Idle Mode, він буде намагатися під’єднатися до HPLMN в пріоритеті над VPLMN.

3) Для процедури Cell Selection використовується багато обчислень та вимірювань, параметри для яких наведені в табл. 1 [3].

Таблиця 1 - Параметри для розрахунку критерію Cell Selection

S_{rxlev}	Значення RX рівня для вибіру стільника (dBm)
S_{qual}	Значення якості для вибіру стільника (dB)
$Q_{rxlevmeas}$	Виміряний RX рівень стільника (RSRP)
$Q_{qualmeas}$	Виміряний рівень якості стільника (RSRQ)

$Q_{rxlevmin}$	Мінімальний допустимий RX рівень в стільнику (dBm)
$Q_{qualmin}$	Мінімальний допустимий рівень якості в стільнику (dB)
$Q_{rxlevminoffset}$	Offset(укр. – “зміщення”), використовується у формулах для розрахунку рівня сигналу.
$Q_{qualminoffset}$	Offset(укр. – “зміщення”), використовується у формулах для розрахунку рівня сигналу.
$P_{compensation}$	$Max(P_{EMax}-P_{PowerClass}, 0)$ (dB)
P_{EMax}	Максимальна TX потужність терміналу для uplink.
$P_{PowerClass}$	Максимальна радіочастотна вихідна потужність терміналу.

Після вимірювання всіх параметрів, термінал може виконати розрахунки. Критерій для обрання стільника: $S_{rxlev}>0$ і одночасно $S_{qual}>0$. Формули для розрахунку:

$$S_{rxlev}= Q_{rxlevmeas}-(Q_{rxlevmin}+ Q_{rxlevminoffset})- P_{compensation};$$

$$S_{qual}=Q_{qualmeas}-(Q_{qualmin}+Q_{qualminoffset})$$

4) Останньою є процедура Cell Reselection. Вона відбувається, якщо рівень сигналу стільника, з яким з'єднаний пристрій, падає нижче критерію для Cell Selection. Процедура Cell Reselection є дуже подібною до Cell Selection, і використовує ті ж самі параметри для вимірювання.

Таким чином, мною було розглянуто процедуру поведінки терміналу в Idle Mode в технології LTE. Сподіваюсь, ця процедура стала більш зрозумілою. Звісно, я не можу описати всі процедури та специфікації, адже в 3GPP є цілий величезний документ на цю тему - TS 36.304. Підводячи підсумок, я хотів би ще раз зазначити, що не дивлячись на те, що зі сторони термінал в Idle Mode-і нічого не робить, він виконує дуже багато обчислень та вимірювань. Через це, наприклад, під час включення телефону він може одразу розрядитися на 1-2% від повного заряду.

Список використаних джерел:

1. 3GPP: TS 36.304: E-UTRA — UE Procedures in Idle Mode. URL: https://www.tech-invite.com/3m36/tinv-3gpp-36-304.html

2. 4G/LTE Basic Procedures. Cell Selection Criterion. URL: https://www.sharetechnote.com/html/Handbook_LTE_Cell_Selection_Criterion.html

3. 4G/LTE Basic Procedures. Cell Search. URL: https://www.sharetechnote.com/html/BasicProcedure_LTE_Cell_Search.html

СИСТЕМА УПРАВЛІННЯ ТА МОНІТОРИНГУ SNMP

Кузьменко Максим Юрійович
Державний університет телекомунікацій

SNMP (Simple Network Management Protocol) - це протокол мережевого управління, який дозволяє моніторити та керувати мережевими пристроями. SNMP складається з трьох основних компонентів: система управління мережею (NMS), агент та MIB (Management Information Base).

NMS (Network Management System) - це система управління мережею, яка використовується для моніторингу та керування мережевими пристроями.

Система управління мережею (NMS) дозволяє ідентифікувати, конфігурувати, моніторити, оновлювати та усувати несправності мережевих пристроїв. Вона включає в себе програмне та апаратне забезпечення для відстеження різних аспектів мережі та її роботи, таких як трафік, використання пропускної здатності та час безвідмовної роботи.

Основні переваги використання систем управління мережею полягають у забезпеченні чіткої видимості всіх підключених пристроїв в мережі, покращенні ефективності та швидкому виявленні та усуненні несправностей. Крім того, системи управління мережею дозволяють зменшити ручну роботу для IT-команд, що дає можливість присвятити більше часу критичним проектам для організації.

Агент SNMP - це процес SNMP, який постійно знаходиться на управляємому пристрої та взаємодіє з NMS. Агент SNMP обмінюється даними управління мережею з програмним забезпеченням диспетчера SNMP, яке працює на NMS або хості. Агент відповідає на запити щодо інформації та дій від менеджера. Агент також керує доступом до MIB агента, набору об'єктів, які може переглядати або змінювати менеджер SNMP.

MIB (Management Information Base) - це база даних управління, яка містить ієрархічну структуру об'єктів управління. Об'єкти MIB визначають управляючі об'єкти в мережевому пристрої. Об'єкти MIB пов'язані з ідентифікатором об'єкта (OID), який називає об'єкт. Об'єкти MIB можуть бути стандартними або корпоративними.

SNMP (Simple Network Management Protocol) та RMON (Remote Network Monitoring) - це два різних протоколи мережевого управління. SNMP відстежує основні метрики “здоров'я” мережевих пристроїв та дозволяє необхідні зміни конфігурації. RMON є розширенням SNMP та надає дані про потоку трафіку для усунення несправностей та контролюється з центральної консолі.

RMON (Remote Network Monitoring) - це протокол мережевого моніторингу, який дозволяє моніторити мережевий трафік. RMON складається з двох основних компонентів: RMON-1 та RMON-2.

Оригінальна версія RMON (RMON-1) фокусувалася на інформації рівня OSI 1 та 2 в мережах Ethernet та Token Ring, він складається з десяти груп MIB: статистика, історія, сповіщення, хости, хости top N, матриця, фільтр, події, протоколи та додатково.. RMON-2 додав підтримку моніторингу мережевого та додаткового рівнів та SMON, який додав підтримку для комутованих мереж, загалом він додає дев'ять груп даних, які стосуються мережевого та додаткового рівнів OSI моделі.

SMON (Switch Monitoring) - це розширення RMON, яке додає підтримку для комутованих мереж. SMON дозволяє моніторити трафік на комутаторах та виявляти проблеми в мережі.

СИСТЕМИ ІДЕНТИФІКАЦІЇ ЗОБРАЖЕННЯ ТА ЇЇ ЗАСТОСУВАННЯ

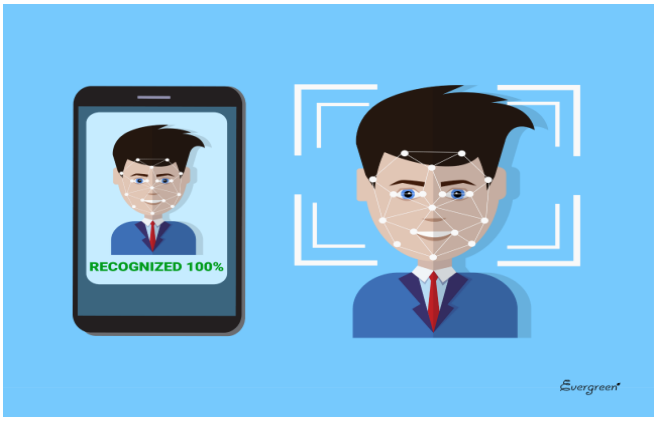
Поліщук Дмитро Анатолійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

На сьогоднішній день дуже важко уявити світ без сучасних технологій та розробок . Щодня ми стикаємось або використовуємо технічні прилади , які потребують нашої

ідентифікації як користувача (USER) . Наведу досить примітивний та очевидний приклад а саме мобільний телефон : Якщо користувач переживає за свої данні (а саме фотографії , соціальні мережі , додатки) він з вірогідністю у 100% може встановити пароль . Це як раз та сама система безпеки яка і ідентифікує користувача як так би мовити “свого” і надає весь свій функціонал пристрою після проходження ідентифікації . То що ж саме таке ідентифікація?

Ідентифікація це – сукупність заходів перевірки щодо користувача як правило за допомогою наперед визначеного імені , яке дозволяє недопущення взлому зловмисниками. Сам принцип ідентифікації виник дуже давно. Класифікацій ідентифікації дуже багато на слайдах буде доведено більш конкретизована інформація щодо цього терміну :

1. На цьому слайді ми можемо побачити як мобільний пристрій використовує ідентифікацію для надання доступу до ресурсів користувачу методом розпізнавання користувача по обличчю



2. Тут же ми бачимо як завдяки контролю технічними засобами проводиться ідентифікація людини по сітчатці ока
3. Також можлива ідентифікація по відбитку пальця

Отже підсумовуючи наявні методи а також багату кількість класифікацій вище згаданих в даній темі можливо сказати що на сьогоднішній день , такий метод збереження власних даних та доступу до окремих ресурсів є досить надійним завдяки своїй технологічності і цифровим якостям та можливостям. В перспективі на сьогоднішній день інженери виконують багату кількість досліджень та наукових експериментів задля ще більшої модернізації ідентифікаційних засобів.

АНАЛІЗ ТЕХНОЛОГІЙ РЕАЛІЗАЦІЇ SMART HOUSE

Лісогор Гліб Денисович
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій

Такі протоколи як Zigbee і Z-Wave, Wi-Fi є найчастіше використовуваними у домашнійї автоматизації, які застосовують на даний момент. Технології безпроводової мережі застосовують малопотужні радіосигнали малого радіусу дії для підключення систем

«розумного будинку». Незалежно від того, що одні і ті самі додатки орієнтовані для «розумного будинку», дальність зв'язку Z-Wave є 30 м. до 10 м, а також є меншскладною технологією чим Zigbee. Чіпи Zigbee реалізують декілька компаній, а Z-Wave доступні тільки від Sigma Designs.

Приклад протоколів представлений на рис.1.

Рис. 1. Технології розумного будинку

Характеристики деяких технологій «розумного будинку» наведено у таблиці 1.

Таблиця 1.

Характеристики деяких технологій «розумного будинку»

Технологія	Wi-Fi	Bluetooth	ZigBee	Thread
Стандарт зв’язку	IEEE 802.11	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.4
Швидкість передачі даних	300+Мбіт	До 3 Мбіт	250 Кбіт	250 Кбіт
Енерговикористання	Високе	Низьке	Низьке	Низьке
Частотний діапазон	2,4 ГГц	2,4 ГГц	2,4 ГГц	2,4 ГГц
Підтримка IP-технології	+			+
Топологія	Зірка	Зірка	mesh	mesh

Центр «розумного будинку» є апаратним пристроєм, що є центральною точкою системи «розумного будинку» і має можливість сприймати, виконувати обробку даних та надавати мобільний зв'язок. Система об'єднує різного роду додатки в один додаток для «розумного будинку», яким користувачі мають змогу віддалено керувати.

Як приклад центру «Smart House» є Amazon Echo, Google Home, Insteon Hub Pro, Samsung SmartThings і Wink Hub і інші.

Деякі системи «Smart House» створюються з нуля, як приклад, із застосуванням Raspberry Pi або іншої плати для макетування. Інші можуть бути куплені у виді комплекту «розумного будинку» - який ще називають платформа «розумного будинку» і складається з елементів, необхідних для застосування автоматичним керуванням будинку.

У простій схемі «розумного будинку» події зазвичай синхронізовані, чи ініційовані. Короткочасні події що засновані по годинникам, як приклад, о 18:00, а ініційовані події залежні від дій в автоматизованій системі; як наприклад, якщо смартфон користувача підносять до дверей, розумний замок виконує розблокування,або як приклад загоряється світло.

Аналіз показав що машинне навчання стає популярним для використання в системах «розумного будинку», збльшуючи ефективність та адапнованість автоматизації домашніх пристроїв до їх середовища. Прикладом є голосові системи, такі як Amazon Echo чи Google

Home, які містять віртуальних помічників, за допомогою яких виконується навчання та налаштування «розумного будинку» до своїх вподобань і моделями жителів.

Список використаних джерел:

1. P. I. Grammatikis, P. G. Sarigiannidis, I. D. Moscholios, "Securing the Internet of Things: Challenges, threats, and solutions", Internet of Things, Vol. 5, 2019, pp. 41–70.

2. K. Ashton, et al., "That internet of things thing", Radio Frequency Identification (RFID) Journal Vol. 22, Issue 7, 2019, pp. 97–114.

МЕТОДИ ПОБУДОВИ СУЧАСНИХ VPN-МЕРЕЖ

Чорний Олексій Володимирович
Державний університет телекомунікацій

За останні десятиліття інтернет став невід'ємною частиною нашого повсякденного життя. Зростання кількості підключених пристроїв та обсягу передаваних даних створює потребу у забезпеченні безпеки та конфіденційності інформації. У цьому контексті виникає необхідність використання VPN-мереж (Virtual Private Networks) для забезпечення захищеного з'єднання та обміну даними між вузлами мережі. У даному есе будуть розглянуті методи побудови сучасних VPN-мереж та їх роль у забезпеченні безпеки та приватності.

Аналіз сучасних методів побудови VPN-мереж та їх використання для забезпечення безпеки та конфіденційності даних. Сучасні методи побудови VPN-мереж базуються на різних протоколах та технологіях, таких як IPsec, SSL/TLS, OpenVPN, WireGuard тощо. Ці методи забезпечують шифрування та аутентифікацію даних, що передаються через мережу, забезпечуючи конфіденційність та цілісність інформації. Використання VPN-мереж дозволяє створити віртуальний тунель між вузлами мережі та захистити дані від несанкціонованого доступу.

Проектування оптимальної архітектури VPN-мережі з урахуванням вимог ефективності та масштабованості. При проектуванні VPN-мереж необхідно враховувати вимоги до швидкості передачі даних та масштабованості мережі. Використання ефективних протоколів та алгоритмів дозволяє забезпечити оптимальну пропускну здатність та швидкість передачі даних в межах VPN-мережі. При проектуванні мережі також необхідно враховувати потреби організації та розподіл ресурсів для забезпечення масштабованості мережі під зростаюче навантаження.

Імплементація та впровадження сучасних протоколів і технологій в побудові VPN-мереж для забезпечення надійного з'єднання та захисту даних. Успішна реалізація VPN-мереж вимагає імплементації та впровадження сучасних протоколів та технологій. Наприклад, використання IPsec забезпечує захищене з'єднання на рівні мережевого протоколу, тоді як SSL/TLS дозволяє створити безпечне з'єднання через веб-браузер. Також, використання клієнтських програм та мобільних додатків дозволяє зручно підключатися до VPN-мереж та забезпечувати безпеку під час передачі даних.

Аналіз ефективності та безпеки різних методів шифрування та аутентифікації в сучасних VPN-мережах. Використання ефективних методів шифрування та аутентифікації є важливим аспектом у побудові VPN-мереж. Аналіз різних методів, таких як симетричне та асиметричне шифрування, алгоритми хешування, протоколи аутентифікації, дозволяє визначити найбільш ефективні та безпечні засоби захисту даних у межах VPN-мереж

Методи побудови сучасних VPN-мереж є ключовими у забезпеченні безпеки та конфіденційності даних в сучасному інтернеті. Використання ефективних методів шифрування, аутентифікації та протоколів дозволяє створити захищене з'єднання між вузлами

мережі та забезпечити безпеку під час передачі даних. Проектування оптимальної архітектури та імплементація сучасних протоколів і технологій є важливими етапами в розробці VPN-мереж. Аналіз ефективності та безпеки різних методів допомагає визначити найкращі практики в побудові VPN-мереж для задоволення вимог безпеки та ефективності передавання даних.

Література:

1.Anderson, B. (2017). Mastering WireGuard. Packt Publishing Ltd.

2.Dinha, H. T., Al-Jarrah, O. Y., Al-Qirim, N. A., & Yang, L. T. (2019). A comprehensive survey on VPN technologies: Current challenges and solutions. IEEE Access, 7, 65480-65503.

3.Peterson, L. L., & Davie, B. S. (2011). Computer networks: a systems approach. Morgan Kaufmann.

4.Singh, K. (2018). Secure VPN communication using IPsec. International Journal of Engineering and Technology, 7(4.19), 269-273.

ПІДВИЩЕННЯ ЯКІСТІ ПЕРЕДАЧІ ДАНИХ ТА ЗАБЕЗПЕЧЕННЯ ВИСОКОЇ ЕФЕКТИВНІСТІ МЕРЕЖІ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ QOS ТА ОБЛАДНАННЯ CISCO

Луцюк Іван Валерійович
Державний університет телекомінікацій
Навчально-науковий інститут телекомунікацій

В сучасному світі, де мережі є невід'ємною складовою бізнесу, передача даних стає все більш важливою. Висока якість передачі даних та швидкість стають критичними для бізнес-процесів, що залежать від мережі. Тому забезпечення ефективності мережі стає важливою задачею.

Технологія Quality of Service (QoS) - це механізм управління трафіком, який дозволяє забезпечити високу якість передачі даних в мережі. Вона забезпечує гарантовану якість обслуговування (Quality of Service - QoS) на рівні мережі, що дозволяє забезпечити приоритетність передачі даних, зменшити затримки та втрати пакетів.

Обладнання Cisco працює на різних рівнях мережі, QoS може бути налаштований для керування різними видами трафіку, що дозволяє розподіляти пропускну здатність мережі для кращого забезпечення приоритетних бізнес-процесів.

Застосування технології QoS на базі обладнання Cisco дозволяє досягти найвищої ефективності мережі, що дозволяє забезпечити бізнес-процеси якісною передачею даних. Тому використання технології QoS на базі обладнання Cisco є ключовим фактором в забезпеченні ефективності мережі та успішного розвитку бізнесу.

Одним з найбільш важливих аспектів технології QoS є можливість призначення пріоритету для різних видів трафіку. Наприклад, голосовий трафік має вищий пріоритет ніж трафік інтернет-браузера або відео, що дозволяє забезпечити якісну передачу голосу без затримок та переривань. Також, технологія QoS дозволяє встановлювати обмеження на рівень трафіку та використання пропускної здатності, що дозволяє уникнути перевантаження мережі та забезпечити оптимальну роботу.

Іншим важливим аспектом технології QoS є можливість моніторингу та аналізу трафіку. Обладнання Cisco має різноманітні інструменти для моніторингу трафіку та аналізу його характеристик. Це дозволяє оперативно реагувати на проблеми в мережі та вносити коригування для забезпечення найвищої ефективності мережі.

Технологія QoS на базі обладнання Cisco дозволяє забезпечити гнучке управління трафіком та ефективне використання пропускної здатності мережі. Це важливо для підвищення ефективності бізнес-процесів та забезпечення високоякісної передачі даних. Використання технології QoS на базі обладнання Cisco є необхідним кроком для забезпечення успішного розвитку бізнесу в умовах сучасної технологічної економіки.

Отже, можна стверджувати, що технологія Quality of Service (QoS) є ключем до підвищення ефективності мереж на базі обладнання Cisco. Застосування технології QoS на базі обладнання Cisco є особливо важливим для компаній, які працюють з великим обсягом даних, мають значну кількість користувачів та оперують з великим обсягом мультимедійного контенту.

Також слід відзначити, що технологія QoS не є універсальним рішенням для всіх випадків використання мереж. Відповідне налаштування та підбір параметрів є дуже важливими для досягнення максимальної ефективності мережі. Тому перед впровадженням технології QoS на базі обладнання Cisco необхідно провести детальний аналіз потреб користувачів та врахувати особливості конкретної мережі.

У підсумку, можна стверджувати, що технологія Quality of Service (QoS) є важливим інструментом для підвищення якості передачі даних та забезпечення найвищої ефективності мереж на базі обладнання Cisco. Її застосування є особливо важливим для компаній, які працюють з великим обсягом даних та мають значну кількість користувачів. Проте перед впровадженням технології необхідно провести детальний аналіз потреб користувачів та врахувати особливості конкретної мережі для досягнення максимальної ефективності та якості роботи мережі.

Література:

1. Cisco Systems. (2021). Quality of Service (QoS). https://www.cisco.com/c/en/us/products/ios-nx-os-software/quality-of-service-qos/index.html

2. Chen, G., & Das, S. K. (2011). Quality of service in wireless sensor networks: a survey. IEEE Communications Surveys & Tutorials, 13(2), 274-287.

3. Liu, Y., Zhou, J., & Xiao, Y. (2015). QoS provisioning in software defined networks: a survey. IEEE Communications Surveys & Tutorials, 17(3), 1294-1330.

4. Kaur, G., & Singh, A. K. (2016). A review on Quality of Service (QoS) in wireless sensor networks. International Journal of Computer Applications, 148(1), 20-24.

ОСОБЛИВОСТІ МІКРОСЕРВІСНИХ СИСТЕМ

Бондар Дмитро Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Мікросервісна архітектура - це підхід до розробки програмного забезпечення, в якому додаток розбивається на невеликі індивідуальні компоненти, які називаються мікросервісами. Кожен мікросервіс відповідає за виконання конкретної функції додатку та має власний інтерфейс програмування додатків (API).

Ці мікросервіси можуть бути розгорнуті та масштабовані незалежно один від одного, що дозволяє розробникам швидко внести зміни в окремі компоненти без впливу на решту додатку. Це забезпечує гнучкість та швидкість розробки та підтримки додатків.

Кожен мікросервіс може бути розгорнутий на своєму власному сервері та може бути написаний різними мовами програмування або використовувати різні технології. Це дає розробникам можливість використовувати найкращі рішення для кожного компонента.

Мікросервісна архітектура дозволяє підвищити масштабованість, доступність та стійкість до відмов, оскільки кожен мікросервіс може бути масштабований окремо, а проблеми в одному мікросервісі не повинні впливати на решту системи.

Основні особливості мікросервісних систем можуть включати наступні пункти:

Розбиття на окремі сервіси: в основі мікросервісної архітектури лежить розбиття додатку на невеликі незалежні сервіси, які можуть функціонувати окремо або спільно з іншими сервісами.

1. Розподілена архітектура: кожен сервіс може бути розгорнутий на різних серверах, що дозволяє розподіляти навантаження і підвищувати масштабованість.
2. Компонентна природа: кожен сервіс може бути реалізований окремо, використовуючи будь-яку технологію та стек технологій.
3. Незалежність: кожен сервіс може бути розроблений, тестований та розгорнутий окремо від інших сервісів.
4. Гнучкість: додавання або видалення нових сервісів може бути здійснено з легкістю, що дозволяє змінювати функціональність системи без значних змін у коді.
5. Надійність: якщо один сервіс не працює, це не впливає на інші сервіси.
6. Спрощення розробки та підтримки: дрібний розмір кожного сервісу дозволяє розробникам більш швидко розробляти та тестувати нові функції, а також робити зміни в існуючому коді.
7. Розширюваність: мікросервісна архітектура дозволяє легко додавати нові функції та змінювати функціональність сервісів з мінімальним впливом на систему в цілому.

Для контролю і розробки систем підхом мікросервісних архітектури потрібно розумітись також в інструментах які для цього існують. Наприклад найпопулярніші інструменти для розробників пропонує Amazon і Google.

Google та Amazon Web Services (AWS) - це два провідних хмарних провайдери, які надають різноманітні хмарні послуги, включаючи мікросервісну архітектуру.

Google Cloud Platform (GCP) містить такі сервіси, як Kubernetes та Cloud Functions, що дозволяють розробникам створювати мікросервісні додатки. Kubernetes - це оркестратор контейнерів, який дозволяє автоматизувати розгортання та управління мікросервісами. Cloud Functions - це сервіс, який дозволяє розробникам написати та розгорнути функції, що можуть бути викликані з інших додатків або сервісів.

AWS також має свої власні сервіси мікросервісної архітектури. Наприклад, Amazon Elastic Container Service (ECS) - це сервіс, що дозволяє керувати контейнерами Docker. Amazon Elastic Kubernetes Service (EKS) - це повністю управляємий сервіс Kubernetes, який дозволяє автоматизувати розгортання, масштабування та управління мікросервісами. Amazon Lambda - це сервіс, що дозволяє розробникам написати функції, які автоматично масштабуються та виконуються при запитах.

Крім того, обидва провайдери пропонують різноманітні інструменти для моніторингу та логування мікросервісів, такі як Stackdriver для GCP та CloudWatch для AWS. Також існують різні сервіси для забезпечення безпеки, такі як Google Cloud Security та AWS Identity and Access Management (IAM).

У загальному, Google та AWS пропонують широкий спектр інструментів та сервісів для створення, моніторингу та управління мікросервісними додатками в хмарі.

Загалом, мікросервісна архітектура дозволяє розробникам створювати більш гнучкі, швидкі та масштабовані додатки, що можуть швидко реагувати на зміни в бізнес-логіці та технологічних вимогах.

РОЗБІР ТА АНАЛІЗ МЕТОДІВ ВИКОРИСТАННЯ СУПУТНИКОВОГО ЗВ'ЯЗКУ

Лижов Олексій Михайлович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Супутниковий зв'язок є суттєвим компонентом сучасних комунікаційних систем. Це технологія, яка дозволяє передавати голос, дані та іншу інформацію через комунікаційні супутники, розташовані на орбіті навколо Землі. Використання супутникового зв'язку має безліч методів, які можуть бути розглянуті з різних перспектив.

Одним із основних методів використання супутникового зв'язку є телекомунікація. Комунікаційні супутники дозволяють передавати сигнали між різними точками на Землі. Цей метод використовується для мобільного зв'язку, супутникового телебачення, супутникового Інтернету та інших комунікаційних послуг. Супутникова телекомунікація дозволяє забезпечити зв'язок в місцях, де традиційні мережі можуть бути недоступними або неефективними, наприклад, у віддалених районах, на морі або у повітрі.

Наступний метод - це навігація. Супутникові системи, такі як GPS (Глобальна система позиціонування), GLONASS (Глобальна навігаційна супутникова система) та Galileo, дозволяють визначати місцезнаходження, швидкість та напрямок руху об'єктів з високою точністю. Це дозволяє навігаційним пристроям, таким як автомобільні навігатори, мобільні додатки та системи стеження, прокладати оптимальні маршрути, контролювати рух транспорту та забезпечувати безпеку під час подорожей.

Третій метод - це наукові дослідження та дослідження космосу. Супутниковий зв'язок дозволяє науковцям збирати дані з космічного простору, проводити астрономічні спостереження, досліджувати планети та інші об'єкти у Сонячній системі. Крім того, використання супутникових систем у наукових цілях дає можливість спостерігати та вивчати Землю з великої відстані, що надає нові можливості для геологічних, метеорологічних та інших досліджень.

У аналізі методів використання супутникового зв'язку також важливо враховувати технологічний аспект. Супутникові системи вимагають розробки та впровадження комплексної інфраструктури, включаючи супутники, наземні станції, антени, комунікаційні протоколи та інше обладнання. Важливо аналізувати ефективність та надійність супутникових систем, впроваджувати нові технології та шукати способи покращення якості комунікаційного зв'язку.

Додатково, супутниковий зв'язок використовується для моніторингу довкілля та наукових досліджень. Супутники здатні збирати дані про кліматичні зміни, виявляти природні катастрофи, контролювати забруднення повітря та води, слідкувати за рухом льодовиків та багато іншого. Ці дані є цінним джерелом інформації для науковців, урядових органів та різних галузей промисловості, що допомагає в прийнятті рішень та вирішенні проблем, пов'язаних зі змінами клімату та станом довкілля.

Інтеграція супутникового зв'язку у сучасне життя має великий вплив на різні аспекти нашого повсякденного і професійного життя. Він полегшує спілкування, поліпшує доступ до інформації, забезпечує безпеку та зручність у подорожах, сприяє науковим дослідженням та забезпечує розвиток сучасних технологій. Інтеграція супутникового зв'язку з іншими технологіями, такими як штучний інтелект, Інтернет речей та хмарні обчислення, відкриває нові можливості та сприяє швидкому технологічному прогресу. Також важливо враховувати не лише переваги, але й потенційні виклики та обмеження. Наприклад, забезпечення конфіденційності та кібербезпеки можуть бути важливими аспектами, які потребують уваги та заходів захисту.

Виходячи з дослідженнь та оцінки різних аспектів спутникового зв'язку, хочу виділити наступні переваги:

- Доступність
- Якість зв'язку
- Швидкість та пропускна здатність
- Надійність та стабільність
- Більша кількість прикладів застосування

Загалом, супутниковий зв'язок є невід'ємною частиною нашого сучасного життя і має великий потенціал для подальшого розвитку. Розуміння методів використання супутникового зв'язку та їх впливу на сучасне життя допомагає нам більш повноцінно використовувати цю технологію та розробляти нові інноваційні рішення для різних сфер діяльності.

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ОПТИМІЗАЦІЇ ШВИДКОСТІ КЛІЄНТ-СЕРВЕРНИХ ВЕБ-ДОДАТКІВ

Кузьмук Андрій
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Клієнт-серверні веб-додатки є неодмінною складовою сучасного інтернет-простору. Проте, задоволення користувачів та конкурентоспроможність додатків залежать від їхньої швидкості та продуктивності. Тому, оптимізація швидкості є важливою задачею для розробників. Розглянемо огляд та аналіз сучасних методів оптимізації швидкості клієнт-серверних веб-додатків, зосередившись на таких аспектах, як мінімізація розміру переданих даних, кешування, асинхронна комунікація, оптимізація баз даних та мобільна оптимізація.

Мінімізація розміру переданих даних: Зменшення обсягу переданих даних є важливим кроком для покращення швидкості завантаження сторінок. Застосування методів стиснення, таких як gzip, дозволяє зменшити розмір статичних ресурсів, таких як CSS, JavaScript та зображення. Крім того, мініфікація CSS та JavaScript файлів шляхом видалення зайвих пробілів, коментарів та зайвих символів допомагає зменшити їхній обсяг.

Кешування: Використання кешування є ефективним підходом до оптимізації швидкості клієнт-серверних веб-додатків. HTTP-кешування дозволяє зберігати копії сторінок та ресурсів на стороні клієнта або проксі-сервера. Це дозволяє уникнути повторного завантаження при наступних запитах, що сприяє швидкому завантаженню сторінок. Крім того, кешування на рівні бази даних може покращити продуктивність, зменшуючи час виконання запитів до бази даних.

Асинхронна комунікація: Використання асинхронної комунікації між клієнтом та сервером дозволяє покращити швидкість взаємодії. Застосування технологій, таких як AJAX, дозволяє виконувати асинхронні запити до сервера та оновлювати вміст сторінки без перезавантаження. Це дозволяє паралельно обробляти багато запитів та зменшує час очікування користувача.

Оптимізація баз даних: Ефективна організація та оптимізація баз даних є важливим аспектом для покращення швидкості клієнт-серверних веб-додатків. Використання індексів для швидкого пошуку та оптимізація запитів для зменшення навантаження на базу даних можуть покращити продуктивність. Крім того, розподілення навантаження, використання кешування та пам'яткових структур можуть сприяти збільшенню швидкості виконання запитів.

Мобільна оптимізація: З урахуванням поширення мобільних пристроїв, важливо оптимізувати клієнт-серверні веб-додатки для роботи на цих пристроях. Використання адаптивного дизайну дозволяє пристосовувати вигляд та розмір елементів до різних екранних розмірів. Оптимізація для обмеженої пропускної здатності забезпечує швидке завантаження на мобільних мережах. Крім того, реагування на взаємодію з користувачем та зменшення

кількості запитів до сервера також покращують швидкість роботи додатків на мобільних пристроях.

Використання кешування на рівні клієнта: Застосування механізмів кешування на стороні клієнта, таких як локальне сховище та кешування веб-браузера, дозволяє зберігати локальні копії ресурсів та сторінок. Це зменшує кількість запитів до сервера і скорочує час завантаження для повторних відвідувачів.

Використання CDN (мережі доставки контенту): CDN є розподіленою мережею серверів, що знаходяться в різних локаціях по всьому світу. Використання CDN дозволяє клієнтам отримувати вміст з сервера, що знаходиться фізично ближче до них, забезпечуючи швидше завантаження сторінок та ресурсів. CDN також може здійснювати кешування, що дозволяє знизити навантаження на сервери та прискорити доставку контенту.

Використання HTTP/2 протоколу: HTTP/2 є новітнім версією протоколу передачі гіпертексту, який пропонує ряд поліпшень у порівнянні з попередньою версією HTTP/1.1. Використання HTTP/2 дозволяє множинні запити та відповіді, стиснення заголовків, серверний push та інші функції, що покращують швидкість завантаження сторінок та знижують навантаження на сервер.

Дослідження розкриває різноманітні підходи до покращення продуктивності веб-додатків. Врахування оптимізації клієнтської сторони, використання кешування, мобільна оптимізація та використання швидкодіючих протоколів, таких як HTTP/2, мають велике значення для забезпечення швидкості завантаження та зниження навантаження на сервер. Підвищення продуктивності веб-додатків є важливим завданням для веб-розробників та може мати позитивний вплив на користувальницький досвід та конкурентоспроможність.

ШЛЯХИ РОЗВИТКУ БЕЗДРОТОВИХ СЕНСОРНИХ ТЕХНОЛОГІЙ

Шаран Дмитро Олегович
Державний університет телекомінікацій
Навчально-науковий інститут Телекомунікацій

Актуальність технологій які були винайдені кілька років тому знижується, а потреби користувачів з кожним днем збільшуються тому розвиток в кожній важливій сфері для людства повинен відбуватися майже кожен день. Розглядаючи телекомунікаційну сферу то бездротові сенсорні технології використовують майже всі на світі.

Бездротові сенсорні мережі (Wireless Sensor Networks, WSN) - розподілена мережа, що самоорганізується та складається із безлічі датчиків (сенсорів) і виконуючих пристроїв, об'єднаних між собою за допомогою радіосигналу. Кожен вузол мережі включає в себе сенсори, мікроконтролери, бездротовий модуль комунікації та джерело живлення.

Основна мета бездротових сенсорних мереж полягає у зборі інформації з фізичного середовища (наприклад, температури, вологості, руху, освітленості і т. д.) за допомогою розташованих у різних точках сенсорних вузлів. Ці дані можуть бути використані для моніторингу, контролю, аналізу або передачі на віддалені сервери для подальшої обробки.

Ось кілька шляхів розвитку:

1. Розширення мережі Інтернет речей (Internet of Things, IoT): IoT є сферою, в якій бездротові сенсори використовуються для збору та передачі даних. Шляхи розвитку IoT включають покращення безпеки мереж, розширення протоколів зв'язку, збільшення енергоефективності та стандартизацію пристроїв IoT.
2. Вдосконалення енергоефективності: Одним із викликів для бездротових сенсорних технологій є продовження тривалості роботи батарей або використання альтернативних джерел енергії. Розвиток енергоефективних бездротових протоколів передачі

даних, низькопотужних мікросхем та енергозберігаючих алгоритмів стають важливими факторами для подальшого розвитку.

3. Розширення бездротового зв'язку: Розвиток бездротових комунікаційних технологій, таких як Bluetooth, Wi-Fi, Zigbee, LoRa та інших, дозволяє створювати більш швидкі, надійні та широкомасштабні бездротові сенсорні мережі. Шляхи розвитку включають вдосконалення швидкості передачі даних, збільшення покриття мереж та зниження енергоспоживання пристроїв.

4. Застосування в медицині та здоров'ї: Бездротові сенсори мають великий потенціал у медицині та здоров'ї. Вони можуть бути використані для моніторингу показників здоров'я, відстеження вживання ліків, вимірювання фізіологічних параметрів та іншого. Розвиток безпечних, зручних у використанні та точних бездротових медичних пристроїв є важливим напрямком розвитку.

5. Застосування в "розумному" середовищі: Бездротові сенсорні технології можуть бути використані для створення "розумного" середовища, такого як "розумні" будинки, міста, транспортні системи та інші. Розвиток інтегрованих бездротових рішень, які забезпечують збір та аналіз даних з різних джерел, є важливим для розвитку таких середовищ.

Ці шляхи розвитку бездротових сенсорних технологій вказують на постійний розвиток і вдосконалення цієї галузі для забезпечення більшого зручності, надійності та ефективності бездротових сенсорних систем.

Література:

1. Wireless Sensor Network (WSN) (2023). https://www.geeksforgeeks.org/wireless-sensor-network-wsn/
2. M.A. Matin and M.M. Islam (2012). Overview of Wireless Sensor Network.
3. What Are Wireless Sensor Networks? https://toolsense.io/glossary/wireless-sensor-network/

РОЗВИТОК АЛГОРИТМІВ ШИФРУВАННЯ ІНФОРМАЦІЇ У МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ

Луценко Павло
Державний університет телекомунікацій

Бездротова сенсорна мережа (БСМ) — розподілена мережа, що самоорганізується та складається із безлічі датчиків (сенсорів) і виконуючих пристроїв, об'єднаних між собою за допомогою радіосигналу. Область покриття подібної мережі може становити від декількох метрів до декількох кілометрів за рахунок здатності ретрансляції повідомлень від одного елемента до іншого.

Розвиток алгоритмів шифрування інформації у мобільних сенсорних мережах є важливим аспектом забезпечення безпеки та конфіденційності передачі даних в цих мережах. Мобільні сенсорні мережі включають в себе мобільні пристрої, такі як смартфони, планшети та носимі пристрої, які збирають дані з різних датчиків і взаємодіють між собою для обробки та передачі цих даних.

Оскільки мобільні сенсорні мережі зазвичай працюють у бездротовому середовищі, вони піддаються ризику атак із зовнішнього середовища. Шифрування вважається ефективним методом захисту інформації від несанкціонованого доступу. Основні вимоги до алгоритмів шифрування в мобільних сенсорних мережах включають безпеку, ефективність, низьку споживання енергії та сумісність з обмеженими обчислювальними ресурсами мобільних пристроїв.

Деякі з основних алгоритмів шифрування, які використовуються в мобільних сенсорних мережах, включають наступні:

1. AES (Advanced Encryption Standard): Цей алгоритм шифрування використовується широко і є стандартом для багатьох бездротових протоколів, таких як Wi-Fi і Bluetooth. Він забезпечує сильну безпеку і високу швидкість шифрування.

2. RSA (Rivest-Shamir-Adleman): Цей алгоритм базується на складності факторизації великих простих чисел і використовується для захисту ключів шифрування. RSA часто використовується в комбінації з іншими алгоритмами шифрування для забезпечення безпеки

3. ECC (Elliptic Curve Cryptography): Цей алгоритм шифрування базується на складних математичних обчисленнях на еліптичних кривих і забезпечує високий рівень безпеки при використанні коротших ключів порівняно з іншими алгоритмами.

4. ChaCha20: Цей потоковий алгоритм шифрування є альтернативою AES і забезпечує високу швидкість шифрування при низькому споживанні енергії. Він стає все більш популярним в мобільних пристроях.

Окрім цих алгоритмів, постійно проводяться дослідження та розробки нових алгоритмів шифрування, щоб відповідати зростаючим вимогам безпеки та ресурсам мобільних пристроїв. Наприклад, нейромережі та квантові алгоритми шифрування можуть мати потенціал для майбутнього розвитку в цій галузі.

Алгоритми шифрування в мобільних сенсорних мережах постійно розвиваються і вдосконалюються. Ось декілька шляхів, якими вони розвиваються:

1- Академічні дослідження: Університети, дослідницькі лабораторії та інші науково-дослідні установи проводять дослідження з метою створення нових алгоритмів шифрування або вдосконалення існуючих. Ці дослідження включають аналіз поточних алгоритмів, пошук уразливостей і розробку нових методів шифрування, які були б безпечні, ефективні та відповідали більшим вимогам мобільних сенсорних мереж.

2- Стандартизація: Організації, такі як Національний інститут стандартів і технологій (NIST) в США та Міжнародна електротехнічна комісія (IEC), ведуть роботу з розробки та стандартизації алгоритмів шифрування. Це включає проведення конкурсів для вибору нових стандартів шифрування та розгляд пропозицій від різних організацій та дослідників.

3- Відкритий доступ і спільнота: Багато алгоритмів шифрування, таких як AES, є відкритими та доступними для загального використання. Це сприяє перевірці їх безпеки та виявленню потенційних проблем. Спільнота криптографів та безпекових експертів також активно співпрацює для обговорення нових ідей, виявлення уразливостей і покращення існуючих алгоритмів шифрування.

4- Технологічні зміни: Розвиток мобільних пристроїв і їх обчислювальних можливостей впливає на розвиток алгоритмів шифрування. Нові технології, такі як квантові обчислення, можуть відкрити нові можливості для шифрування даних в мобільних сенсорних мережах.

Всі ці шляхи співпрацюють, щоб забезпечити постійний розвиток алгоритмів шифрування в мобільних сенсорних мережах і забезпечити захист даних та безпеку користувачів у цих мережах.

СУТНІСТЬ ТА ОСОБЛИВОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Хропост Павло Вікторович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Телекомунікаційні системи спеціального призначення використовуються для забезпечення зв'язку та обміну інформацією в рамках спеціальних вимог та завдань, які необхідні для діяльності певних організацій або установ. Особливості таких систем полягають

у їхній спрямованості на вирішення конкретних завдань і вимог щодо безпеки, надійності та конфіденційності інформації.[2]

Основні сутність і особливості телекомунікаційних систем спеціального призначення включають:

Безпека і захист інформації: Телекомунікаційні системи спеціального призначення мають високі вимоги до захисту інформації від несанкціонованого доступу, перехоплення та зламу. Вони використовують спеціальні механізми шифрування, протоколи безпеки та інші заходи для забезпечення конфіденційності та цілісності даних.

Безпека і захист інформації є однією з найважливіших особливостей телекомунікаційних систем спеціального призначення. Оскільки ці системи використовуються в критичних сферах, таких як військові, правоохоронні агентства, урядові установи та інші організації, вони повинні забезпечувати найвищий рівень захисту інформації.

Для забезпечення безпеки і захисту інформації телекомунікаційні системи спеціального призначення використовують такі механізми:

Шифрування даних: Використання шифрування дозволяє захистити інформацію від несанкціонованого доступу. Дані шифруються за допомогою криптографічних алгоритмів, що перетворюють їх у незрозумілу форму, доступну тільки авторизованим користувачам з правильними ключами. Такий підхід забезпечує конфіденційність даних.

Протоколи безпеки: Телекомунікаційної системи спеціального призначення використовують спеціальні протоколи безпеки для захисту передачі даних. Ці протоколи включають механізми аутентифікації, контролю цілісності даних та захисту від перехоплення.

Фізичний захист: Крім захисту даних під час їх передачі, телекомунікаційні системи спеціального призначення також забезпечують фізичний захист обладнання та інфраструктури. Це включає контроль доступу до приміщень, використання захищених областей для розміщення серверів та мережевого обладнання, а також захист від несанкціонованого зв'язку та перешкод.

Надійність: Телекомунікаційні системи спеціального призначення повинні забезпечувати надійну передачу інформації навіть в умовах високого навантаження, перешкод та аварій. Вони використовують резервування каналів, механізми коригування помилок та інші технології для забезпечення надійності передачі даних.[1]

Надійність є важливою характеристикою телекомунікаційних систем спеціального призначення. Оскільки ці системи використовуються в критичних сферах, таких як військові операції, екстрені ситуації або командування та контроль, надійна передача інформації є необхідною.

Основні методи забезпечення надійності телекомунікаційних систем спеціального призначення включають:

Резервування каналів: Телекомунікаційні системи спеціального призначення використовують дублювання та резервування каналів для забезпечення неперервної передачі даних. Це означає, що в разі відмови або збою в одному каналі, інформація автоматично перемикатиметься на інший резервний канал, що забезпечує безперебійну роботу системи.

Механізми коригування помилок: Телекомунікаційні системи спеціального призначення використовують спеціальні механізми коригування помилок для виявлення та виправлення помилок, що можуть виникнути під час передачі даних. Це дозволяє забезпечити точність та цілісність передачі інформації навіть при наявності шуму, перешкод або помилок в каналах зв'язку.

Мережева архітектура з резервуванням: Телекомунікаційні системи спеціального призначення використовують мережеві архітектури з резервуванням, які дозволяють автоматично виявляти та усувати відмови в мережі.

Спеціалізовані вимоги: Телекомунікаційні системи спеціального призначення мають конкретні вимоги, що відповідають особливостям діяльності організацій, для яких вони

розробляються. Це може включати підтримку певних протоколів комунікації, спеціальних форматів даних.

Телекомунікаційні системи спеціального призначення враховують специфічні потреби та вимоги організацій, для яких вони розробляються. Це можуть бути такі спеціалізовані вимоги:

Підтримка спеціальних протоколів комунікації: Деякі організації мають власні спеціалізовані протоколи комунікації, які вимагаються для ефективної взаємодії та обміну інформацією. Телекомунікаційні системи спеціального призначення можуть бути розроблені з підтримкою цих протоколів, що дозволяє їм ефективно інтегруватися з існуючими системами та мережами.

Спеціальні формати даних: Деякі організації можуть використовувати спеціалізовані формати даних для обміну інформацією. Телекомунікаційні системи спеціального призначення можуть підтримувати ці формати та мати можливість конвертувати дані відповідно до вимог організації

Забезпечення інтеграції з іншими системами: Телекомунікаційні системи спеціального призначення можуть потребувати інтеграції з іншими системами, такими як системи керування, бази даних, аналітичні системи тощо. Вони повинні мати можливість обмінюватися даними з цими системами і забезпечувати зручну і ефективну роботу в єдиному інформаційному середовищі.

Отже, телекомунікаційні системи спеціального призначення враховують спеціалізовані вимоги організацій, для яких вони розробляються. Ці вимоги можуть включати підтримку спеціальних протоколів комунікації, спеціальних форматів даних, інтеграцію з іншими системами, а також надійність, масштабованість та продуктивність системи.

Розуміння та врахування цих спеціалізованих вимог дозволяє телекомунікаційним системам спеціального призначення ефективно виконувати свої завдання в конкретних областях, де вони застосовуються. Важливо розробляти системи, що відповідають унікальним потребам та вимогам організацій, забезпечуючи надійну, безпечну та ефективну передачу та обробку інформації.[3,4]

Список використаних джерел

1.Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі: Підручник [для вищих навчальних закладів] Київ : САММІТ-Книга, 2010. 708 с

2.Голь В.Д., Толстова А.В. Телекомунікаційні та інформаційні мережі. Керівництво з лабораторних занять та курсового проектування. Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2019. 45 с.

3.Методика проведення експертизи телекомунікаційної мережі : звіт про НДР / НАДПСУ, № 210-0018 І. – Хмельницький, 2010. – 98 с.

4.Наталенко П.П. Телекомунікаційні та інформаційні мережі : навчальний посібник. Київ : ВІТІ, 2011. 384 с.

ОГЛЯД МАРШРУТИЗАТОРІВ CISCO: АРХІТЕКТУРА ТА ФУНКЦІОНАЛЬНІСТЬ

Луцюк Іван Валерійович
Державний університет телекомінікацій
Навчально-науковий інститут телекомунікацій

Маршрутизатори Cisco є одними з найпоширеніших маршрутизаторів у світі мережевих технологій. Вони забезпечують надійне керування трафіком у мережі і можуть бути

використані в різних сценаріях, від невеликих домашніх мереж до великих корпоративних інфраструктур.

Архітектура маршрутизаторів Cisco базується на використанні операційної системи IOS (Internetwork Operating System), яка надає доступ до широкого спектру функціональності, такої як маршрутизація, комутація, безпека, QoS та інші. Крім того, маршрутизатори Cisco можуть бути конфігуровані за допомогою мови програмування CLI (Command Line Interface) або з використанням графічного інтерфейсу користувача.

Однією з ключових функцій маршрутизаторів Cisco є їх здатність працювати з різними протоколами маршрутизації, такими як OSPF, EIGRP, BGP та інші. Це дозволяє маршрутизаторам Cisco забезпечувати оптимальне керування трафіком в мережі і забезпечувати високу доступність.

Крім того, маршрутизатори Cisco можуть бути налаштовані для роботи з різними типами інтерфейсів мережі, включаючи Ethernet, Wi-Fi, T1/E1, DSL та інші. Це дозволяє маршрутизаторам Cisco бути універсальними інструментами для побудови будь-яких мереж.

У сучасних мережах безпека є критично важливим питанням. Маршрутизатори Cisco надають широкі можливості забезпечення безпеки мережі, включаючи захист від атак, віддалений доступ, захист протоколів та інші заходи безпеки. Наприклад, маршрутизатори Cisco можуть бути налаштовані для використання VPN-тунелей, що дозволяє захищати трафік від несанкціонованого доступу. Крім того, маршрутизатори Cisco можуть бути налаштовані для використання механізмів фільтрації пакетів, що дозволяє захищати мережу від різних видів атак.

Маршрутизатори Cisco - це потужні мережеві пристрої з високим рівнем безпеки та надійності, які забезпечують широкі можливості конфігурування мережі та надають розширену функціональність для оптимальної маршрутизації, контролю якості обслуговування, а також забезпечення безпеки мережі. Вони мають різні архітектури, які відрізняються за потужністю, масштабом та функціональністю, що дозволяє вибрати оптимальний варіант для вирішення конкретних бізнес-потреб.

Література:

1. Cisco Systems. (2021). Огляд маршрутизаторів Cisco. https://www.cisco.com/c/uk_ua/products/routers/index.html

2. Shukla, S., & Mishra, S. (2021). Understanding Cisco Router Architecture: A Comprehensive Guide. Springer.

3. Pal, M., & Gupta, N. (2017). Cisco routers for the desperate: Router and switch management, the easy way. Apress.

4. Nguyen, T. D., & Arora, R. K. (2015). Performance Analysis of Cisco Routers. International Journal of Computer Applications, 123(6), 25-30.

SIP-ТЕЛЕФОНІЯ ДЛЯ ВНУТРІШНЬООРГАНІЗАЦІЙНИХ ТА МІЖОРГАНІЗАЦІЙНИХ ЗВ'ЯЗКІВ

Глущенко Олексій Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

SIP (Session Initiation Protocol) — це протокол передачі даних. Його можна порівняти з мовою, що допомагає пристроям зрозуміти один одного і обмінюватися даними без помилок.

Він використовується для різноманітних цілей: для IP-телефонії, відео та аудіо конференцій, навіть онлайн-ігор. Він працює за схемою “клієнт-сервер”, постійно чергуючи запити і відповіді.

Як можна дзвонити і приймати дзвінки за допомогою SIP:

- за допомогою комп’ютера або ноутбука, якщо встановити на нього спеціальну програму (SIP-клієнт) і оснастити його навушником і мікрофоном;
- через WI-FI або 3g/4g за допомогою SIP-програм для планшетів і мобільних телефонів;
- використовуючи спеціальний стаціонарний SIP-телефон, який включаються в роутер;
- підключити звичайний телефон до VoIP-шлюзу, а сам шлюз — до роутера.

Основні функції SIP протокола

Функція	Опис
Розташування та реєстрація користувачів	Кінцеві точки (телефони) повідомляють SIP-проксі (оператора зв'язку) про своє місцезнаходження. SIP протокол визначає, які кінцеві точки братимуть участь у виклику
Доступність користувачів	SIP посилає кінцевим точкам запит INVITE (який містить опис сеансу зв'язку), щоб визначити, “відповідають” вони на виклик
Можливості	SIP узгоджує мультимедійну можливість кінцевих точок: чи зможуть вони взаємно підтримувати голосові кодеки
Налаштування сеансу	SIP протокол окрім INVITE, використовує ще 5 інших запитів, щоб організувати виклик (ACK, BYE, Register, Cancel)
Управління сесією	SIP використовується для передачі, завершення та зміни параметрів дзвінка в середині сеансу

Однією з крутих особливостей SIP є те, що це текстовий протокол, змодельований на основі моделі запиту/відповіді, яка використовується в HTTP. Це спрощує налагодження, оскільки повідомлення легко створювати (якщо ви розробник) та легко побачити (якщо ви адміністратор мережі).

Висновок: SIP-телефонія — чудове рішення для бізнесу, що тільки стартує, та для компаній, які прагнуть практично та зручно організувати бізнес-процеси. Це не тільки можливість заощадити, а шанс значно підвищити рівень обслуговування клієнтів, а також побудувати повноцінну аналітику для компанії. Саме тому SIP-телефонія набуває все більшої популярності.

ОСОБЛИВОСТІ ВОЛОКОННО-ОПТИЧНОГО КАБЕЛЯ

Сержанський Станіслав Станіславович
Державний університет телекомунікацій

Оптоволоконний кабель – конструкція з одного або кількох ізольованих один від одного оптичних волокон (оптоволокно), укладених в оболонку. Крім власне оптичних волокон і ізоляції може містити екран, силові елементи та інші конструктивні елементи. Також це фізичний медіум, що складається з певної кількості оптичних волокон, оточених спільною захисною оболонкою, та використовується для передачі світлового потоку.[1,с.1]

Оптичні кабелі розрізняють за матеріалом волокна, за місцем і умові монтажу і прокладки.

Оптичний кабель складається з певної кількості оптичних волокон, оточених загальною захисною оболонкою і складається з:

- серцевини,
- оптичної оболонки,
- захисного покриття,
- буферного покриття (опціонально).

Розрізняють одномодове і багатомодове волокно. Одномодове (SM) волокно буває: 8/125 і 9/125 мкм. Многомодове (ММ) волокно буває: 50/125 та 62/125 мкм. Одномодове волокно дешевше многомодового і дозволяє передавати оптичний імпульс на великі відстані, але в той же час приймальнопередавальне обладнання для нього значно дорожче. У багатомодового волокна збільшується розсіювання на виході і зменшується відстань передачі сигналу.[2,с.1]

Оптичне волокно є найсучаснішим та перспективним каналом для передачі великого масиву інформації з високою швидкістю та на далекі відстані.

Принцип поширення кванта електромагнітної енергії від передавача до приймача скляною трубкою був відомий ще в 19 столітті. Але лише у другій половині 20 століття вдалося створити оптичне волокно з низьким згасанням сигналу.

Спеціалісти прогнозують вже в недалекому майбутньому створення мереж з пропускною спроможністю вище за Тбіт/с. І ці сподівання пов’язані саме з розвитком волоконно-оптичних технологій.

Захисний шар лаку збільшує міцність волокна та захищає від подряпин та забруднення. Він також служить для фарбування волокон у модулі кабелю. Це необхідно для дотримання з’єднання “колір у колір” при монтажі або ремонті кабелю.

Оптичне волокно в спеціальних закритих барабанах поставляється на заводи, де на його основі виробляють різні марки волоконно-оптичного кабелю.

За своєю структурою оптичний кабель нагадує коаксіальний. У загальному випадку він складається з наступних елементів:

1. Осьовий елемент у вигляді склопластикового або металевого прутка для надання жорсткості кабелю.
2. Пластикові модулі заповнені гідрофобним гелем, в яких знаходяться оптичні волокна. Перший модуль завжди має червоне забарвлення. Поруч із ним розташовуєтьсядругий кольоровий модуль. У напрямку розташування цього модуля щодо годинникової стрілки нумеруються й інші. При ремонтно-монтажних роботах на них наклеюють відповідні бирки.
3. Плівка із гідрофобним покриттям, яка накладається зверху пластикових трубок.
4. Внутрішня поліетиленова оболонка для захисту від вологи.
5. Броньовий покрив із дроту або кевларових ниток.
6. Зовнішня оболонка із міцного поліетилену для захисту внутрішніх шарів кабелю.

Залежно від умов монтажу та призначення розрізняють такі види оптичного кабелю:

- для прокладання всередині приміщень

- для прокладання в ґрунт
- для монтажу в кабельних каналах
- для підвісу на опорах за допомогою троса
- для прокладання під водою

У маркуванні кабелю виробники вказують діаметр серцевини та оболонки – 9/125 або 50/125, за якою можна визначити тип волокна. Тут же вказується і кількість волокон, яка може бути від 2 до 144, залежно від призначення кабелю.

Для виробництва кабелю виробники розробляють свої ТУ, тому єдиної системи позначення оптичного кабелю немає. При виборі марки слід орієнтуватися на конкретний завод-виробник.[3,с.1]

ДОСЛІДЖЕННЯ ДОСТУПНИХ МІКРОКОНТРОЛЕРІВ ДЛЯ СИСТЕМИ РОЗУМНОГО БУДИНКУ

Ходаківський Дмитро Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Системи розумного будинку набувають все більшої популярності, оскільки вони дозволяють забезпечити зручність, енергоефективність та безпеку в побутових умовах. Ці системи базуються на мікроконтролерах - малих комп'ютерах, що виконують управління та контроль різних пристроїв і систем у будинку. Дослідження доступних мікроконтролерів є важливим кроком для визначення оптимального варіанту для реалізації системи розумного будинку.

Огляд доступних мікроконтролерів:

1. Arduino:

Arduino є одним з найпопулярніших і доступних мікроконтролерів на ринку. Він має велику спільноту користувачів, багато додаткових модулів та легку у використанні програмне забезпечення. Arduino підтримує різні мови програмування, такі як C і C++, і може бути використаний для реалізації різних функцій у системі розумного будинку.

2. Raspberry Pi:

Raspberry Pi - це ще один популярний мікроконтролер, який має значно більше обчислювальної потужності, порівняно з Arduino. Він базується на Linux-платформі і має можливості для підключення до мережі Інтернет. Raspberry Pi може бути використаний для реалізації складніших функцій у системі розумного будинку, таких як обробка відео, сервер даних тощо.

3. ESP8266 та ESP32:

ESP8266 та ESP32 - це недорогі мікроконтролери з підтримкою Wi-Fi, що робить їх ідеальними для систем розумного будинку з підключенням до Інтернету. Вони мають велику кількість входів/виходів (GPIO) та можуть бути програмовані за допомогою Arduino IDE або мови MicroPython. ESP8266 та ESP32 підходять для реалізації проектів з IoT-технологіями та безпроводовими комунікаціями.

4. STM32:

STM32 - це сімейство мікроконтролерів, що базуються на архітектурі ARM Cortex-M. Вони мають високу обчислювальну потужність, багато входів/виходів та широкі можливості підключення. STM32 підтримує різні мови програмування, включаючи мову C, і має багато

розширень та додаткових модулів, що робить його привабливим вибором для систем розумного будинку.

Вибір оптимального мікроконтролера:

Вибір оптимального мікроконтролера для системи розумного будинку залежить від конкретних вимог проекту. Потрібно врахувати такі фактори, як функціональні можливості, вартість, доступність, легкість програмування та розширюваність. Наприклад, якщо вам потрібен мікроконтролер з підтримкою Wi-Fi, ви можете звернути увагу на ESP8266 або ESP32. Якщо вам потрібні додаткові можливості обчислювальної потужності, Raspberry Pi або STM32 можуть бути кращими варіантами.

Висновок: Дослідження доступних мікроконтролерів є важливим етапом перед реалізацією системи розумного будинку. Різні мікроконтролери, такі як Arduino, Raspberry Pi, ESP8266, ESP32 та STM32, мають свої переваги та особливості, що робить їх відповідними для різних сценаріїв застосування. Вибір оптимального варіанту залежить від конкретних вимог та потреб проекту системи розумного будинку.

СУЧАСНІ МЕТОДИ РОЗРОБКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Зінченко Олександр Михайлович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Телекомунікаційні мережі - це комплекс технічних засобів та споруд, призначених для передавання та приймання інформації на відстань за допомогою електричних, оптичних або електромагнітних сигналів. Телекомунікаційні мережі можуть мати різну структуру, архітектуру, протоколи та технології, залежно від призначення, функціональності, масштабу та вимог до якості обслуговування.

Сучасні методи розробки телекомунікаційних мереж базуються на застосуванні нових принципів, стандартів, алгоритмів та інструментальних засобів, що дозволяють підвищити ефективність, надійність, безпеку та гнучкість телекомунікаційних систем. До таких методів належать:

- Використання інтегрованих сервісних мереж (ISDN), що дозволяють передавати різні типи інформації (голос, дані, відео) по одному каналу зв'язку.

- Використання мереж з пакетною комутацією (IP-мереж), що дозволяють динамічно розподіляти пропускну здатність мережі між різними користувачами та сервісами[1].

- Використання бездротових технологій (Wi-Fi, WiMAX, LTE, 5G), що дозволяють забезпечити мобільний доступ до телекомунікаційних мереж та послуг.

- Використання оптоволоконних ліній зв'язку (ОВЛ), що дозволяють передавати великі обсяги інформації з високою швидкістю та якістю.

- Використання супутникових систем зв'язку (GPS, GLONASS, Galileo), що дозволяють забезпечити глобальне покриття та навігацію.

- Використання хмарних технологій (Cloud Computing), що дозволяють зберігати, обробляти та надавати інформацію за допомогою віддалених серверів та мережевих ресурсів.

- Використання інтелектуальних технологій (AI, IoT, Big Data), що дозволяють аналізувати, оптимізувати та управляти телекомунікаційними мережами та сервісами за допомогою автоматизованих алгоритмів та пристроїв.

Сучасні методи розробки телекомунікаційних мереж сприяють розвитку інформаційного суспільства, економіки, освіти, науки, культури, медицини та інших сфер життєдіяльності людини. Вони також ставлять нові виклики та проблеми, пов'язані з безпекою, конфіденційністю, доступністю та якістю інформації. Тому необхідно постійно вдосконалювати та адаптувати сучасні методи розробки телекомунікаційних мереж до змінних умов та потреб суспільства.

Список використаних джерел:

1. Телекомунікаційні та інформаційні мережі. https://ela.kpi.ua/bitstream/123456789/45409/1/TIM_navch_posib.pdf.

МЕТОДИ ВИВЧЕННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Хропост Павло Вікторович
Державний Університет Телекомунікацій
Навчально-науковий інститут телекомунікацій

Телекомунікаційні системи спеціального призначення є невід'ємною складовою сучасного суспільства, забезпечуючи комунікаційні потреби важливих секторів, таких як оборона, безпека, надзвичайні ситуації та інші. Вивчення цих систем має вирішальне значення для їх ефективного функціонування, вдосконалення і впровадження нових технологій. У цій статті розглядаються методи вивчення телекомунікаційних систем спеціального призначення, їх напрацювання та перспективи для майбутнього розвитку цієї галузі.[3;4]

Моделювання та симуляція:

Один з ключових методів вивчення телекомунікаційних систем спеціального призначення - це використання моделювання та симуляції. Ці методи дозволяють створювати віртуальні моделі систем, що досліджуються, та аналізувати їх роботу в різних умовах. Вони дозволяють оцінити продуктивність, ефективність та стійкість системи до зовнішніх впливів.

Аналіз сигналів і протоколів:

Дослідження телекомунікаційних систем спеціального призначення також включає аналіз сигналів і протоколів, що використовуються в цих системах. Цей аналіз дозволяє з'ясувати особливості передачі даних, швидкості передачі, помилок, а також виявити можливість атак та загроз безпеці.

Експериментальні дослідження:

Одним з важливих методів вивчення телекомунікаційних систем спеціального призначення є проведення експериментальних досліджень. Ці дослідження включають наочну перевірку реальних систем на майданчиках чи в спеціально обладнаних лабораторіях.

Вони дають можливість отримати практичні результати, оцінити функціональність системи в реальних умовах та виявити потенційні проблеми.[1]

Аналіз даних та статистичні методи:

Аналіз даних та використання статистичних методів є необхідною складовою методів вивчення телекомунікаційних систем спеціального призначення. Цей підхід дозволяє обробляти великі обсяги даних, отриманих з реальних вимірювань, моделювання або симуляції. Він допомагає здійснювати статистичний аналіз результатів, виявляти закономірності, залежності та тренди, що сприяють покращенню роботи системи.

Інженерія систем та оптимізація:

Методи вивчення телекомунікаційних систем спеціального призначення також включають інженерію систем та оптимізацію. Це означає розробку та вдосконалення архітектури, протоколів, алгоритмів та компонентів системи з метою забезпечення максимальної продуктивності, надійності та ефективності. Інженерія систем включає аналіз вимог, проектування, тестування та впровадження нових рішень.

Методи вивчення телекомунікаційних систем спеціального призначення є важливою складовою їх розвитку та вдосконалення. Використанвання методів моделювання, симуляції, аналізу сигналів, експериментальних досліджень, аналізу даних та статистичних методів, а також інженерії систем та оптимізації дозволяє отримати глибоке розуміння принципів функціонування та виявити потенційні проблеми телекомунікаційних систем спеціального призначення.

Напрацювання на основі цих методів стимулює розвиток нових технологій та покращення комунікаційних систем спеціального призначення.[2]

Наприклад, результати досліджень можуть використовуватися для впровадження нових протоколів передачі даних, розробки більш ефективних алгоритмів передачі, а також для забезпечення кращої стійкості до зовнішніх впливів та загроз безпеці.

Перспективи розвитку методів вивчення телекомунікаційних систем спеціального призначення полягають у вдосконаленні інструментів моделювання та симуляції, розширенні масштабу експериментальних досліджень, розвитку нових аналітичних методів обробки даних та застосуванні штучного інтелекту для автоматизації аналізу та оптимізації систем.

Загалом, методи вивчення телекомунікаційних систем спеціального призначення грають важливу роль у забезпеченні надійності, ефективності та безпеки цих систем. Подальше дослідження та застосування цих методів сприятимуть розвитку телекомунікаційного сектору та забезпеченню задоволення комунікаційних потреб важливих галузей суспільства.[3;4]

Список використаних джерел

1. Воробієнко П.П. Телекомунікаційні та інформаційні мережі: підручник/ П.П.Воробієнко, Л.А. Нікітюк, П.І. Резніченко. К.: САММІТ-Книга, 2010. – 708с
2. Довгий С.О., Савченко О.Я., Воробієнко П.П. та ін.Сучасні телекомунікації: мережі, технології,економіка, управління, регулювання / За ред.С.О. Довгого. – К.: Український Видатничій Центр,2002. – 520 с
3. Стеклов В.К., Беркман Л.Н. Проектування телекомунікаційних мереж: навчальний посібник. Київ : “Техніка”, 2003. 923 с.
4. Стеклов В.К., Беркман Л.Н. Телекомунікаційні мережі : навчальний посібник. Київ : “Техніка”, 2001. 526 с.

ОЦІНКА РІЗНИХ МЕТОДОЛОГІЙ РЕЗЕРВНОГО КОПІЮВАННЯ ДАНИХ ДЛЯ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Подобєдов Максим Ігорович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

У сучасну цифрову епоху, дані є одним із найцінніших активів підприємства будь-якої сфери діяльності. Втрата даних через системні збої, кібератаки чи стихійні лиха може мати значний вплив на діяльність організації, її репутацію та фінансову стабільність. Тому для підприємств надзвичайно важливо впровадити ефективні методології резервного копіювання

даних, для забезпечення балансу між надійністю, кількістю задіяних ресурсів та часом відновлення своїх даних.

Для корпоративних інформаційних систем доступно декілька методологій резервного копіювання даних, кожна з яких має свої переваги та недоліки.

Першим і, мабуть, найбільш традиційним методом резервного копіювання даних є резервне копіювання на стрічку. Резервне копіювання на стрічку передбачає використання магнітних стрічок для зберігання копій даних. Цей метод підходить для підприємств, які не мають великих обсягів даних для резервного копіювання або потребують частих резервних копій. Даний метод почав використовуватися ще з 1950 років. Переваги даного методу — економічність, великий обсяг пам'яті відносно своєї ціни, портативність, у випадку транспортування за межі підприємства, довговічність відносно жорстких дисків, висока надійність у порівнянні з іншими методами резервного копіювання. Недоліки даного методу — повільний час резервного копіювання та відновлення, обмежений доступ до даних, вразливість до факторів навколишнього середовища, можливі проблеми сумісності з новими комп'ютерними системами.

Друга методологія — це резервне копіювання на диск, яке передбачає копіювання даних на дисковий пристрій. Цей метод швидший, ніж резервне копіювання на стрічку, і може виконувати резервне копіювання часто, іноді навіть у режимі реального часу. Резервне копіювання на основі диска також забезпечує швидший час відновлення даних, ніж резервне копіювання на стрічку. Однак резервне копіювання на основі диска може бути дорожчим, ніж резервне копіювання на стрічку, і може потребувати спеціального обладнання та програмного забезпечення.

Третя методологія — резервне копіювання в хмарі, яке передбачає зберігання резервних копій даних у хмарі. Хмарне резервне копіювання стає все більш популярним завдяки своїй масштабованості, гнучкості та економічній ефективності. Хмарні рішення для резервного копіювання можуть надавати безпечні та надійні послуги резервного копіювання організаціям будь-якого розміру. Однак хмарні рішення для резервного копіювання вимагають надійного та швидкого підключення до Інтернету, і існують проблеми щодо безпеки та конфіденційності даних. Четвертою методологією є гібридне резервне копіювання, яке поєднує дві або більше методологій резервного копіювання для створення комплексного рішення резервного копіювання.

Четверта методологія — Аварійне відновлення як послуга (DRaaS) — це нова методологія резервного копіювання даних, яка набирає популярності. DRaaS передбачає аутсорсинг аварійного відновлення сторонньому постачальнику, який керує даними та відновлює їх у разі аварії. Це економічно ефективне рішення для компаній з обмеженими IT-ресурсами, оскільки воно зменшує потребу в локальному обладнанні та персоналі. Однак для DRaaS потрібне надійне підключення до Інтернету, і він може не підходити для компаній, які мають великі обсяги даних для резервного копіювання.

Підсумовуючи, вибір правильної методології резервного копіювання даних для інформаційної системи підприємства вимагає ретельного розгляду потреб підприємства, ресурсів і бюджету. Резервне копіювання на стрічку, резервне копіювання диска, хмарне резервне копіювання та DRaaS — це життєздатні варіанти, кожен зі своїми перевагами та недоліками. Зрештою, найкраща стратегія резервного копіювання даних – це та, яка відповідає конкретним потребам бізнесу та забезпечує надійне та безпечне резервне копіювання та відновлення даних.

Вибираючи метод резервного копіювання для інформаційних систем підприємства, необхідно враховувати кілька факторів:

- Обсяг даних: вибраний метод резервного копіювання має відповідати об'єму даних, які потрібно створити резервну копію. Для великих обсягів даних рекомендується використовувати дискові рішення для резервного копіювання.

- Частота резервного копіювання: частота резервного копіювання повинна визначатися критичністю даних і швидкістю змін. Для дуже важливих даних або даних, які часто змінюються, рекомендується виконувати резервне копіювання принаймні раз на день.
- Цільовий час відновлення: Цільовий час відновлення (RTO) – це кількість часу, необхідного для відновлення даних після збою системи. Метод резервного копіювання повинен відповідати вимогам RTO організації.
- Безпека: метод резервного копіювання має гарантувати, що резервні копії даних є безпечними та захищеними від несанкціонованого доступу або крадіжки.
- Масштабованість: метод резервного копіювання має бути масштабованим, здатним обробляти майбутнє зростання даних та інформаційних систем.
- Вартість: слід враховувати вартість методу резервного копіювання, включаючи апаратне забезпечення, програмне забезпечення та витрати на поточне обслуговування.
- Надійність: метод резервного копіювання має бути надійним, давати змогу виконувати резервне копіювання послідовно та без помилок.

Врахування цих факторів під час вибору методу резервного копіювання може допомогти переконатися, що вибраний метод відповідає потребам організації та забезпечує ефективний захист інформаційних систем підприємства.

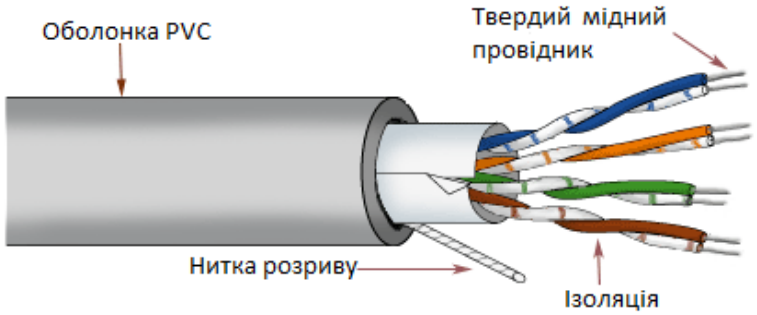
Список використаних джерел:

1. Computer Backup. URL: https://www.acronis.com/en-us/blog/posts/computer-backup/ (дата звернення: 15.04.2023).

КОНФІГУРАЦІЯ ЛОКАЛЬНОЇ МЕРЕЖІ ІЗ ВИКОРИСТАННЯМ КАБЕЛЮ ВИТОЇ ПАРИ

Харченко Олександр
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Вита пара - вид кабелю зв'язку, являє собою одну або кілька пар ізольованих провідників, скручених між собою, покритих пластиковою оболонкою.



Звивання провідників проводиться з метою підвищення ступеня зв'язку між собою провідників однієї пари і подальшого зменшення електромагнітних перешкод від зовнішніх джерел, а також взаємних наведень при передачі диференціальних сигналів. Для зниження зв'язку окремих пар кабелю в кабелях UTP категорії 5 і вище дроти пари звиваються з різним кроком. Вита пара - один з компонентів сучасних структурованих кабельних систем. Використовується в телекомунікаціях і в комп'ютерних мережах як фізичне середовище передачі сигналу в багатьох технологіях, таких як Ethernet, Arcnet і Token ring. На даний момент часу, завдяки своїй дешевизні і легкості в монтажі, є найпоширенішим рішенням для побудови дротових локальних мереж.

Залежно від наявності захисту - електрично заземленої мідної сітки або алюмінієвої фольги навколо скручених пар, визначають різновиди даної технології:

- неекранована вита пара (англ. UTP - Unshielded twisted pair) - без захисного екрану;
- фольгована вита пара (англ. FTP - Foiled twisted pair), також відома як F / UTP) - присутній один загальний зовнішній екран у вигляді фольги;
- екранована вита пара (англ. STP - Shielded twisted pair) - присутній захист у вигляді екрану для кожної пари і загальний зовнішній екран у вигляді сітки;
- фольгована екранована вита пара (англ. S / FTP - Screened Foiled twisted pair) - зовнішній екран з мідної обплетення і кожна пара в фольгованої оплетке;
- незахищена екранування вита пара (SF / UTP - або з англ. Screened Foiled Unshielded twisted pair) Відмінність від інших типів кручених пар полягає в наявності подвійного зовнішнього екрана, зробленого з мідної обплетення, а також фольги.

Існує декілька категорій кабелю витої пари, які нумеруються від CAT1 до CAT7 і визначають ефективний частотний діапазон. Кабель вищої категорії зазвичай містить більше пар дротів і кожна пара має більше витків на одиницю довжини. Категорії неекранованої витої пари описуються в стандарті EIA / TIA 568 (Американський стандарт проводки в комерційних будівлях) і в міжнародному стандарті ISO 11801.

Для того щоб розібратися чи підходить нам даний спосіб об'єднання двох локальних мереж звернемося до різновидів технології передачі даних Ethernet. Залежно від швидкості передачі даних і передавального середовища існує декілька варіантів технології. Більшість Ethernet-карт і інших пристроїв має підтримку декількох швидкостей передачі даних, використовуючи автовизначення швидкості і дуплексності, для досягнення найкращого з'єднання між двома пристроями. Якщо автовизначення не спрацьовує, швидкість підстроюється під партнера, і включається режим напів-дуплексної передачі. Наприклад, наявність в пристрої порту Ethernet 10/100 говорить про те, що через нього можна працювати за технологіями 10BASE-T і 100BASE-TX, а порт Ethernet 10/100/1000 - підтримує стандарти 10BASE-T, 100BASE-TX і 1000BASE- T.

Опис роутерів, швидкість портів Ethernet 10/100/1000 Мбіт/с, то вони підтримують стандарти:

- 100BASE-T - загальний термін для позначення стандартів, які використовують в якості середовища передачі даних виту пару. Довжина сегмента до 100 метрів. Включає в себе стандарти 100BASE-TX, 100BASE-T4 і 100BASE-T2.
- 100BASE-TX, IEEE 802.3u - розвиток стандарту 10BASE-T для використання в мережах топології «зірка». Задіяна кручена пара категорії 5, фактично використовуються тільки дві неекрановані пари провідників, підтримується дуплексна передача даних, відстань до 100 м.
- 1000BASE-T, IEEE 802.3ab - стандарт, який використовує виту пару категорій 5e. У передачі даних беруть участь 4 пари. Швидкість передачі даних - 250 Мбіт/с по одній парі. Використовується метод кодування PAM5, частота основної гармоніки 62,5 МГц. Відстань до 100 метрів.

Список використаних джерел:

1. Кульгін М.С. Комп'ютерні мережі. Практика побудови – СПб, Пітер, 2007 – 462 с.
2. Нанс Б. Комп'ютерні мережі: Пров. з англ. – М.: «БІНОМ», 2006. – 400 с.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Кирсенко Андрій
Державний університет телекомунікацій

Впровадження штучного інтелекту (ШІ) в різних сферах людського життя має великий потенціал для покращення ефективності і зручності процесів. Однією з галузей, де застосування ШІ має особливу вагу, є телекомунікаційна індустрія. Використання штучного інтелекту в телекомунікаційних системах сприяє покращенню якості комунікації, надійності мереж та забезпеченню безпеки даних.

Однією з основних переваг використання штучного інтелекту в телекомунікаційних системах є покращення ефективності мереж. ШІ дозволяє автоматизувати процеси моніторингу, аналізу та оптимізації мережевих структур. Наприклад, системи, що використовують нейронні мережі, можуть аналізувати великі обсяги даних та прогнозувати навантаження на мережу, що дозволяє забезпечити оптимальне розподілення ресурсів. Це сприяє зменшенню перебоїв у роботі мережі, підвищує швидкість передачі даних та поліпшує загальну якість зв'язку для користувачів.

Крім того, використання ШІ у телекомунікаційних системах сприяє підвищенню надійності мереж та прогнозуванню можливих несправностей. За допомогою машинного навчання і аналізу великих обсягів даних, системи ШІ можуть виявляти аномалії, передбачати виникнення проблем та приймати відповідні заходи з попередження або виправлення несправностей. Це сприяє зменшенню часу простою мереж та забезпечує більш швидкий відгук на проблеми, що виникають.

Однак, однією з найважливіших аспектів використання ШІ в телекомунікаційних системах є забезпечення безпеки даних. З розвитком технологій з'єднання мереж та збільшення обсягів передачі даних, виникає багато викликів у забезпеченні захисту інформації. ШІ може використовуватись для виявлення та запобігання кібератак, виявлення шкідливих програм та інших загроз безпеці мережі. Застосування алгоритмів машинного навчання дозволяє виявляти недостатні заходи безпеки, прогнозувати нові загрози та вчасно реагувати на них, що забезпечує захист важливої інформації та приватності користувачів.

Одним з прикладів використання ШІ в телекомунікаційних системах є вирішення проблеми забруднення мережевого трафіку небажаними повідомленнями (спамом). Використовуючи алгоритми машинного навчання, системи можуть автоматично виявляти спамові повідомлення та блокувати їх перед появою в поштовій скринці користувача. Це сприяє покращенню ефективності роботи з електронною поштою та підвищенню задоволення користувачів від використання телекомунікаційних послуг.

Висновок

Використання штучного інтелекту в телекомунікаційних системах має значний потенціал для покращення якості комунікації, ефективності мереж та безпеки даних. ШІ дозволяє автоматизувати процеси аналізу, оптимізації та прогнозування, що покращує якість зв'язку та надійність мереж. Крім того, використання алгоритмів машинного навчання дозволяє ефективно боротися з кіберзагрозами та забезпечувати безпеку даних. Застосування ШІ є необхідним кроком у розвитку телекомунікаційної індустрії і сприяє поліпшенню якості та доступності телекомунікаційних послуг для користувачів.

ПРОЕКТУВАННЯ ЛОКАЛЬНИХ МЕРЕЖ

Харченко Олександр
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Загальні принципи організації локальних мереж

Локальною мережею вважається об'єднання двох та більше пристроїв за допомогою кабелю, радіохвиль чи оптичних сигналів, при якому стає можливим обмін даними між ними. Пристрої, котрі розміщенні в одному приміщенні чи будівлі і пов'язані між собою, називають локальною комп'ютерною мережею (LAN – Local Area Network). Кількість пристроїв, які можуть бути підключеними до такої мережі, обмежується можливостями кабельної системи і мережевого обладнання.

Зв'язок між пристроями може бути прямим або з використанням додаткових вузлів зв'язку.

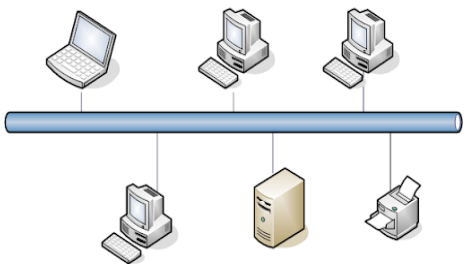
Мережа являє собою магістральну інформаційну структуру, яка складається із логічного і фізичного рівнів або складових, основною метою яких є обмін інформацією.

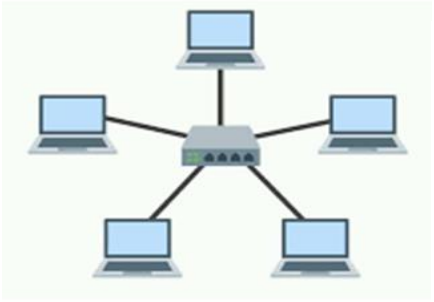
Комп'ютери та інші компоненти локальної мережі можуть бути з'єднаними між собою декількома шляхами. Використана схема фізичного розташування мережевих компонентів називається топологією. Топологія мережі визначається геометричною фігурою, яка створена лініями зв'язку між комп'ютерами, або фізичним розташуванням по відношенню одне від одного комп'ютерів, котрі пов'язані між собою. Топологія мережі може бути одним із фактором для порівняння і класифікації різноманітних комп'ютерних мереж.

Виділяють декілька видів топології мережі:

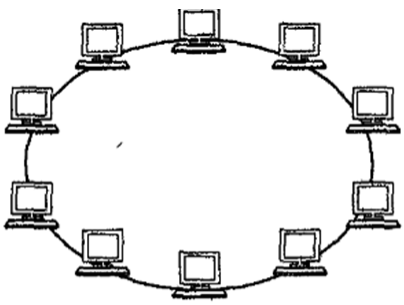
- спільна шина;
- зірка;
- кільце;
- комірка (Mesh);
- змішана.

Топологія зі «спільною шиною»

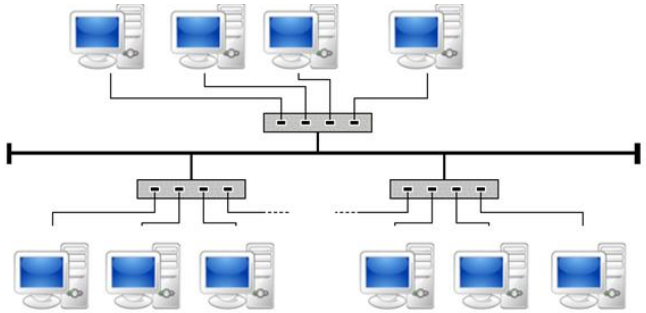




Топологія «Зірка»



Топологія «Кільце»



Мережа з топологією «зірка-шина»

У випадку використання спільної шини всі комп'ютери підключаються через один кабель, який називається шиною даних. При цьому пакет буде прийматися всіма комп'ютерами, які підключені до даного сегменту мережі.

Зоряна топологія - одна з найпоширеніших мережевих налаштувань. У цій конфігурації кожен вузол підключається до центрального мережевого пристрою, наприклад концентратора, комутатора чи комп'ютера. Пристрій центральної мережі працює як сервер, а периферійні пристрої виступають клієнтами. Залежно від типу мережевої карти, що використовується в кожному комп'ютері зіркової топології, для з'єднання комп'ютерів використовується коаксіальний кабель або мережевий кабель RJ-45.

У топології кільця комп'ютери з'єднані одним кільцеподібним кабелем. На відміну від топології шини, немає припинених кінців. Сигнали передаються в циклі в одному напрямку і передаються через кожен комп'ютер. Кожен комп'ютер служить ретранслятором для посилення сигналу та передачі його на наступний комп'ютер. У великих системах декілька локальних мереж можуть бути з'єднані між собою в кільцевій топології. Для цього використовували коаксіальні або волоконно-оптичні кабелі ThickNet.

Змішана топологія (зірка-шина) з'єднує в собі дві або більше топології, утворюючи тим самим завершену мережеву структуру. На даний момент така мережа є найпоширенішою; найбільш часто об'єднують зірко подібну і шинну топологію.

При використанні топології «зірка-шина» кілька мереж, котрі мають зіркоподібну топологію, які підключені до однієї шині.

Список використаних джерел:

1. Мінаєв І.Я. Локальна мережа своїми руками. Самовчитель – М., ТЕХНОЛОГІЇ – 3000, 2004 – 368 с.
2. Оліфер В.Г. Комп'ютерні мережі. Підручник – СПб, Пітер, 2010 – 672 с.
3. Холмогоров В. Комп'ютерна мережа своїми руками. Самовчитель – СПб, Пітер, 2009 – 171 с.
4. Сергєєв А.П. Офісні локальні мережі. Самовчитель – М., Вільямс, 2006 320 с.

ТЕНДЕНЦІЯ РОЗВИТКУ РАДІОЕЛЕКТРОНІКИ ТА ЕЛЕКТРОЗВ'ЯЗКУ В УКРАЇНІ

Макаров Б.О.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Радіоелектроніка та електрозв'язок є важливою складовою сучасного технологічного прогресу. В Україні ці галузі також демонструють високий розвиток, пристосовуючи до нових

вимог та впроваджуючи передові технології. У цій невеликій статистиці я розглянув основні тенденції розвитку радіоелектроніки та електрозв'язку в Україні.

По-перше, слід зазначити, що Україна має сильний потенціал у сфері радіоелектроніки. В Україні працюють багато наукових установок, дослідних центрів та виробничих підприємств, які займаються науковими дослідженнями та виробництвом радіоелектронних компонентів, приладів та систем. Важливим напрямком розвитку є впровадження нових технологій у виробництво, таких як нанотехнології, високочастотна електроніка та інтегральні мікросхеми.

По-друге, зростає значення бездротових технологій у сфері електрозв'язку. Мобільний зв'язок, бездротовий інтернет, сенсорні прилади – все це споживає високоефективних та надійних бездротових комунікаційних систем. Україна активно працює над розвитком державних стандартів та технологій у своїй країні. Наприклад, нещодавно був оновлений стандарт 5G, який дозволяє передавати дані з надійною швидкою швидкістю та надійним завантаженням.

По-третє, розширюватиметься застосування радіоелектронних систем у різних галузях. Наприклад, автомобільна промисловість активно використовує радари та системи допомоги водіям для забезпечення безпеки на дорогах. Іноді радіоелектроніка застосовується в медицині, промисловості та в інших сферах.

По-четверте, значна увага приділяється розвитку високошвидкісних оптичних мереж та інтернет речей (IoT). Оптичні заходи забезпечують високу пропускну здатність, що дозволяє передавати більші обсяги даних в реальному часі. IoT відкриває безособові можливості у сфері автоматизації, управління та моніторингу різних процесів.

Узагальнюючи, розвиток радіоелектроніки та електрозв'язку в Україні можна сказати, що країна активно впроваджує передові технології, розробляє стандарти та системи та залишається важливим гравієм на міжнародних аренах. Завдяки розвитку цих галузей в Україні, з'являються нові можливості для наукових досліджень, розвитку інновацій та підтримки високотехнологічних виробництв.

Література

1. Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку. URL:https://nkrzi.gov.ua/index.php?r=site/index&pg=1&language=uk

СУТНІСТЬ ТА ОСОБЛИВОСТІ NFC

Муравчик Кирило Станіславович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

В данній тезі будуть наведені відповіді на питання що таке взагалі NFC , звідки до нас прийшло , принцип роботи , та використання його в повсякденному житті .

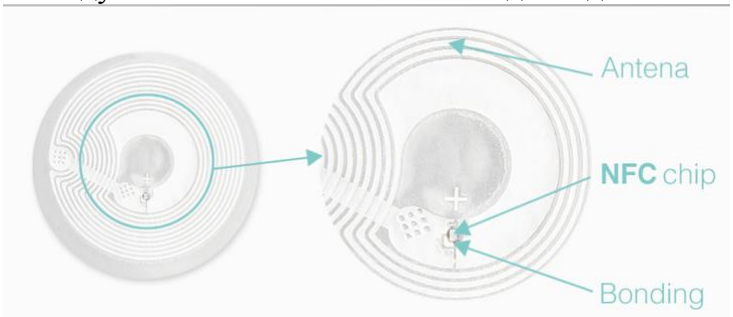
NFC означає Near Field Communication. Це технологія бездротового зв’язку, яка дозволяє двом пристроям обмінюватися даними, коли вони наближаються один до одного, як правило, це відбувається на відстані кількох сантиметрів. Технологія NFC базується на технології радіочастотної ідентифікації RFID (Radio Frequency IDentification що в перекладі означає -радіочастотна ідентифікація) і забезпечує безпечний зв’язок між пристроями, працює завдяки частоті 13,56 МГц.

Розвиток технології NFC можна простежити з 1980-х років, коли дослідники різних компаній і університетів досліджували способи використання радіохвиль для зв’язку на

короткій відстані. Технологія NFC була вперше представлена на початку 2000-х років консорціумом компаній, включаючи Nokia, Sony і Philips, які сформували Форум NFC який є консорціумом компаній з електроніки, телекомунікацій і платежів. Перші телефони з підтримкою NFC були представлені в 2006 році, і з того часу ця технологія все частіше використовується в різних програмах: таких як мобільні платежі, оформлення квитків на транспорт , системи контролю доступу, лояльність і маркетинг, а також охорону здоров'я .

Принцип роботи NFC включає два основні компоненти: пристрій читання/запису NFC і тег NFC. Пристрій зчитування/запису NFC генерує електромагнітне поле, яке живить тег NFC і забезпечує зв'язок між двома пристроями. Коли тег NFC потрапляє в зону дії пристрою зчитування/запису NFC, він використовує електромагнітне поле для генерування невеликого електричного струму, який живить тег і дозволяє йому надсилати інформацію назад до пристрою зчитування. Тег NFC містить невелику антену та мікрочіп, який зберігає інформацію, таку як контактна інформація, URL-адреси та платіжні дані. Фізично технологія NFC влаштована дуже просто:

- **Котушка-антена**. Спіраль із металевого матеріалу, в якій виникає індукційний струм.
- **Кремнієвий чип**. Він дуже маленький і може мати від 128 до 888 байт вільної пам'яті.



Таке влаштування дозволяє програмувати NFC-мітки (теги). На подібну мітку можна записати певну команду, яка виконуватиметься, коли ви підносите до неї телефони, годинники або ключі . Випускаються теги у вигляді наклейок, брелків, карток. Ці мітки досить дешеві – на момент написання статті від 18 гривень за штуку зараз можливо дорожче. Для програмування мітки не потрібне спеціальне обладнання. Достатньо лише смартфона з NFC. На нього потрібно встановити програму NFC Tools Pro (версія для iPhone, для Android), TagWriter (для iPhone, Android), Kevo (для iPhone, Android) або подібні. Хороша новина: вони дозволяють задати чимало команд. Погана: подібні програми дуже незручні, і доведеться витратити час, щоб розібратися. Зате коли ви розберетесь, відкриється багато цікавих способів використання тегів. Варіанти застосування в побуті та в бізнесі я навожу нижче.

Сьогодні технологія NFC є ключовою функцією багатьох смартфонів, нею користуються мільйони людей у всьому світі. Його популярність пояснюється простотою використання, безпекою та зручністю, що робить його ідеальною технологією для різноманітних застосувань у нашому все більш зв'язаному світі. Наприклад з допомогою NFC можливо виконати наступні речі :

- **Керування розумним будинком**. Сценаріїв безліч. Наприклад, наклеїти мітки у книгу рецептів. Потім запрограмувати мітки на включення духовки на певний час і температуру (залежно від страви), і щоб паралельно запускалася витяжка. Або розмістити стікер біля ліжка, і коли ви підноситимете до нього телефон, він переходитиме в беззвучний режим, а штори закриватимуться.

- **Швидка синхронізація гаджетів**. Наявність пасивного чипа в електроніці дозволяє проводити моментальну синхронізацію. Наприклад, NFC у телевізорі дозволяє швидко перетворити телефон на пульт або увімкнути на великому екрані медіафайли з пам'яті смартфона

- **NFC кільце**. Зручна фішка, якщо у вас є сумісний електронний дверний замок. Ви просто беретеся за дверну ручку, і двері відчиняються. Не потрібно шукати ключ у кишені чи відкривати програму на смартфоні. Перед покупкою такого кільця переконайтеся, що замок підтримує відкриття за допомогою NFC.

- **Домофон**. Ми згадували, що NFC та RFID – схожі технології. У деяких випадках ключ від домофону можна «клонувати» собі в телефон. Це робиться за допомогою NFC Card Emulator Pro (для Android), NFC Tools (для iPhone) або інших програм. Метод спрацьовує не завжди, тому що можуть не збігатися робочі частоти, або домофон може мати просунутий захист.

- **Нашийники для домашніх тварин**. В них використовується мітка, у якій записуються контактні дані власника. Якщо ваш домашній улюбленець загубиться, такий нашийник підвищить шанси, що з вами зв'яжуться люди, які його знайдуть.

- **Бездротове заряджання від смартфона**. У перспективі модуль NFC дозволить використовувати телефон як павербанк із підтримкою бездротової зарядки. Поки що це не реалізована, але теоретично можлива перевага. Ми згадували, що у роботі NFC-модуля використовується взаємоіндукція. Вона ж лежить в основі бездротової зарядки, тому потенційно модуль може використовуватися для зворотної зарядки. Вона буде повільною через маленьку потужність, але достатньою для підзарядки бездротових навушників або смарт-годинників.

Також наведу роботу NFC у бізнес-процесах

- **POS-термінал у смартфоні**. Функція, орієнтована на малий бізнес. Вона дозволяє приймати безготівкові платежі за допомогою телефону. Для цього потрібно завантажити одну з програм: ОщадPAY (ОщадБанк), Термінал (ПриватБанк), STARKASA (Київстар), Термінал у смартфоні (Райффайзен).

- **Пропускна система**. При встановленні сумісного зі стандартом NFC зчитувача, замість пластикових перепусток персонал зможе використовувати смартфон.

- **Інформація про товар**. Біля стендів з товарами можна залишати NFC-мітки, які відправлятимуть покупця на сторінку з детальною інформацією про продукт або відеоогляд.

- **Інтерактивна реклама**. Теги NFC розміщують на зовнішній рекламі. Втім, використовувати QR-коди в промоматеріалах дешевше, і вони зручніші для користувача, тому що їх можна відсканувати здалеку.

- **Обмін візитками**. На великих конференціях за допомогою NFC можна обмінюватись електронними візитками.

СИСТЕМИ IoT

Ручко В.В.
Державний університет телекомунікацій

Системи Інтернет речей (IoT) перетворюються на невід'ємну частину сучасного світу. Вони впливають на нашу повсякденну діяльність, дозволяючи нам підключати різноманітні пристрої до мережі Інтернет та обмінюватися даними з ними. Ця технологія відкриває безліч можливостей у різних сферах, включаючи промисловість, медицину, сільське господарство, транспорт та багато іншого.

Одним із ключових переваг систем IoT є збільшення ефективності у різних галузях. Приклад, у промисловості, системи IoT дозволяють контролювати роботу, забезпечену в режимі реального часу, збирати дані про енергопостачання та виявляти можливі поломки чи несправності. Це дозволяє здійснювати своєчасне технічне обслуговування та дізнатися про непередбачувані проблеми.

У галузях медицини системи IoT також бачиться важлива роль. Завдяки використанню спеціальних датчиків і пристроїв, лікарі можуть спостерігати за показниками здоров'я пацієнтів у режимі реального часу, навіть якщо вони знаходять вдома. Це дозволяє більш точно діагностувати стан хворих та вчасно реагувати на будь-які зміни.

Системи IoT також роблять значний внесок у розвиток сільського господарства. Вони дозволяють фермерам контролювати умови вирощування врожаю, а також збирати дані про довкілля наприклад: клімат та рівень вологості. За допомогою цього фермери можуть вживати ефективних заходів для збільшення врожаю.

Транспортні перевезення також використовують систему IoT в своїх цілях. Завдяки вбудованим датчиками та GPS, можна відстежувати місце знаходження транспорту, контролювати їхній стан та збирати дані про трафік. Це дозволяє скоротити час простою транспорту, оптимізувати маршрути та повністю забезпечити безпеку дорожнього руху.

Наостанок я би хотів сказати, що системи IoT може мати великий потенціал у різних галузях. Вони можуть змінити наш спосіб життя, забезпечуючи ефективність, зручність та безпеку. Проте, необхідно приділяти увагу питанням приватності та кібербезпеки, якщо забезпечити стійкість та успіх розвитку цих систем то у майбутньому, IoT просунеться та займе центральне місце у технологічному прогресі та сформує нашу цифрову епоху.

ОСНОВНІ ПРИНЦИПИ ОРГАНІЗАЦІЇ МЕРЕЖ NGN

Степаненко Юрій Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Мережі нового покоління (NGN) є еволюцією традиційних телекомунікаційних мереж, які забезпечують передачу голосу, даних та інших типів трафіку.

Основним принципом організації мереж NGN є забезпечення однакової якості обслуговування (QoS) для різних типів трафіку, таких як голосові дзвінки, відеоконференції та передача даних. Це досягається завдяки використанню технологій пакетної комутації даних, які дозволяють оптимізувати використання мережевих ресурсів та забезпечити більш ефективне керування трафіком.

Інший принцип полягає в тому, що мережі NGN мають бути орієнтовані на послуги (service-oriented), а не на технології. Це означає, що мережа повинна бути побудована таким чином, щоб забезпечити ефективну передачу різних типів послуг, таких як мультимедіа, мережеві ігри, IP-телефонія та інші.

Третій принцип організації мереж NGN - це забезпечення мережевої безпеки. Мережі NGN повинні бути забезпечені різноманітними механізмами захисту, такими як аутентифікація, авторизація та контроль доступу, щоб захистити мережеві ресурси від несанкціонованого доступу та атак.

Четвертий принцип - це гнучкість та масштабованість мережі. Мережа повинна бути побудована таким чином, щоб вона могла ефективно працювати та розширюватись в

залежності від потреб користувачів та розвитку технологій. Для цього можуть використовуватись різні механізми, такі як віртуалізація мережевих ресурсів, або використання облачних технологій.

Останнім принципом є забезпечення інтероперабельності та стандартизації. Це означає, що мережа повинна бути забезпечена механізмами, які дозволяють різним системам та пристроям взаємодіяти між собою, незалежно від їх виробника та моделі. Для цього використовуються різні стандарти, такі як SIP (Session Initiation Protocol), IMS (IP Multimedia Subsystem) та інші.

Усі ці принципи взаємодіють між собою та доповнюють один одного, забезпечуючи ефективну та надійну роботу мереж NGN. Ці принципи є основою для розробки та впровадження нових технологій телекомунікацій та їх інтеграції в мережі NGN.

Щоб забезпечити успішну реалізацію принципів організації мереж NGN, необхідно враховувати ряд технічних та організаційних викликів. Одним з найбільших технічних викликів є відмова від традиційних комутаторів на користь пакетної комутації. Це вимагає розробки та впровадження нових технологій, таких як MPLS (Multiprotocol Label Switching), яка забезпечує швидку та ефективну передачу даних.

Іншим технічним викликом є забезпечення високої якості обслуговування (QoS), що вимагає розробки та використання різноманітних механізмів для забезпечення мінімальної затримки, високої пропускної здатності та надійності.

Організаційні виклики пов'язані зі створенням сприятливого середовища для розробки та впровадження нових технологій. Це включає в себе встановлення сприятливих правил та стимулів для інвестицій у розвиток мереж NGN, підтримку стандартизації та регулювання телекомунікаційного ринку.

Наприкінці хотів би підкреслити, що впровадження мереж NGN є невід'ємною частиною розвитку телекомунікаційного сектору та може значно покращити якість та ефективність комунікацій. Однак, для досягнення успіху в цій галузі необхідно продовжувати працювати над технічними та організаційними викликами та розвивати нові технології, які забезпечать ефективну та надійну роботу мереж NGN.

АНАЛІЗ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ В УКРАЇНІ

Федосеєнко А.С.
Державний університет телекомунікацій

Сучасний світ входить у фазу надзвичайно важливого розвитку. Глобальні зміни стосуються всіх сфер людської діяльності. Майбутнє світу невизначено так само, як і майбутнє окремих напрямів його розвитку. Ця невизначеність є благодатним підґрунтям для розвитку та вдосконалення певних аспектів життя людини. На фоні цього проявляються деякі закономірності, які домінують у загальному розвитку суспільства. До таких закономірностей належить інформатизація суспільства. Передача, зберігання та обробка інформації стають головною рушійною силою розвитку суспільства. Отже, розвиток телекомунікацій має значущу роль в розвитку економічної та соціальної діяльності суспільства, забезпечує стабільну та швидку передачу інформації. Розвиток телекомунікацій – це перспективний напрямок, здійснюється паралельно розвитку економіки країни і є одним із основних параметрів успішного процвітання економіки країни.

Україна переживає певні кризові явища в економіці, але телекомунікації продовжують розвиватися, постійно випереджаючи показники зростання економіки країни.

Одночасно, темпи зростання окремих видів телекомунікаційних мереж та обсяги споживання послуг є недостатніми і це призводить до відносного відставання України у телекомунікаційній сфері. Оскільки телекомунікації є важливою інфраструктурною складовою в економіці України, то недостатній розвиток телекомунікацій зменшує темпи розвитку економіки України. Виходячи з вищесказаного, можна зазначити, що системний та регулярний аналіз процесів функціонування українських телекомунікацій є актуальним. Він має проводитися досконало, щоб попередити небажані процеси затримки розвитку. За допомогою постійного вивчення та вдосконалення телекомунікацій, проведення аналізу та усунення недоліків в роботі телекомунікаційних мереж ми прямо пропорційно впливаємо на розвиток своєї країни. Україна має великий кадровий потенціал вчених та розробників в галузі телекомунікацій та інформаційних технологій, отже потрібно зосередити увагу і наявний потенціал для розвитку даної сфери.

При аналізі розвитку телекомунікацій в Україні необхідно використовувати системний підхід. Телекомунікації України потрібно розглядати як єдину систему, хоча вона і має складну структуру: багато мереж, багато операторів зв'язку та ін., застосовуючи при цьому системний підхід. Перш за все, сферу комунікацій та її основні процеси регулює

Закон України "Про телекомунікації". В ньому чітко прописано принцип дії, основні положення та структура телеконунікацій України. Отже, при організації телекомунікаційних мереж чи запровадженні новітніх технологій, чи оновленні мереж а також інших новаціях ми повинні насамперед керуватися Законом.

Системний підхід використовується і в забезпеченні потреб споживачів у телекомунікаційних послугах. А задоволення потреб користувачів і отримання з них плати за надані послуги є основою діяльності господарюючих суб'єктів ринку телекомунікацій.

Також, системний підхід до розвитку телекомунікацій є необхідним при об'єднанні різних видів телекомунікаційних мереж в єдину багатооператорну і багатопровайдерську мережу наступного покоління (NGN). Цьому сприяє постійний технологічний прогрес у телекомунікаційній сфері.

Процес формування сучасних телекомунікацій був довгий та складний. В результаті цього процесу, телекомунікації України було лібералізовано і дерегульовано. Технічна політика розвитку телекомунікацій проводиться операторами телекомунікацій самостійно, спираючись на розвиток світових телекомунікацій та на можливість розвитку власного бізнесу шляхом використання технічних і програмних рішень із технічно розвинутих країн.

Держава регулює розвиток телекомунікацій шляхом тарифного регулювання, введення ліцензування, правил взаємодії між операторами та правил надання послуг.

Аналіз розвитку телекомунікацій у світі.

Потенціал розвитку українських телекомунікацій в більшості залежить від розвитку телекомунікацій в інших країнах світу. Швидкий та прогресивний розвиток телекомунікацій в інших країнах створює для України умови затримки у інформативному, соціальному та економічному розвитку. Створення та виробництво нового сучасного телекомунікаційного обладнання та нових програмних продуктів в технічно-розвинених країнах та можливість придбання їх Україною, водночас створює можливість розв'язання проблем розвитку українських телекомунікацій, вдосконалення цього процесу.

Основні проблеми розвитку телекомунікацій України були успадковані від попередньої історії їх розвитку. Основними проблемами слід вважати:

- відставання від більшості країн світу, по рівню забезпечення користувачів сучасними комунікаційними послугами;
- неоднакова забезпеченність користувачів засобами телекомунікацій по території країни;
- застарілість великої частини стаціонарних телекомунікаційних мереж;

- невдоволеність користувачів наявними телекомунікаційними послугами, особливо їх сучасними видами, в зв’язку з повільним розвитком сучасних телекомунікацій;

- проблеми з єдинством технічної та грошової політики в сфері телекомунікацій;

- труднощі із забезпеченням державної підтримки діяльності операторів в віддалених районах.

Резюмуючи вищенаведене, можемо сказати, що технічно-виробничий потенціал українських телекомунікацій досить застарілий, фізично та технічно зношений і має лиш незначні резерви, які можуть бути швидко задіяні для розвитку мереж наступного покоління. Так потрібна в Україні масовість сфери телекомунікацій потребує нового будівництва, новітніх технологій та задіяння кадрового потенціалу країни. Отже, потрібно ретельно планувати розвиток телекомунікацій в Україні, щоб досягти максимально можливої масовості та економічної ефективності.

Література

1. І.В. Горбатий, А.П. Бондарев “Телекомунікаційні системи та мережі Принципи функціонування, технології та протоколи”.

2. Г.Ф. Конахович, В.М. Чуприн, І.О. Мачалін, О.П. Ткаліч “Експлуатація телекомунікаційних систем”

СУЧАСНИЙ РОЗВИТОК СФЕРИ ТЕЛЕКОМУНІКАЦІЙ

Волонтир І.В
Державний університет телекомунікацій

Сучасний розвиток сфери телекомунікацій передбачає низку значних змін, включаючи стрімке зростання мобільних технологій, широке поширення бездротових мереж, підвищення швидкості передачі даних, розширення спектру послуг та зростання впливу Інтернету речей. Ці тенденції суттєво впливають на наш спосіб життя, роботу, комунікацію та взаємодію з оточуючим світом.

Спостерігається стрімке зростання мобільних технологій, що дозволяють людям бути постійно підключеними до мережі. Смартфони стали невід'ємною частиною нашого повсякденного життя, надаючи широкий спектр функцій, від звичайного телефону до портативного комп'ютера. Швидкий розвиток мобільних технологій відкриває нові можливості для комунікації, доступу до інформації та розваг. Завдяки бездротовим мережам, таким як 5G, ми можемо насолоджуватися високошвидкісним інтернетом, стрімінговим відео та миттєвим доступом до послуг в будь-якому місці та часі.

Окрім мобільних технологій, бездротові мережі знаходять все більше застосувань у сучасному світі. Розширення Wi-Fi технологій та розвиток мереж покриття широкого радіусу дозволяють людям підключатися до Інтернету у різних місцях, таких як кафе, громадські приміщення та транспортні засоби. Це сприяє зручності, забезпечує стабільний доступ до інформації та збільшує продуктивність.

Підвищення швидкості передачі даних є однією з найважливіших тенденцій у сфері телекомунікацій. З'явлення широкосмугових мереж, таких як 5G, пропонують неймовірні швидкості передачі даних, які відкривають нові можливості для послуг, які вимагають великого обсягу даних, наприклад, відеозв'язок високої якості, віртуальну реальність та розширену реальність. Швидкість передачі даних впливає на швидкість завантаження веб-сторінок, завантаження файлів та ігровий процес, що поліпшує взаємодію з мережею та забезпечує неперервну комунікацію.

Розширення спектру послуг є ще однією важливою характеристикою сучасного розвитку телекомунікаційної сфери. Поміж класичних послуг, таких як голосовий зв'язок та текстові повідомлення, з'явилися нові послуги, включаючи відеозв'язок, стрімінгове відео, хмарні обчислення, віртуальну телефонію та послуги мобільного банкінгу. Ці нові можливості розширюють спектр комунікаційних послуг та створюють нові можливості для бізнесу та особистого використання.

Зростання впливу Інтернету речей (IoT) є ще однією важливою тенденцією в сфері телекомунікацій. IoT включає підключення різних пристроїв та сенсорів до Інтернету, що дозволяє їм обмінюватися даними та взаємодіяти між собою. Це відкриває нові можливості у багатьох галузях, таких як смарт-доми, розумні міста, автомобільна промисловість, охорона здоров'я та сільське господарство. IoT дозволяє збирати та аналізувати великі обсяги даних, що сприяє усуненню проблем та покращенню ефективності в різних сферах.

Сучасний розвиток телекомунікаційної сфери має значний вплив на наш спосіб життя, комунікацію та взаємодію з оточуючим світом. Ми стаємо більш мобільними, постійно підключеними та залежними від швидкого доступу до інформації. Телекомунікації стають основою сучасного суспільства, де вони забезпечують ефективну комунікацію, покращують якість життя та стимулюють економічний розвиток. Ці зміни не тільки відкривають нові можливості, але й вимагають від нас адаптації та розуміння нових технологій, щоб ефективно використовувати їх у нашому повсякденному житті.

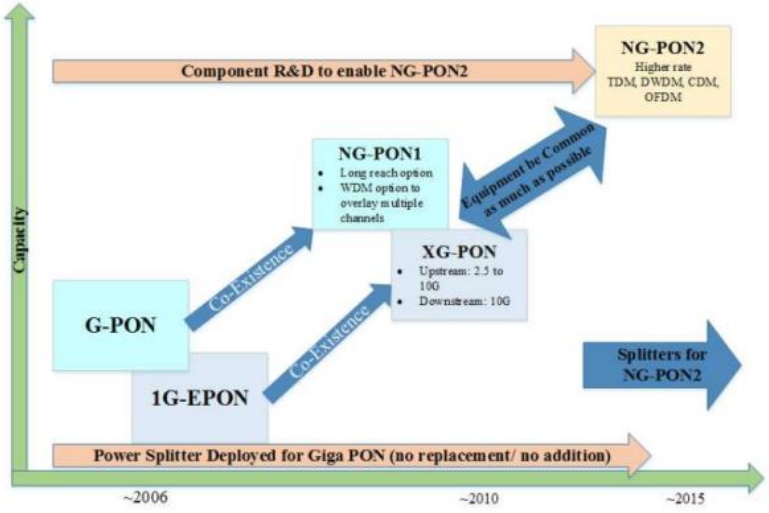
АНАЛІЗ ПРОЦЕСУ РОЗВИТКУ ПАСИВНИХ ОПТИЧНИХ МЕРЕЖ

Шуляк Дарія Геннадіївна
Державний університет телекомунікацій

Пасивна оптична мережа (PON) — це телекомунікаційна мережа, яка використовується для надання широкосмугового доступу кінцевим користувачам. Його конструкція реалізує топологію, в якій одне оптичне волокно використовується для з’єднання кількох кінцевих точок за допомогою оптичних розгалужувачів без живлення для розділення смуги пропускання волокна.

FSAN і ITU-T багато працюють над волокном до дому (FTTH) і розробили два несхожі стандарти пасивних оптичних мереж. Інший запроваджений ними стандарт — гігабітна пасивна оптична мережа (GPON). Мережа має швидкість передачі даних 2,488 Гбіт/с за потоком і 1,244 Гбіт/с вгору. Мережі GPON розгортаються по всьому світу. Через зростання попиту на Інтернет з боку кінцевих користувачів, GPON далі розширено до XG-PON, 10GPON і NG-PON для збільшення коефіцієнта розподілу та швидкості передачі даних. Усі ці стандарти запроваджено ITU-T.

Діаграма розвитку пасивних оптичних мереж наведена на малюнку 1. Цю діаграму надає FSAN. Відповідно до цієї діаграми пасивні оптичні мережі (PON) розвиваються до NG-PON 2 для мереж до 100 км. У цій мережі були застосовані різні методи модуляції для досягнення кращих результатів.



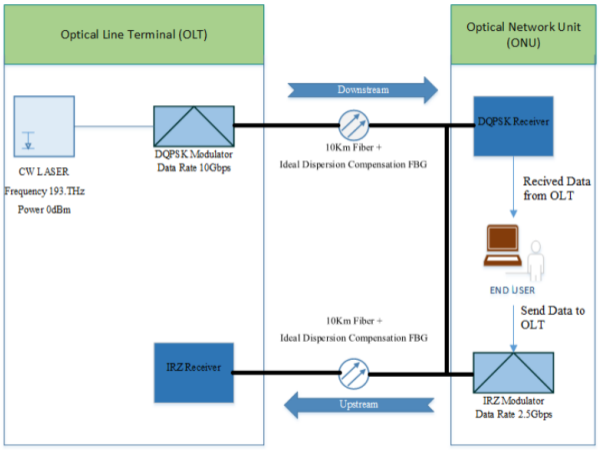
Малюнок 1: Еволюція пасивних оптичних мереж (PON) з часом.

Пасивні оптичні мережі (PON) були представлені як мережі FTTH, щоб покращити швидкість передачі даних у Гбіт/с для більшої кількості клієнтів із меншою платою за обслуговування. Він забезпечує зв'язок «точка-точка» між утилітою (оптичним лінійним терміналом) і кінцевим користувачем, що називається блоком оптичної мережі (ONU). PON перетворився на NG-PON2 з попитом на більш високі швидкості передачі даних.Нові інтернет-додатки та послуги підвищили попит на високу пропускну здатність. Мережа FTTH розвинулася та була стандартизована як G-PON для досягнення швидкості передачі даних у Гбіт/с для задоволення потреб у пропускній здатності. Відповідно до рекомендацій стандарту ITU-T, G-PON введено зі швидкістю 2,5 Гбіт/с для швидкості передачі сигналу вниз і 1,5 Гбіт/с для висхідного потоку. Це встановлено для технології TDMPON, коли кожен ONU отримує повну пропускну здатність для певного часового інтервалу, призначеного центральним офісом (CO). Щоб задовольнити вимоги щодо вищої швидкості передачі даних і збільшення кількості клієнтів, G-PON перетворено на XG-PON. XG-PON було визначено як процес, у якому сигнал даних 10 Гбіт/с передається від OLT до ONU, а сигнал даних 2,5 Гбіт/с надсилається назад від ONU до OLT відповідно до стандарту ITU-T Rec. G987.x. Для модуляції сигналу OLT і ONU можна використовувати різні методи модуляції, такі як диференціальна квадратурна фазова маніпуляція (DQPSK), NRZ, інвертований повернення до нуля (IRZ) і маніпуляція увімкнення-вимкнення (OOK). Ця технологія залежить від WDM. Це дозволяє окрему смугу від кожного OLT до відповідного ONU. NG-PON2 стандартизовано ITU-T. В результаті широкого використання інтернет-додатків і збільшення кількості користувачів Інтернету необхідно досягти швидкості передачі даних вище 40 Гбіт/с. Досягнуті швидкості передачі даних становлять 40 Гбіт/с для низхідних каналів і 10 Гбіт/с для висхідних каналів на основі мультиплексування за довжиною хвилі (WDM) і технологія пасивної оптичної мережі наступного покоління (NG-PON).

Пасивні оптичні мережі складаються з пасивних і активних компонентів. Він складається з трьох основних частин. Перший – це термінал оптичної лінії (OLT). Це початкова точка мережі. Другий – це оптичне волокно, яке використовується як середовище в мережі. Третій — оптичний мережевий блок (ONU), який діє як кінцевий користувач у пасивній оптичній мережі. Загальна блок-схема PON така наведено на малюнку 2.

Мережа починається з терміналу оптичної лінії (OLT). Він також відомий як утиліта або постачальник послуг. Він надає послуги кінцевим користувачам. Він складається з передавача, який передає дані, які запитує кінцевий користувач, і приймає запити або дані,

надіслані кінцевими користувачами. Оптоволокно використовується як середовище між утилітою та пристроєм користувача. Він підтримує високу швидкість передачі даних з невеликою кількістю помилок і високою ефективністю. Клієнтська сторона мережі



Малюнок 2: Блок-схема пасивної оптичної мережі (NG-PON2).

називається ONU. Він відомий як кінцевий користувач. Він складається з приймача інформації з Інтернету, а також має передавач, який використовується для передачі запитів користувача.

Список використаних джерел:

1. Ragheb, A. M., & Fathallah, H. (2011, December). Performance analysis of next generation PON (NG-PON) architectures. In 8th International Conference on High-Capacity Optical Networks and Emerging Technologies (pp. 339-345). IEEE

АНАЛІЗ ЗАСОБІВ БЕЗПЕКИ ОПЕРАЦІЙНИХ СИСТЕМ

Гордієнко Т.Б. завідуюча кафедрою, доктор технічних наук, професор,
Державний університет телекомунікацій, м. Київ
Кондратюк І.О. студент, група САДМ-51,
Державний університет телекомунікацій, м. Київ

Засоби безпеки операційних систем - це програмні інструменти та методи, які забезпечують захист комп'ютерної системи від загроз зовні та зсередини. Ці засоби можуть бути вбудованими в операційну систему або встановлюватися окремо. Деякі з таких засобів безпеки можуть бути налаштовані на автоматичну роботу та попереджати користувача про потенційні загрози, в той час як інші засоби можуть вимагати активного втручання користувача для їх використання.

Загальною метою засобів безпеки операційних систем є забезпечення безпеки даних та захисту від зловмисних дій, що можуть призвести до втрати даних, порушення приватності користувачів та інших негативних наслідків. Тому важливо мати належно налаштовані та оновлювані засоби безпеки операційних систем, щоб забезпечити захист комп'ютерної системи від потенційних загроз та зберегти цінні дані та ресурси.

Найпоширеніші засоби безпеки операційних систем включають:

- Фаєрволи - програми, які забезпечують захист від небажаних з'єднань та небезпечного трафіку;
- Антивіруси - програми, які забезпечують захист від вірусів, троянів та іншого шкідливого програмного забезпечення;
- Шифрування - метод, що захищає дані, зашифровуючи їх таким чином, що тільки авторизованим користувачам можна отримати доступ до них;
- Аутентифікація та авторизація - засоби, що забезпечують визначення та перевірку прав доступу користувачів до системи та різних її функцій;
- Оновлення системи та програмного забезпечення - регулярне оновлення дозволяє закрити вразливості в операційній системі та зменшити ризики злому або атак.

Засоби безпеки операційних систем важливі для забезпечення надійної та безпечної роботи комп'ютера. Використання цих засобів може зменшити ризики порушення конфіденційності, цілісності та доступності даних, а також захистити від атак зовні та зсередини.

Розглянемо детальніше засоби безпеки найпопулярніших операційних систем:

Windows:

- Перевірка цифрових підписів драйверів та програм. Це забезпечує безпеку від потенційно шкідливих програм та драйверів, які можуть пошкодити систему.
- UAC (User Account Control) - система контролю облікових записів користувачів. Вона запитує дозвіл на виконання важливих дій в системі та запобігає незаконним діям.

- Windows Defender - вбудована система антивірусного захисту, яка сканує систему на наявність вірусів та шкідливого програмного забезпечення.
- BitLocker - інструмент шифрування диска, який забезпечує захист від втрати конфіденційної інформації, якщо пристрій потрапляє в руки зловмисника.
- Windows Firewall - забезпечує захист від небажаного доступу до мережі та заблоковує небезпечний трафік.

Недоліки: Windows має деякі відомі вразливості, які можуть бути використані зловмисниками для атак. Також, у Windows можуть бути проблеми з доступом до ресурсів, оскільки система має широкі права доступу до файлів та реєстру. Крім того, автоматичні оновлення можуть бути надмірно агресивними, що може призводити до проблем зі сумісністю або втратою даних.

macOS:

- Gatekeeper - система безпеки, яка запобігає встановленню та виконанню небезпечного програмного забезпечення.
- XProtect - інструмент антивірусного захисту, який сканує систему на наявність вірусів та шкідливого програмного забезпечення.
- FileVault - інструмент шифрування диска, який забезпечує захист від втрати конфіденційної інформації.
- Firewall - забезпечує захист від небажаного доступу до мережі та заблоковує небезпечний трафік.
- iCloud Keychain - інструмент, який зберігає дані ваших облікових записів та паролів в зашифрованому вигляді.

Недоліки: Одним з недоліків macOS є те, що за замовчуванням деякі засоби безпеки, такі як файрвол та антивірус, вимкнені. Також, macOS має відомі вразливості, наприклад, шкідливе програмне забезпечення, яке може відкривати доступ зловмисникам до важливих даних. Крім того, в macOS є певні проблеми з безпекою на рівні ядра.

Linux:

- AppArmor або SELinux - це розширення ядра Linux, які надають додаткові механізми контролю доступу до ресурсів системи, таких як файли, мережеві протоколи, процеси тощо.
- Файрвол - захист від небажаного доступу до мережі.
- Пакетні менеджери - забезпечують безпеку шляхом перевірки цифрових підписів та автоматичної валідації пакетів перед їх встановленням.
- Антивірусне програмне забезпечення - багато Linux-дистрибутивів мають свої вбудовані антивірусні програми або можуть встановлювати стороннє програмне забезпечення для захисту від вірусів та шкідливого ПЗ.
- Доступ до прав користувача - деякі дистрибутиви Linux мають систему безпеки, що забезпечує контроль прав доступу користувачів та забезпечує ізоляцію даних.

Недоліки: Незважаючи на те, що Linux вважається однією з найбільш безпечних операційних систем, вона також має свої недоліки. Наприклад, у Linux можуть виникати проблеми з безпекою на рівні ядра, які можуть використовуватися для отримання неповного доступу до системи. Крім того, деякі дистрибутиви Linux можуть мати погану документацію або недостатній рівень підтримки користувачів. [1]

Нижче розглянемо загальну структуру взаємодії операційної системи з користувачем. Це дасть нам можливість зрозуміти загальний взаємозв’язок.

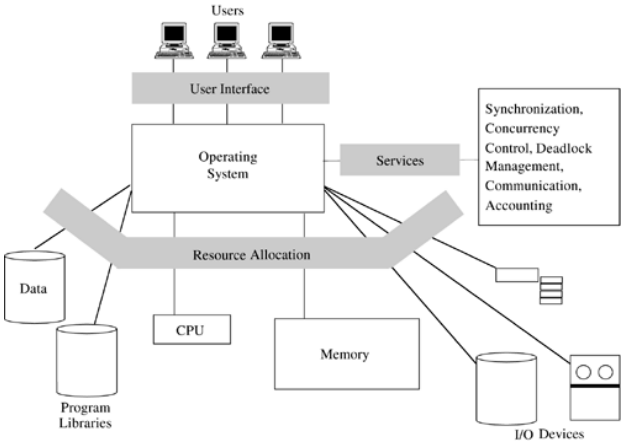


Рисунок 1 – взаємодія операційної системи з користувачем.

Малюнок 1 ілюструє, як операційна система взаємодіє з користувачами, надає послуги та розподіляє ресурси. Ми бачимо, що система виконує кілька конкретних функцій, пов’язаних із безпекою комп’ютера:

Аутентифікація користувача (User authentication). Операційна система повинна ідентифікувати кожного користувача, який запитує доступ, і повинна переконатися, що користувач насправді є тим, за кого себе видає. Найпоширенішим механізмом автентифікації є порівняння паролів.

Захист пам'яті (Memory protection). Програма кожного користувача повинна виконуватися в частині пам'яті, захищеній від несанкціонованого доступу. Захист, безумовно, запобігатиме доступу сторонніх осіб, а також може контролювати власний доступ користувача до обмежених частин програмного простору.

Контроль доступу до файлів і пристроїв введення/виведення (File and I/O device access control). Операційна система повинна захищати файли користувача та системи від доступу неавторизованих користувачів. Так само має бути захищено використання пристроїв введення/виведення. Захист даних зазвичай досягається пошуком у таблиці, як у випадку з матрицею контролю доступу.

Міжпроцесний зв'язок і синхронізація (Interprocess communication and synchronization). Виконуваним процесам іноді потрібно спілкуватися з іншими процесами або синхронізувати їх доступ до спільних ресурсів. Операційні системи надають ці послуги, діючи як міст між процесами, відповідаючи на запити процесу для асинхронного зв’язку з іншими процесами. Міжпроцесовий зв'язок здійснюється за допомогою таблиць керування доступом.

Захищені дані операційної системи (Protected operating system protection data). Операційна система повинна підтримувати дані, за допомогою яких вона може забезпечити захист. Очевидно, що якщо ці дані не захищені від несанкціонованого доступу, то операційна система не може забезпечити виконання. Різноманітні методи, включаючи шифрування, контроль апаратного забезпечення та ізоляцію, підтримують ізоляцію даних захисту операційної системи. [2]

Тепер проаналізуємо роботи відомих авторів по засобам безпеки операційних систем. "A Comparative Analysis of Security Features in Linux and Windows Operating Systems" авторства М. Кумара, де порівнюються засоби безпеки в операційній системі Linux та Windows. У дослідженні розглядаються такі аспекти, як біометрична аутентифікація, шифрування файлів, мережева безпека та безпека віртуальних машин.

Одним з недоліків цього дослідження може бути те, що воно не зводиться до однієї конкретної проблеми безпеки, а складається з різних аспектів. Також, при порівнянні засобів безпеки різних операційних систем, необхідно враховувати різниці функціональності та призначенні операційних систем, що можуть вплинути на ефективність та безпеку їх засобів безпеки.

"Windows 10 Security Features: A Comparative Analysis with Windows 8.1 and Windows 7" авторства В. Джеймса, В. Балакришнана та С. Багаватхі. У цьому дослідженні досліджувалась ефективність та безпека різних засобів безпеки в операційній системі Windows 10 порівняно з Windows 8.1 та Windows 7.

Одним з недоліків цього дослідження є те, що воно орієнтоване тільки на операційні системи Windows, тоді як інші операційні системи (наприклад, macOS, Linux) можуть мати інші особливості та засоби безпеки, які також варто розглянути. Також, враховуючи швидкий темп змін у технологіях та безпеці, результати дослідження можуть втратити актуальність з часом.

Висновки:

Загалом, всі три операційні системи мають схожі засоби безпеки, такі як фаєрвол та шифрування диску. Однак, кожна з них має свої унікальні засоби безпеки, які забезпечують надійний захист від різних видів загроз. Для кожної конкретної ситуації необхідно використовувати підходящі засоби безпеки, щоб забезпечити найвищий рівень захисту.

Windows має високий рівень використання, тому його часто атакують. Проте, він має вбудовані засоби безпеки, які допомагають убезпечити систему, такі як антивірус та файрвол.

macOS має малу кількість вірусів та шкідливих програм, але його засоби безпеки залежать від того, які програми встановлені на комп'ютері. Якщо користувач не оновлює програми регулярно, то система може бути під загрозою.

Linux має високий рівень безпеки завдяки вбудованому захисту, а також відкритому вихідному коду, який дозволяє досконало перевірити безпеку системи. Але, так як він менш популярний, зловмисники рідше спрямовують свої атаки на нього.

Отже, вибір операційної системи залежить від потреб користувача та відповідних засобів безпеки, які можуть забезпечити надійний захист від різних видів загроз.

Список посилань

1. Jaeger T. Operating System Security / Trent Jaeger., 2008. – 192 с. – (Morgan & Claypool Publishers).
2. Tanenbaum A. Structured Computer Organization / Andrew Tanenbaum., 2012. – 808 с. – (6th edition).

РОЗРОБКА АРХІТЕКТУРИ СИСТЕМИ НА ОСНОВІ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Добровольський Роман Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

У теперішньому цифровому світі безпека даних у телекомунікаційних системах є критично важливою. Зростання обсягу та розповсюдження цифрової інформації ставить під загрозу конфіденційність, цілісність та доступність даних. У цьому контексті блокчейн-технології виявляються потужним інструментом для забезпечення безпеки даних, оскільки вони пропонують розподілену та незмінну платформу, яка дає змогу ефективно відстежувати та захищати дані в телекомунікаційних системах.

Блокчейн-технології базуються на розподіленій базі даних, в якій кожен блок містить хеш попереднього блоку, утворюючи послідовний ланцюжок блоків. Ця структура дозволяє забезпечити безпеку даних, оскільки будь-яка спроба внесення змін в один блок вимагатиме внесення змін у всі наступні блоки, що вимагатиме великої обчислювальної потужності та узгодженості більшості учасників мережі.

Однією з переваг використання блокчейн-технологій у телекомунікаційних системах є можливість відстежувати та аудитувати безпекові події. Блокчейн забезпечує історичну

перспективу транзакцій та змін, що дозволяє легко виявляти та аналізувати можливі порушення безпеки. Наприклад, в сфері телекомунікацій можна стежити за несанкціонованим доступом до мережевих вузлів або намаганнями підробки даних.

Крім того, блокчейн-технології дозволяють забезпечити конфіденційність даних шляхом застосування криптографічних методів. Учасники мережі можуть використовувати криптографічні ключі для захисту даних від несанкціонованого доступу. Такий підхід може бути особливо корисним у випадках передачі чутливої інформації, наприклад, особистих даних абонентів телекомунікаційних послуг.

Додатковою перевагою використання блокчейн-технологій є можливість створення незмінної та недоступної для змін бази даних. Це може бути особливо важливо в контексті телекомунікаційних систем, де важлива цілісність та достовірність інформації. Наприклад, блокчейн може використовуватись для реєстрації та верифікації мобільних телефонів, що забезпечить достовірність даних про власників та запобіжить використанню вкрадених або підроблених пристроїв.

Крім того, блокчейн-технології можуть бути застосовані для реалізації механізмів мікроплатежів та управління даними про використання послуг. Наприклад, в мобільних мережах блокчейн може використовуватись для автоматизованого та безпечного збору та передачі платежів за роумінг та додаткові послуги, що спрощує процес оплати та зменшує ризик шахрайства.

Приклади використання блокчейн-технологій для забезпечення безпеки даних у телекомунікаційних системах вже поширені. Наприклад, компанія Telefónica випустила проект "TrustOS", який базується на блокчейні та забезпечує безпеку та конфіденційність трафіку в їхніх мережах. Крім того, використання блокчейну в телекомунікаційних системах може сприяти уніфікації та стандартизації процесів обміну даними між різними операторами, що полегшить взаємодію та забезпечить безпеку комунікацій.

Список використаних джерел:

1. Swan, M. (2015). Blockchain: Blueprint for a New Economy.
2. Decker, C., & Wattenhofer, R. (2013). Information Propagation in the Bitcoin Network.
3. Yli-Huumo, J., et al. (2016). Where is Current Research on Blockchain Technology? A Systematic Review.
4. Telefónica. "TrustOS: Blockchain-Based Secure Communication." Retrieved from https://www.telefonica.com/en/web/press-office/-/telefonica-launches-trustos-a-blockchain-based-system-for-secure-communication

ОСОБЛИВОСТІ ТА СУТНІСТЬ ОПТИЧНОГО БЕЗДРОТОВОГО ЗВ’ЯЗКУ

Шуляк Дарія Геннадіївна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Концепція оптичного бездротового зв’язку проста і подібна до оптоволоконного зв'язку з тією різницею, що середовищем передачі є вільний простір. Напрямок оптичного променя та його спрямованість можна визначити відносно застосування, і це можна визначити такими простими оптичними компонентами, як лінзи або призми. Оптичні канали вільного простору суворо обмежені стандартами безпеки очей (і безпеки шкіри), що визначають максимально допустиму потужність випромінювання, яка не має шкідливого впливу на користувачів. Оптичний бездротовий зв'язок є міждисциплінарною областю дослідження. Тип оптичної

передачі у вільному просторі визначається як функція розбіжності променя, класифікуючи канал за трьома різними топологіями.

Зв'язок прямої видимості (LOS) або точка-точка - це зв'язок із квазівирівнюванням між передавачем і приймачем. Промінь з низькою розбіжністю (FOV), детектори з вузьким полем огляду дозволяють відкидати високий відсоток шуму від навколишнього освітлення. Цей тип зв'язку з вузьким розходженням не передбачає велике покриття. Однак досягається менше загасання порівняно з іншими топологіями з більшою розбіжністю, і відстань зв'язку може бути довшою. Тоді як повне узгодження з оптичним сигналом неможливе, але також для того, щоб запропонувати деяку гнучкість каналу, ця геометрія вільного простору включає топології дуже малої розбіжності (< 3◦), що називається вузьким LOS (NLOS).Ця топологія вимагає прямого огляду між передавачем і приймачем, що зменшує гнучкість зв'язку та робить його дуже чутливим до будь-яких перешкод. У цій конфігурації сигнал не страждає від багатопроменевого спотворення, отже, немає міжсимвольної інтерференції (ISI), яка робить швидкість зв'язку залежною лише від бюджету потужності. У каналі LOS швидкість передачі даних може бути збільшена за допомогою методів просторового мультиплексування. Ступінь мобільності також можна збільшити шляхом збільшення кількості LOS-зв'язків або за допомогою систем відстеження, які досягають 155 Мбіт/с на відстані майже 2 м у приміщенні. Незважаючи на те, що більшість каналів LOS використовують один передавач і приймач, вищого посилення можна досягти, використовуючи кілька передавачів і приймачів. Реалізація системи з декількома входами та декількома виходами (MIMO) вимагає використання лазерних і фотодіодних матриць або просторового модулятора світла як передавача та пристрою зображення як приймача. Посилання MIMO LOS використовується в багатьох додатках, таких як двовимірні штрих-коди, сторінково-орієнтований запис, голографічне зберігання і канал оптичного зв'язку MIMO.

Широка лінія прямої видимості (WLOS) характеризується передавачем з більшим кутом розбіжності порівняно з LOS. Приймач, який використовується, також має більший кут зору. Геометрія зв'язку не вимагає вирівнювання між передавачем і приймачем, на відміну від прямого огляду між ними, що важливо. WLOS характеризується вищим загасанням порівняно з LOS або NLOS, що зменшує відстань зв'язку. Передавач широкого променя в цій топології може спричинити багатопроменевість через відбиття від стіни та об'єктів у кімнаті, таким чином створюючи ISI та впливаючи на швидкість передачі даних і якість сигналу. Ця топологія адаптована для додатків «точка-багатоточка» (PmP), де система містить точку доступу з передавачем і кількома мобільними приймачами в закритій зоні .

Розсіяний внутрішній оптичний канал, у цій конфігурації оптичний передавач розсіює оптичний сигнал у всіх можливих напрямках. Сигнал на приймачі - це оптична потужність, зібрана фотодіодом, що надходить від передавача безпосередньо або після багатьох відображень. Даний тип зв'язку не потребує прямого огляду між передавачем і приймачем. Цей тип з'єднання зазвичай вивчається для внутрішнього середовища. Для виявлення відбитків розсіяного сигналу всередині кімнати та встановлення зв'язку використовується передавач із широким променем і приймач із великим полем зору. Прийнятий сигнал страждає від багатопроменевої дисперсії, викликаної великою кількістю відбитих променів на вході приймача. Як наслідок, високий ISI, який зменшує максимальну швидкість передачі даних.

Першу дифузну інфрачервону систему запропонували Гфеллер і Бапст, забезпечуючи 1Мбіт/с на довжині хвилі 950 нм. Найшвидшою повністю дифузною системою є повідомлена Марш і Кан, пропонуючи бітрейт 50 Мбіт/с, використовує 805 нм оптичний носій довжини хвилі.

Список використаних джерел:

1. M. Uysal and H. Nouri, "Optical Wireless Communications – An Emerging Technology", 16th International Conference on Transparent Optical Networks (ICTON), Graz, Austria, July 2014

2. H. Hemmati, Deep Space Optical Communications, Wiley-Interscience, 2006

ОГЛЯД ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ 50G-PON

Мацелюк Максим Євгенович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Анотація:

Технологія пасивної оптичної мережі (PON) швидко розвивається, надаючи все більше швидкості та пропускної здатності для передачі даних. Однією з передових технологій PON є 50G-PON, яка пропонує значне покращення продуктивності порівняно зі стандартною 10G-PON.

Підвищення вимог до швидкості передачі даних та зростання обсягу мультимедійного контенту ставлять перед оптичними мережами нові виклики. 50G-PON є одним із варіантів, який пропонує забезпечити значне збільшення швидкості передачі даних в PON. Ця технологія використовує методи мультиплексування та модуляції для досягнення швидкості до 50 Гбіт/с.

Огляд технології 50G-PON:

Технологія 50G-PON застосовує одну хвилю (single-wavelength) як для низхідного (1340-1344 нм) так і для висхідного (1260-1280, 1290-1310 нм в залежності від обраного стандарту в існуючій мережі PON) потоку даних. Слід зауважити, що використовуються відмінні від GPON та XG(S)-PON довжини хвиль, що забезпечує співіснування декількох технологій у наявній мережі PON та дозволяє запроваджувати нові послуги для користувачів [1].

Обладнання 50G-PON розташовується у центральному офісі мережі доступу. Воно забезпечує висхідний зв'язок з сервісною мережею і низхідний зв'язок з користувачами через різні користувацькі інтерфейси ONU. 50G-PON підтримує топологію "точка-багатоточка", а також послуги передачі відео, даних і голосу. Як GPON і 10G PON, 50G-PON використовує мультиплексування з поділом по довжині хвилі для реалізації двонаправленої передачі даних по одному волокну і використовує TDM для низхідного трафіку і TDMA для висхідного трафіку для реалізації зв'язку "точка-багатоточка" між OLT і ONU [3].

Функціональні можливості та параметри технології 50G-PON описуються стандартами ITU-T G.9804 та IEEE 802.3ca [2].

Передача даних може бути як симетричною зі швидкістю 50/50 Гбіт/сек, так і асиметричною зі швидкістю 50/25, 50/12.5, 50/10 Гбіт/сек.

ITU-T використовує NRZ-код для 50G-PON оскільки у такому випадку забезпечується найкраща продуктивність. Для реалізації FEC (Forward Error Correction) використовується LDPC (Low-Density Party Check) (17280, 14592). Ефективність становить близько 85% [1, 3].

Для низхідного та висхідного потоку даних застосовується шифрування AES128, а для критично важливих об’єктів є можливість впровадження AES256 та інших криптографічних протоколів схвалених Міжнародною організацією зі стандартизації ICO [2]. Для досягнення найменших затримок використовуються технології DAW (Dedicated Activation Wavelengths) та CoDBA (Coordinated Dynamic Bandwith Allocation) [1, 3].

Переваги технології 50G-PON:

Технологія 50G-PON має декілька значних переваг, які роблять її привабливою для впровадження в оптичних мережах. Ось деякі з них:

1. Висока швидкість передачі даних: технологія 50G-PON забезпечує швидкість передачі даних до 50 Гбіт/с, що є значним покращенням порівняно зі стандартними 10G-PON. Це дозволяє передавати великі обсяги даних швидше і ефективніше.

2. Покращена пропускна здатність: завдяки використанню нових методів мультиплексування та модуляції, 50G-PON забезпечує більшу пропускну здатність порівняно з попередніми стандартами PON. Це дозволяє підтримувати високу швидкість передачі даних навіть при зростаючому навантаженні мережі.

3. Більша кількість користувачів на одній лінії: завдяки покращеній ефективності спектру, технологія 50G-PON дозволяє підключати більше користувачів на одному оптичному волокні. Це зменшує вартість і складність розгортання мережі та робить її більш економічно ефективною.

4. Підтримка різних послуг: 50G-PON може задовольняти високі вимоги до пропускної здатності для різних послуг і додатків. Вона підходить для високоякісного відео стрімінгу, віртуальної реальності, хмарних служб, мультимедійних додатків та Інтернету речей (IoT). Це відкриває нові можливості для розвитку телекомунікаційних послуг.

5. Зворотна сумісність: технологія 50G-PON є зворотно сумісною з попередніми стандартами PON. Це означає, що існуючі мережеві інфраструктури можуть бути оновлені до 50G-PON без потреби в повній заміні обладнання. Це значно спрощує процес переходу до нової технології і зменшує витрати операторів зв'язку.

6. Майбутні можливості розширення: технологія 50G-PON має потенціал для подальшого розширення і покращення. Наприклад, можливе збільшення швидкості передачі даних до 100 Гбіт/с і більше у майбутньому. Це робить 50G-PON масштабованою та готовою до викликів швидкозростаючих мереж та послуг.

Високі швидкості передачі даних, покращена пропускна здатність, більша кількість користувачів на одному волокні, підтримка різних послуг, зворотна сумісність та майбутні можливості розширення роблять технологію 50G-PON перспективною та ефективною в сучасних телекомунікаційних мережах. Її впровадження може сприяти задоволенню зростаючих вимог користувачів і забезпечити стійку та швидку передачу даних у майбутньому.

Перспективи впровадження технології 50G-PON:

На Китай припадає понад 70% розгорнутих у світі GPON ONU. Прокладання оптоволоконних кабелів є найдорожчою частиною розгортання FTTx. Після того, як волокно доступне, оновлення до більш високих швидкостей не є таким дорогим. Китай, безумовно, отримав вигоду від урядової політики, згідно з якою всі нові багатоквартирні будинки оснащуються оптоволокном. На початку 2022 року країна повідомила про 550 мільйонів абонентів FTTH і лідирує у світі за впровадженням 10G PON. Отже, є всі підстави очікувати, що Китай буде першим і найбільшим у розгортанні PON наступного покоління.

Три великі китайські оператори дали зрозуміти, що вони переходять на 50G-PON після 10G-PON.

Представник China Telecom Zhang Dezhi заявив у 2021 році, що "50G PON - це майбутнє PON з трьох причин: 50G-PON може уніфікувати наступні покоління технологій PON, може співіснувати з 10GEPON або XG(S)-PON і збільшує пропускну здатність у п'ять разів порівняно з 10G PON, що в більшій мірі задовольняє нові вимоги, такі як 4K/8K, VR/AR, IoT та хмарні сервіси." [4]

У європейських країнах оператори вже деякий час тестують прототипи наступного покоління PON, і багато з них також віддають перевагу 50G-PON як наступнику 10G-PON [4]:

1. Керівник мереж фіксованого доступу Orange Jesús Vallejo заявив у березні 2022 року, що 50G-PON став одноголосним вибором наступного покоління PON. За його словами, Orange віддає перевагу 50G-PON, оскільки він дозволяє повторно використовувати існуючі мережеві ресурси, одночасно розвиваючись в напрямку 50G-PON.

2. Swisscom протестував 50G-PON в жовтні 2020 року, модернізувавши існуючий OLT до 50G-PON і досягнувши швидкості 50 Гбіт/с у низхідному потоці і 25 Гбіт/с у висхідному потоці в фіксованій мережі. Представник компанії заявив, що спочатку впроваджена технологія буде обслуговувати малий бізнес і мобільний трафік 5G.

3. Директор з інформаційних технологій Telefonica Enrique Blanco заявив у вересні 2021 року, що 50G-PON - це вибір його компанії для фіксованого доступу за межами поточного використання 10G XG(S)-PON.

4. Turkcell заявив, що планує розгорнути 50G-PON у 2024 році.

5. Vodafone випробував 100G-PON у 2021 році і, схоже, перейде від 10G-PON безпосередньо до 100G через деякий час у майбутньому. Технологічний менеджер Vodafone заявив у 2020 році, що "10G-PON, ймовірно, буде достатньо до 2030 року".

Висновки:

У статті було проведено огляд основних компонентів та принципів роботи технології 50G-PON, аналізовано її переваги, включаючи високу швидкість передачі даних та покращену ефективність спектру. Також було обговорено перспективи впровадження 50G-PON у майбутніх оптичних мережах, враховуючи потенційні сценарії застосування та важливі аспекти, що потребують уваги.

Заключаючи, технологія 50G-PON представляє собою важливий крок у розвитку оптичних мереж, забезпечуючи велику швидкість передачі даних та пропускну здатність. Впровадження 50G-PON має потенціал для задоволення зростаючих вимог користувачів і сприяння розвитку майбутніх телекомунікаційних мереж.

Список використаних джерел

1. 50G-PON – technology overview [Електронний ресурс] – Режим доступу до ресурсу: https://forum.huawei.com/enterprise/en/50g-pon-technology-overview/thread/893475-100181

2. 50G-PON: The First ITU-T Higher-Speed PON System [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/359490845_50G-PON_The_First_ITU-T_Higher-Speed_PON

3. White paper on 50G-PON technology [Електронний ресурс] – Режим доступу до ресурсу: https://res-www.zte.com.cn/mediares/zte/Files/PDF/white_book/White_Paper_on_50G-PON_Technology_20201210_EN.pdf

4. Why 50G PON Looks Like a Clear Winner vs 25G [Електронний ресурс] – Режим доступу до ресурсу: https://blog.huawei.com/2022/07/08/50g-pon-clear-winner-25g/

СТАТИЧНА ТА ДИНАМІЧНА МАРШРУТИЗАЦІЯ: ПОРІВНЯЛЬНИЙ АНАЛІЗ

Бєлобородов Вадим Дмитрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Статична і динамічна маршрутизація є двома підходами до керування мережевим трафіком і направлення пакетів даних від одного вузла до іншого в комп'ютерних мережах. Проаналізуємо їх за декількома основними критеріями:

Гнучкість: Статична маршрутизація проста і не змінюється відповідно до стану мережі, тоді як динамічна маршрутизація може адаптуватися до змін і незавпаціній зміни маршрутів.

Надійність: Динамічна маршрутизація може забезпечити вищу надійність, оскільки вона може швидко виявляти та уникати проблеми з маршрутизаторами або мережевими з'єднаннями.

Обслуговування: Статична маршрутизація має нижчу накладну витрату на обробку, оскільки маршрути вже встановлені. Динамічна маршрутизація потребує обчислень та обміну повідомленнями для визначення та оновлення маршрутів.

Масштабованість: Динамічна маршрутизація зазвичай більш масштабована, оскільки може адаптуватися до змін у складності та розмірі мережі. Статична маршрутизація практична в менших мережах, але може стати складною для керування великими мережами з багатьма маршрутизаторами.

Вибір між статичною та динамічною маршрутизацією залежить від розміру та складності мережі, потреб у надійності та гнучкості, а також ресурсів, доступних для керування маршрутизацією. Часто великі мережі використовують комбінацію обох підходів для оптимального керування мережевим трафіком.

Статична маршрутизація:

В статичній маршрутизації маршрути задаються вручну адміністратором мережі. Маршрути залишаються постійними і не змінюються автоматично відповідно до зміни умов мережі. Інформація про маршрути зберігається в маршрутизаційній таблиці на кожному маршрутизаторі. Низька накладна витрата на обробку, оскільки маршрути вже встановлені. Використовується в невеликих мережах з незмінними топологіями. Приклад с озсновних протоколів статичної маршрутизації що наразі активно використовуються:

Static Route Protocol (статичний маршрутний протокол) - це базовий протокол статичної маршрутизації, який дозволяє адміністратору вручну налаштувати статичні маршрути. Адміністратор вручну вказує IP-адреси мережних сегментів та відповідні маршрути до них.

Routing Information Protocol (RIP). Хоча RIP є протоколом динамічної маршрутизації, він також може бути використаний для статичної маршрутизації. За допомогою RIP можна налаштувати статичні маршрути, вказавши їх метрики як "безкінечні" (infinity), що призводить до виключення цих маршрутів з таблиці маршрутизації RIP.

Open Shortest Path First (OSPF) - OSPF є протоколом динамічної маршрутизації, але також може бути використаний для налаштування статичних маршрутів. Адміністратор може вручну налаштувати маршрути OSPF, використовуючи команди OSPF в мережному пристрої.

Border Gateway Protocol (BGP) - BGP є зовнішнім протоколом маршрутизації, який використовується для обміну маршрутами між автономними системами (AS). Хоча BGP переважно використовується для динамічної маршрутизації, він також може бути використаний для встановлення статичних маршрутів між автономними системами.

Динамічна маршрутизація:

В динамічній маршрутизації маршрути обчислюються автоматично з використанням протоколів маршрутизації, які обмінюються інформацією про стан мережі з іншими маршрутизаторами. Маршрути можуть динамічно змінюватись в залежності від стану мережі, наприклад, в разі відмови маршрутизатора або зміни шляху з найкращими метриками. Вона потребує розрахунку маршрутів і обміну інформацією між маршрутизаторами, що може займати певний обсяг пропускної здатності та обробки. Застосовується в більших мережах з динамічною топологією, де вимагається автоматичне адаптування до змін. Які протоколи динамічної маршрутизації активно використовуються у наш час:

Routing Information Protocol (RIP). RIP є одним з найпоширеніших протоколів маршрутизації. Він використовує алгоритм з обмеженнями на кількість переходів (hop count) для визначення оптимальних маршрутів. RIP використовує періодичні оновлення та запити для обміну інформацією про маршрути з іншими маршрутизаторами у мережі.

Open Shortest Path First (OSPF). OSPF є протоколом маршрутизації на основі стану каналу (link-state), що означає, що він заснований на інформації про стан каналу у всій мережі. OSPF використовує алгоритми Дейкстри для визначення найкоротших шляхів та обміну LSDB (Link State Database) між маршрутизаторами. Він дозволяє більш точне визначення оптимальних маршрутів та підтримує багатофункціональні мережі.

Enhanced Interior Gateway Routing Protocol (EIGRP). EIGRP є протоколом пропріетарного розробника Cisco Systems і поєднує в собі переваги протоколів векторних відстаней та протоколів стану каналу. Він використовує алгоритми Дейкстри та заснований на векторах відстаней для визначення найкоротших шляхів. EIGRP має високу швидкодію та ефективно використовує пропускну здатність мережі.

Border Gateway Protocol (BGP). BGP є протоколом маршрутизації на рівні системи автономних систем (AS). Він використовується для обміну маршрутною інформацією між різними провайдерами Інтернету та великими мережами. BGP забезпечує визначення найкоротших шляхів на основі різних метрик, таких як шляхи до призначення, пропускна здатність та політики маршрутизації.

Література:

1. Комп'ютерні мережі. 6-те вид. Таненбаум Е. С., Фімстер Н., Уезеролл Д.

РОЗВИТОК ТЕЛЕКОМУНІКАЦІЙНОЇ ГАЛУЗІ В УМОВАХ ВІЙНИ

Зінченко Олександр Михайлович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Розвиток телекомунікаційної галузі в умовах війни в Україні є необхідною умовою забезпечення стійкості та гнучкості держави перед агресією Росії, яка використовує інформаційну сферу як один із інструментів гібридної війни. Для цього Україна має реалізувати цифрову трансформацію економіки та суспільства, забезпечити модернізацію та розвиток цифрової інфраструктури, посилити кіберзахист, а також інтегруватися у єдиний цифровий ринок з ЄС. Це дозволить покращити якість надання державних послуг, зміцнити національну ідентичність та сприяти подальшому розвитку демократичних інститутів.

Цифрова трансформація економіки та суспільства в умовах війни передбачає впровадження нових цифрових технологій, які забезпечують ефективність, прозорість та інноваційність різних сфер діяльності. Зокрема, це стосується таких напрямків, як е-урядування, е-освіта, е-медицина, е-соціальне забезпечення, е-транспорт, е-торгівля тощо. Завдяки цифровим послугам громадяни можуть отримувати необхідну інформацію та документи в онлайн-режимі, без необхідності відвідувати державні установи або стикатися з корупцією. Це також сприяє покращенню доступності та якості освіти, медичної допомоги, соціальної підтримки та інших сфер життєдіяльності населення.

Модернізація та розвиток цифрової інфраструктури в умовах війни полягає у забезпеченні надійного та безперебійного функціонування мереж зв’язку та інтернету на всій території України, включаючи зони проведення антитерористичної операції та оборони від агресора. Для цього необхідно використовувати новітні технології, такі як 5G, супутниковий зв’язок, оптоволоконні лінії тощо. Також важливо відновлювати та будувати нову цифрову інфраструктуру на звільнених територіях, щоб забезпечити їхню інтеграцію у єдиний інформаційний простір України. Для цього Україна може розраховувати на фінансову підтримку з боку ЄС, який виділяє кошти на розбудову цифрової інфраструктури в рамках програми CEF та інших інструментів.

Посилення кіберзахисту в умовах війни є необхідною умовою для захисту критичної інфраструктури, державних органів, бізнесу та громадян від кібератак агресора. Для цього потрібно розвивати національну систему кібербезпеки, яка забезпечує координацію дій між різними стейкхолдерами, моніторинг та прогнозування кіберзагроз, реагування на кіберінциденти, попередження та ліквідацію їх наслідків. Також важливо підвищувати рівень кіберграмотності та кібергігієни населення, щоб зменшити ризик стати жертвою кіберманіпуляцій, шахрайства, шпигунства тощо.

Інтеграція у єдиний цифровий ринок з ЄС в умовах війни є стратегічним напрямком для України, який сприятиме її економічному розвитку, конкурентоспроможності та поглибленню європейської інтеграції. Для цього Україна має гармонізувати своє законодавство з нормами та стандартами ЄС у сфері цифрових послуг, захисту персональних даних, інтелектуальної власності, електронної комерції тощо. Також Україна має брати участь у конкурсах Програми ЄС «Цифрова Європа», яка фінансує проєкти з розвитку суперкомп'ютерів, штучного інтелекту, кібербезпеки, цифрових навичок та інших цифрових технологій.

ВПЛИВ ОПТИЧНОГО РІВНЯ СИГНАЛУ НА ПРОПУСКНУ ЗДАТНІСТЬ В МЕРЕЖІ PON

Мацелюк Максим Євгенович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

ONU (Optical Network Unit) – це активне обладнання, яке використовується в мережах PON на стороні абонента. Низький рівень оптичного сигналу відноситься до явища, коли оптична потужність, отримана ONU, менша, ніж чутливість прийому ONU. Показник чутливості прийому для забезпечення нормального режиму роботи зазвичай становить -27.0 дБм, однак з 2018 року це значення у відповідному стандарті було підвищено до -28.0 дБм.

Явище низького рівня оптичного сигналу є поширеним, причинами цього можуть бути: погонні згасання з урахуванням довжини кабелю, пошкодження при здійсненні монтажу кабелю, втрати на зварних та механічних з'єднаннях, мікро- макропошкодження оптоволокна, втрати на дільниках сигналу, клас оптичної потужності OLT SFP модулю.

Існує багато факторів, які впливають на роботу користувача в інтернеті, проте низький рівень оптичного сигналу в основному впливає на швидкість інтернету. Для того, щоб перевірити вплив рівня сигналу на швидкість інтернету, була побудована наступна тестова модель [1]:

Рисунок 1 Тестова модель

Регулюючи атенюатор, можна збільшити оптичні втрати розподільчої мережі, що призведе до зміни оптичної потужності, яку отримує ONU. Зміни в швидкості передачі даних перевіряються шляхом підключення ONU до ноутбуку за допомогою ethernet кабелю. Цей

метод був використаний для тестування широкосмугового зв'язку з каналом 300 Мбіт/сек, а результати тесту наведені в таблиці 1.

Таблиця 1

Рівень вхідного сигналу на ONU (дБм)	Швидкість інтернету (Мбіт/сек)	
	Низхідний потік даних	Висхідний потік даних
-27.04	336.09	40.67
-27.52	340.49	40.28
-27.98	339.37	40.54
-28.12	186.22	36.58
-28.33	121.88	40.3
-28.5	2.06	40.55
-29.08	1.87	42.54
-29.68	0	0

Дані про рівень вхідного сигналу були отримані за допомогою вимірювача оптичної потужності для мережі PON. З результатів тесту видно, що ONU все ще знаходиться у нормальному робочому режимі, коли оптична потужність перевищує значення -27.98 дБм. Коли рівень сигналу виходить за цю межу, то швидкість низхідного потоку даних падає непропорційно зі зменшенням оптичної потужності до моменту, поки з'єднання з мережею остаточно не буде втрачено [1].

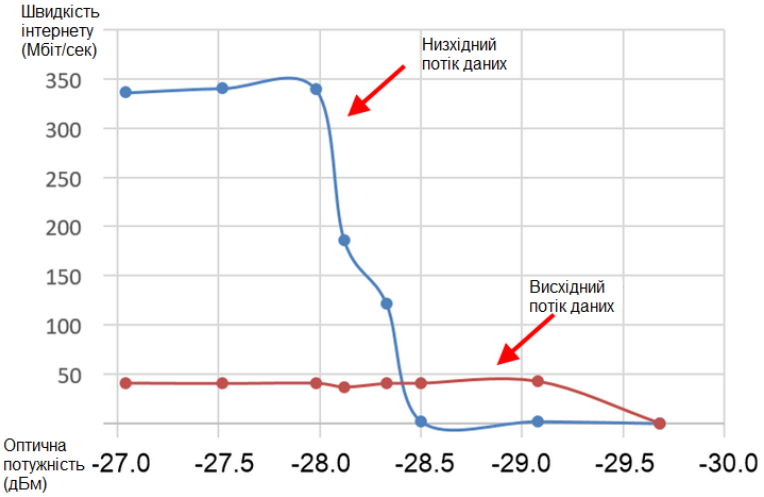


Рисунок 2 Залежність швидкості від оптичної потужності

Різниця у швидкості між низхідним та висхідним потоком даних зумовлюється обмеженням оператора широкосмугового зв'язку. Низький рівень оптичного сигналу практично не впливає на швидкість висхідного потоку, оскільки ONU випромінює сигнал лише тоді, коли отримує дозвіл від OLT та перериває обмін даними якщо такого сигналу немає.

Список використаних джерел

5. Вплив рівня оптичного сигналу на швидкість роботи мережі [Електронний ресурс] – Режим доступу до ресурсу: https://zhuanlan.zhihu.com/p/406909650

ПОРІВНЯЛЬНИЙ АНАЛІЗ CWDM ТА DWDM

Лаптінов Ярослав Борисович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

З початком широкомасштабного впровадження інформаційних технологій у всі сфери життя постала потреба у збільшенні пропускної здатності каналів передачі даних. Тож у сучасному світі для розбудови телекомунікаційно інфраструктури постачальниками широкополосного доступу повсюдно стали застосовуватись методи ущільнення каналів з мультиплексуванням з розділенням довжини хвилі(WDM).

WDM — Wavelength Division Multiplexing (спектральне ущільнення каналів) —це технологія мультиплексування з поділом по довжині хвилі. Використовуючи WDM, ми об'єднуємо мультиплексором серію оптичних сигналів із різних транспондерів в один пучок, але з різними довжинами хвиль та передаємо їх по одному волокну. На приймальному кінці демультиплексор поділяє оптичні сигнали з різними довжинами хвиль та посилає їх у різні транспондери для подальшої обробки та відновлення вихідного сигналу. Таким чином, два або більше оптичних сигналу з різними довжинами хвиль одночасно передаються по одній оптичній лінії, що називається мультиплексуванням з поділом по довжині хвилі.

Історично першими виникли двохвильові системи WDM, що працюють на центральних довжинах хвиль з другого та третього вікон прозорості кварцового волокна (1310 та 1550 нм). Головною перевагою таких систем є те, що через великий спектральний рознос повністю відсутній вплив каналів один на одного. Цей спосіб дозволяє або подвоїти швидкість передачі по одному оптичному волокну, або організувати дуплексний зв'язок.

Сучасні системи WDM існують у вигляді двох технологій: CWDM та DWDM.

Грубі WDM (англ. coarse WDM, скор. CWDM) - системи з частотним рознесенням каналів більше 2500ГГц, що дозволяють мультиплексувати не більше 18 каналів. CWDM, що використовуються в даний час, працюють у смузі від 1271нм до 1611нм, проміжок між каналами 20нм (2500 ГГц), можна мультиплексувати 18 спектральних каналів. Частотний план систем CWDM визначається стандартом ITU G.694.2. Область застосування технології – міські мережі з відстанню до 50 км. Перевагою цього виду WDM систем є [6] низька (проти іншими типами) вартість устаткування внаслідок менших вимог до компонентам.

Щільні WDM (англ. dense WDM, скор. DWDM) - системи з рознесенням каналів 100 ГГц, 50 ГГц, 25 ГГц, 12,5 ГГц дозволяють мультиплексувати до 40, 80, 160 і 320 каналів відповідно. Канали відраховуються з обох боків від центральної частоти 193,1 ТГц, що відповідає довжині хвилі 1552,52 нм. Частотний план систем DWDM визначається стандартом ITU G.694.1. Область застосування – магістральні мережі. Цей вид систем WDM пред'являє більш високі вимоги до компонентів, ніж CWDM (ширина спектра джерела випромінювання, стабілізація температур джерела і т. д.). Поштовх до бурхливого розвитку мереж DWDM дало появу недорогих та ефективних волоконних ербієвих підсилювачів (EDFA), що працюють у проміжку від 1525 до 1565 нм (третє вікно прозорості кварцового волокна).

Висновки

Основна відмінність CWDM та DWDM – рознесення довжин хвиль каналів. Різниця між каналами CWDM становить 20 нм, а різниця між каналами DWDM становить 1,6\0,8\0,4 нм (200 ГГц\100 ГГц\50 ГГц), що набагато менше, ніж CWDM. Це, само собою, відбивається і на пропускну здатність, яку CWDM і DWDM - чим більше каналів може використовуватися, тим більше сигналів можна перенести. Або іншими словами, модуль DWDM додатково збільшує пропускну здатність і пропускну здатність системи, використовуючи ближче розташовані довжини хвиль для передачі більшої кількості сигналів по тому самому волокну.

Грубе рознесення каналів, великий проміжок між ними, дають можливість використання лазера нижчої якості порінянно з DWDM та простіших мультиплексорів та демультиплексорів, що відображається на ціні. Системи з щільним рознесенням каналів дають перевагу у швидкості, що обумовлює їх використання на більш навантажених ділянках мереж.

Література:

1. Горбатий І. В., Бондарєв А. П. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи. Львів : Видавництво Львівської політехніки, 2016. - 336 с.

2. Computer Networks and their Protocols / Д.Дэвис, Д. Барбер, С. Соломонідес, У. Прайс., 1982. – 562 с.

РОЗПОДІЛ НАВАНТАЖЕННЯ КІЛЬКОМА МАРШРУТАМИ У TCP/IP

Бєлобородов Вадим Дмитрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Розподіл навантаження кількома маршрутами (Multi-Path Load Balancing) у TCP/IP може бути виконаний багатьма методами, як самими їми, так і спеціально розробленними протоколами. Дані способи дозволяють знизити загальні витрати на встановлення з'єднань за рахунок скорочення числа зовнішніх маршрутизаторів та серверів. Їх реалізація дозволяє звільнити частину наявних IP-адрес за рахунок більш ефективного використання IP-адрес, що залишилися. За допомогою цього можна підвищити продуктивність самої мережі.

Декілька прикладів самих протоколів та способів, які дозволяють розподілити наватнтаження на мережу:

Equal-Cost Multi-Path (ECMP) - протокол маршрутизації, який дозволяє розділити навантаження між кількома рівнозначними шляхами з однаковими метриками. Дозволяє використовувати більше одного маршруту для пересилання пакетів і таким чином збільшити пропускну здатність та забезпечити більшу надійність мережі. При використанні ECMP маршрутизатори зберігають в своїх таблицях маршрутизації кілька можливих шляхів з однаковою метрикою для кожної мережної адреси. Коли пакет потребує пересилання, маршрутизатор вибирає один з наявних маршрутів з однаковою метрикою за допомогою алгоритму розподілу навантаження, наприклад, round-robin або хешування. ECMP може бути використаний в різних протоколах маршрутизації, таких як OSPF (Open Shortest Path First) або BGP (Border Gateway Protocol).

Link Aggregation (LACP) - дозволяє об'єднати фізичні мережеві порти в логічну групу (link aggregation group або LAG) для створення більш широкої смуги пропускання та розподілу навантаження між цими портами. LACP забезпечує синхронізацію та керування логічною групою портів. Він дозволяє автоматично визначити і налаштувати агреговані порти на пристроях, підтримуючи протокол. Замість ручного налаштування кожного фізичного інтерфейсу, протокол встановлює зв'язок між пристроями та автоматично об'єднує інтерфейси в один логічний агрегований порт, дозволяє розподіляти трафік між фізичними інтерфейсами в агрегованому порті. Це покращує загальну пропускну здатність мережі шляхом розподілу навантаження між доступними інтерфейсами.

Round Robin DNS. Цей метод дозволяє розподілити навантаження, при якому DNS-сервер надає кілька IP-адрес, пов'язаних з доменом, у випадковому порядку (у традиційному налаштуванні DNS сервер повертає одну IP-адресу для запиту на доменне ім'я). Це дозволяє

розподіляти навантаження між різними серверами, які мають одне і те ж доменне ім'я. Клієнти отримують різні IP-адреси для кожного запиту, що розподіляє навантаження між серверами. При цьому відбувається використання доступних ресурсів кожного сервера.

Content Delivery Networks (CDNs) – це розподілені мережі серверів, розташованих у різних географічних місцях по всьому світу. Основна мета CDNs полягає в ефективній та надійній доставці контенту, такого як веб-сторінки, зображення, відео та інші цифрові ресурси, користувачам. CDNs працюють за допомогою кешування та доставки контенту з серверів, які знаходяться найближче до користувачів. Коли користувач запитує контент, CDN постачає його з найближчого сервера (тобто з точки присутності), замість отримання його з оригінального сервера, що дозволяє зменшити затримку та покращити швидкість доставки контенту.

Прикладів протоколів та методів, що дозволяють розподілити навантаження мережі маршрутами у TCP/IP ще дуже багато. Кожні з них та який саме використовувати – треба буде виходити з самих потреб, завантаженню мережі та для чого саме буде використовуватися.

Література:

1. Комп'ютерні мережі. 6-те вид. Таненбаум Е. С., Фімстер Н., Уезеролл Д.

ПІДВОДНІ ВОЛОКОННО-ОПТИЧНІ СИСТЕМИ ЗВ’ЯЗКУ

Наталенко Михайло Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
Бабенко Леонід Петрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Підводні волоконно-оптичні системи зв’язку стали критично важливим засобом передачі даних і зв’язку між різними точками світу. Ці системи використовують оптичні волокна для передачі сигналів під водою, які потім перетворюються на електричні сигнали та надсилаються за призначенням. Розробка та особливості побудови підводних волоконно-оптичних систем зв'язку були предметом інтенсивних досліджень, оскільки інженери продовжують вдосконалювати технологію та оптимізувати її продуктивність.

Однією з основних переваг підводних волоконно-оптичних систем зв’язку є їх швидкість і надійність. Порівняно з іншими формами зв’язку, такими як супутниковий або радіозв’язок, волоконно-оптичні системи можуть передавати дані на набагато вищих швидкостях, з меншою затримкою та більшою надійністю. Це робить їх ідеальними для застосувань, де швидка та точна передача даних є критичною, наприклад, у наукових дослідженнях або військових операціях.

Будівництво підводних волоконно-оптичних систем зв'язку є складним і вимагає ретельного планування та проектування. Інженери повинні брати до уваги низку факторів, таких як глибина та відстань системи, тип використовуваного кабелю та умови навколишнього середовища, яким буде піддаватися система. Наприклад, підводні волоконно-оптичні системи зв’язку повинні бути стійкими до пошкодження тиском води, морським життям та іншими небезпеками, які можуть бути присутні в океані.

Існує декілька типів підводних кабелів, які використовуються для волоконно-оптичних систем зв’язку, кожен із яких має свої унікальні характеристики та переваги. Нижче наведено деякі з найбільш часто використовуваних типів підводних кабелів:

Неброньовані волоконно-оптичні кабелі: це найпростіший тип підводних кабелів, які використовуються у волоконно-оптичних системах зв’язку. Вони складаються з пучка оптичних волокон, загорнутих у захисне пластикове покриття. Ці кабелі гнучкі та легкі, томуїх легко розгортати та ремонтувати. Однак вони не підходять для використання в місцях, де існує високий ризик пошкодження морськими мешканцями або іншими небезпеками.

Броньовані волоконно-оптичні кабелі: броньовані волоконно-оптичні кабелі подібні до неброньованих кабелів, але загорнуті в шар сталі або алюмінію. Ця броня захищає кабелі від пошкодження морськими мешканцями, рибальськими сітками та іншими небезпеками. Ці кабелі важчі та менш гнучкі, ніж неброньовані кабелі, але вони забезпечують чудовий захист і довговічність.

Гібридні кабелі: гібридні кабелі поєднують волоконно-оптичні кабелі з електричними кабелями, що дозволяє їм передавати як дані, так і електроенергію. Ці кабелі зазвичай використовуються на морських нафтових і газових платформах, де вони забезпечують зв’язокі живлення платформи.

Сейсмічні кабелі: Сейсмічні кабелі призначені для використання в морських сейсмічних дослідженнях, де вони використовуються для збору даних про структуру та склад морського дна. Ці кабелі складаються з ряду гідрофонів і акселерометрів, які виявляють і вимірюють сейсмічні хвилі.

Шпорні кабелі: шлангові кабелі використовуються в підводному видобутку нафти та газу, де вони забезпечують живлення, зв’язок і контрольні сигнали для підводного обладнання, такого як насоси, клапани та датчики. Ці кабелі зазвичай набагато більші та складніші за інші типи підводних кабелів.

Однією з ключових особливостей підводних волоконно-оптичних систем зв'язку є їх здатність передавати дані на великі відстані. Це досягається за рахунок використання повторювачів, які підсилюють сигнал і дозволяють йому поширюватися далі, не втрачаючи цілісності. Використання ретрансляторів має вирішальне значення для передачі даних на великі відстані, наприклад між континентами, і революціонізувало спосіб спілкування та обміну інформацією в усьому світі.

Іншою важливою особливістю підводних волоконно-оптичних систем зв'язку є їх здатність працювати в суворих умовах. Ці системи розроблені таким чином, щоб витримувати екстремальні температури, тиск та інші фактори навколишнього середовища, які зазвичай призводять до збою інших типів систем зв’язку. Це робить їх ідеальними для використання під час підводних досліджень, де надійний зв’язок має вирішальне значення для успіху наукових експериментів [2].

Дослідження розробки та особливостей побудови підводних волоконно-оптичних систем зв'язку тривають, інженери постійно працюють над вдосконаленням технології та оптимізацією її роботи.

Однією з головних наукових проблем, з якими ми стикаємося сьогодні при вдосконаленні підводних оптоволоконних ліній зв’язку, є погіршення сигналу, яке спричинене затуханням і дисперсією.

Затухання означає втрату потужності сигналу під час його проходження по оптичному волокну, що може бути спричинено втратами на поглинання, розсіювання та вигин. Під час підводного зв’язку ослаблення є особливо проблематичним через великі відстані та поглинання світла водою. Це може призвести до зниження потужності та якості сигналу, що може обмежити швидкість передачі та відстань системи зв’язку.

Дисперсія означає спотворення сигналу, спричинене різною швидкістю розповсюдження різних довжин хвиль світла. Існує два типи дисперсії: хроматична дисперсія, яка спричинена різними швидкостями різних кольорів світла, і дисперсія поляризаційного режиму, яка спричинена різними поляризаційними станами світла. Розсіювання може спричинити спотворення сигналу та обмежити пропускну здатність системи зв’язку [3].

Щоб вирішити ці наукові проблеми, дослідники працюють над розробкою нових технологій і методів для покращення продуктивності підводних оптоволоконних телекомунікаційних ліній. Наприклад, дослідники вивчають можливість використання нових матеріалів і покриттів для зменшення втрати сигналу через загасання та підвищення довговічності кабелів у суворих підводних умовах. Вони також розробляють нові методи обробки сигналів і алгоритми для компенсації ефектів дисперсії та підвищення якості сигналу. Інші напрямки досліджень зосереджені на вдосконаленні конструкції та розгортанні підводних оптоволоконних телекомунікаційних ліній, таких як розробка більш ефективних і рентабельних методів прокладки та обслуговування кабелю. Крім того, дослідники вивчають використання інноваційних технологій, таких як підводні дрони та автономні транспортні засоби, для покращення моніторингу та обслуговування систем підводного зв'язку.

Список використаних джерел

1. Каток В.Б., Руденко І.Е., Однорог П.М. / Волоконно-оптичні системи зв'язку / посібник, 2016.

ДОСЛІДЖЕННЯ АРХІТЕКТУРИ БЕЗПРОВОДОВИХ МЕРЕЖ СТАНДАРТУ 802.11

Чирва Богдан Миколайович
Державний університет телекомунікацій

За останні кілька десятиліть безпроводові мережі стали невід'ємною частиною нашого життя, а їх популярність тільки зростає. Стандарт 802.11 відноситься до безпроводових мереж локального доступу і використовується у більшості беспровідних мереж Wi-Fi. У цьому есе розглянемо дослідження архітектури безпроводових мереж стандарту 802.11.

Стандарт 802.11 охоплює безпровідні мережі, що працюють в діапазоні радіочастот від 2,4 до 5 ГГц. Основними компонентами архітектури безпровідних мереж 802.11 є точки доступу (AP), клієнти і бездротові мережеві карти. AP - це бездротовий пристрій, який підключає бездротові клієнти до провідної мережі. Клієнти - це пристрої, які підключаються до AP, щоб отримувати доступ до мережі. Бездротові мережеві карти є пристроями, які встановлюються на пристрої і дозволяють йому підключатися до мережі.

Архітектура безпровідних мереж 802.11 базується на режимі доступу з часовим розподілом (TDMA) і режимі доступу з мультиплексуванням частот (OFDM). У режимі TDMA мережа розділяє час на періоди, під час яких можуть передаватися дані. У режимі OFDM сигнал розділяється на кілька сигналів нижчої частоти, що забезпечує більш ефективне використання радіочастотного діапазону.

Однією з основних переваг архітектури безпровідних мереж 802.11 є можливість підключення до мережі з будь-якого місця, де є доступ до мережі.

Стандарт IEEE 802.11 — це найпоширеніша бездротова мережева технологія в світі, яка забезпечує бездротове підключення для всього, від смартфонів і ноутбуків до розумних будинків і пристроїв Інтернету речей. Його популярність значною мірою пояснюється його гнучкістю, масштабованістю та надійністю, що дозволяє адаптувати його до широкого діапазону мережевих топологій і програм.

Стандарт 802.11 визначає фізичний (PHY) і рівень керування доступом до середовища (MAC) для бездротового зв'язку, включаючи використання різних діапазонів частот (2,4 ГГц і 5 ГГц), технологію множинного входу і множинного виходу (MIMO), а також різноманітну модуляцію та кодування. схеми підвищення пропускної здатності та надійності.

Однією з ключових особливостей стандарту 802.11 є його здатність підтримувати кілька точок доступу (AP) і роумінг між ними. Це дозволяє користувачам пересуватися в межах бездротової мережі без втрати з’єднання, що особливо важливо в таких середовищах, як лікарні, склади та мережі.

Проте стандарт 802.11 також має деякі обмеження, зокрема обмежений радіус дії, сприйнятливість до перешкод від інших бездротових пристроїв і вразливість безпеки. З часом ці проблеми були вирішені завдяки розробці нових стандартів і протоколів, таких як 802.11ac і 802.11ax, які забезпечують вищу швидкість, покращений радіус дії та кращу безпеку.

Загалом, стандарт 802.11 кардинально змінив правила бездротових мереж, забезпечивши широке коло додатків і послуг, недоступних для традиційних дротових мереж. Її постійна еволюція та розвиток гарантуватимуть, що вона залишиться ключовою технологією на довгі роки.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ WIMAX ДЛЯ ПОБУДОВИ МЕРЕЖ

Веденєєва Наталья Миколаївна,
Дейнекін Максим Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто Worldwide Interoperability for Microwave Access, більш відому як WIMAX – технології телекомунікацій. Її мета – передача бездротового зв'язку на довгі дистанції для широкого спектру пристроїв – настільні та портативні комп'ютери, мобільні телефони. WIMAX заснований на стандарті 802.16 і має також і іншу назву – Wireless MAN, яка, будучи менш поширеною, є більш правильною, оскільки насправді WIMAX не технологія, а назва форуму, на якому було узгоджено стандарт Wireless MAN.

Технологія WIMAX мала вирішити проблему Wi-Fi мереж – відносно низьку швидкість передачі даних та невисокий рівень покриття, разом з тим зберегти високу мобільність та швидкість розгортання. На даний момент WIMAX технологія може бути використана при побудові магістральних каналів, продовженням яких можуть виступати традиційні кабельні (DSL) та бездротові локальні мережі.[1]

Залежно від типу розв'язуваних завдань (фіксовані або мобільний доступ), є дві окремі версії стандарту, кожна з яких визначає потужність, ширину смуги пропускання, індивідуальний діапазон частот, методи доступу та передачі даних, а також способи модуляції та кодування сигналу, тому WIMAX-системи, що використовують різні версії стандарту, практично несумісні. Специфікацію фіксованої версії WIMAX – 802.16d було затверджено у 2004 році. У цій версії організована підтримка пристроїв користувача, встановлених як усередині, так і зовні приміщень, пряма видимість при цьому необов'язкова. Обладнання використовує діапазон частот 2 – 11 Ггц.

Специфікація мобільної версії WIMAX – 802.16e, була затверджена через рік після затвердження фіксованої версії стандарту. Завдяки застосуванню масштабованого OFDM-доступу стала можливою робота пристроїв в умовах відсутності прямої видимості. Обладнання цієї версії використовує діапазон частот 2,3 – 13,6 ГГц. Конкурентами мобільної версії WIMAX є мобільні технології третього покоління (3G). [2]

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

ЗМІСТ ТА МОЖЛИВОСТІ СУЧАСНИХ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ (VPN)

Верхотуров Денис Олександрович
Державний університет телекомунікацій

VPN (англ. Virtual Private Network - віртуальна приватна мережа) - це комунікаційне середовище, у якому доступ контрольований через дозвіл сполучення між респондентами тільки всередині визначеної спільноти за інтересами і побудований на певних формах спільного використання основного комунікаційного середовища, де це основне комунікаційне середовище забезпечує послуги мережі на невиключній основі.

Можливості VPN мережі:

- Захист у загальнодоступних мережах Wi-Fi (Wireless Fidelity). Безкоштовними загальнодоступними мережами Wi-Fi зручно користуватися під час подорожей. На жаль, це небезпечно, бо вони не захищають навіть від простих кібератак. VPN-мережа шифрує ваші онлайн-дані та захищає особисту інформацію.
- Маскування під час перегляду вебсторінок. Маскування IP-адреси надзвичайно важливе для забезпечення конфіденційності роботи в мережі. Під час підключення до віртуальної приватної мережі ваше розташування та історія переглядів приховані від сторонніх.
- Доступ до сайтів із цензурою. У багатьох країнах доступ до різних веб-сайтів буває обмеженим через геоблокування чи цензуру.
- Захист від продажу особистих даних. Дані вашого браузера - цінна інформація для брокерів даних і маркетологів. VPN-мережа приховує ваші звички під час перегляду вебсторінок та інші дані, роблячи їх менш привабливими для всіх бізнес-об'єктів.
- Безпека та швидкість потокової передачі. VPN-мережа забезпечує конфіденційність підключення до улюблених потокових сервісів. Із надшвидкими серверами та необмеженою пропускною здатністю можна дивитися потоковий контент без обмежень швидкості та буферизації.
- Захист від цінової дискримінації. Веб-сайти та різні служби коригують ціни на свої продукти, використовуючи дані про розташування і файли cookie. За допомогою VPN-мережі можна захиститися від маркетингових прийомів і заощаджувати, коли щось купуєте в Інтернеті.

Принцип дії VPN мережі:

- VPN встановлює безпечне з’єднання. При підключенні до Інтернету VPN-мережа створює віртуальний захищений тунель між користувачем та одним із своїх серверів. Через цей тунель передаватиметься весь ваш інтернет-трафік.
- VPN змінює вашу IP-адресу. Коли ваш інтернет-трафік проходить через VPN-тунель, ваша IP-адреса змінюється. У цьому випадку веб-сайти та служби, до яких ви підключаєтеся, вважають, що ви знаходитеся там, де розташований вибраний вами сервер.
- VPN зашифровує ваші дані. Задля безпеки процесу тунелювання VPN-мережа приховує ваші дані під кодом (зашифровує їх), щоб запобігти їхньому витоку та не дозволити стороннім ідентифікувати вас.

Різновиди VPN-мережі

VPN-мережі для віддаленого доступу. VPN-мережі для віддаленого доступу дозволяє користувачеві безпечно підключатися до віддаленої мережі. Цей спосіб забезпечує той самий рівень безпеки, як і під час підключення до мережі з безпечного місця. Можливо, ви користувалися ним для доступу до внутрішньої мережі своєї компанії, працюючи з дому або іншого місця за межами офісу.

VPN-з'єднання «мережа-мережа». VPN типу «мережа-мережа» дозволяють з'єднувати декілька внутрішніх мереж у єдину мережу. Цією технологією користуються великі компанії з багатьма офісами по всьому світу. VPN типу «мережа-мережа» об'єднує внутрішні мережі всіх офісів в єдину цільну мережу, якою можуть користуватися всі співробітники компанії - при цьому їм не потрібно щоразу підключатися до мереж інших офісів або просити колег пересилати звідти необхідні дані.

Персональні VPN-мережі. Персональні VPN, або VPN споживчого рівня призначені для окремих користувачів. Такий сервіс замість підключення до іншої мережі підключає користувача до VPN-сервера із застосуванням заходів безпеки та шифрування. Перевага такого рішення полягає в тому, що веб-сайт або сервіс, до якого користувач підключається через персональний VPN, вважає це підключенням з VPN-сервера.

VPN-тунелювання

В основі тунелювання лежить механізм інкапсуляції, який приховує VPN-з’єднання в загальнодоступному Інтернеті. Той, хто захоче перевірити ваше інтернет-з’єднання, побачить, що ви використовуєте VPN, але не побачить, що саме ви робите у мережі. VPN-тунелі можуть створюватися різними способами за допомогою різних VPN-протоколів.

VPN-протоколи

- OpenVPN. OpenVPN - це VPN-протокол із відкритим вихідним кодом. В цілому він менш ефективний, ніж IKEV2 і WireGuard.
- WireGuard®. WireGuard - це відносно новий протокол, який перевершує OpenVPN і IPSec за характеристиками енергоспоживання та продуктивності, маючи всього 4000 рядків коду.
- IKEv2/IPSec (Internet Key Exchange). IKEv2 за якістю не поступається протоколу WireGuard.
- PPTP (Point-to-Point Tunneling Protocol) і LT2P/IPSec. Обидва дуже застарілі протоколи тунелювання. Вони досить швидкі, але значно поступаються іншим у безпеці та надійності.
- SSTP (Secure Socket Tunneling Protocol). SSTP - це протокол тунелювання, а не VPN-протокол. Це означає, що йому не вистачає функціональності OpenVPN, IKEv2 і WireGuard.
- Shadowsocks. Shadowsocks - не VPN-протокол, а проксі для тунелювання, однак він може працювати як протокол на VPN-клієнтах. Його створили з єдиною метою - обійти Великий китайський брандмауер.

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ СТАНДАРТУ ПЕРЕДАЧІ ДАНИХ ZIGBEE

Веденєєва Наталья Миколаївна,
Дейнекін Максим Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто ZigBee – стандарт бездротового зв'язку, призначений для систем керування та збору даних. Він дозволяє створювати бездротові мережі, що самостійно організуються і відновлюються, з підтримкою автоматичної ретрансляції повідомлень, а також мобільних і батарейних вузлів.

Останні кілька років спостерігається посилення інтересу з боку розробників радіоелектронної апаратури до технологій та стандартів бездротового зв'язку, що діють на коротких відстанях (ZigBee, Bluetooth, Wi-Fi, UWB).[1]

На сьогоднішній день технологія ZigBee виходить за межі дослідницьких лабораторій, вона знаходить широке застосування на практиці у створенні бездротових мереж датчиків, систем автоматизації будівель, систем управління в промисловості, охоронних системах. Мережі з використанням ZigBee забезпечують захист інформації, що передається, і гарантують цілісну доставку пакетів незважаючи на невелику швидкість передачі даних.

Стандарт передбачає роботу у частотних діапазонах 868 МГц, 915 МГц та 2,4 ГГц. Досягти найбільшої швидкості та перешкодостійкості можливо використовуючи діапазон 2,4 ГГц. З цієї причини багато виробників мікросхем виробляють приймачі саме під цей діапазон. Він передбачає 16 частотних каналів із кроком 5 МГц. Технічна швидкість передачі даних з огляду на службову інформацію досягає 250 кбіт/с. Для передачі корисних даних, залежно від кількості ретрансляцій та завантаженості мережі, середня пропускна здатність вузла варіюється від 5 до 40 кбіт/с.

ZigBee застосовується у разі, коли в межах прямої видимості дальність радіозв'язку є недостатньо великою, і виникає потреба у її нарощуванні із збереженням енергоспоживання на низькому рівні. Під час роботи всередині приміщення, відстані між вузлами мережі можуть становити десятки метрів, на відкритому просторі – сотні метрів. Зону покриття мережі можна значно збільшити за рахунок репітерів.

Характеристики стандарту забезпечують:

- Підтримка високого рівня захисту даних, що передаються;
- Гнучкість у налаштуванні вузлів мережі;
- Отримання швидкості обміну інформацією по радіоканалу до 250 кбіт/с;
- Підтримка однієї мережі до кількох тисяч вузлів;
- Створення складних мережевих рішень, застосовуючи автоматичну маршрутизацію, ретрансляцію пакетів даних, а також відновлення роботи мережі при виході з експлуатації її окремих ділянок.[2]

Топологія мережі

Мережа ZigBee має пористу топологію (mesh-топологія), завдяки чому пристрої зв'язуються один з одним безпосередньо або через проміжні вузли мережі. Ця топологія передбачає й інші варіанти вибору маршруту між вузлами. Пакет передається від одного вузла до іншого, доки не потрапить до кінцевого одержувача. Топологією передбачені альтернативні шляхи проходження повідомлення у випадку, якщо один із елементів мережі виходить з ладу.

Література

1. Є.В. Буров // Комп’ютерні мережі. / 2-е вид., оновл. і доп. – Львів –Бак, 2003,87 с

2. Особенности и применение технологии ZigBee- – Режим доступу до ресурсу: https://real-trac.com/ru/company/blog/tehnologiya_zigbee_ee_osobennosti_i_primenenie/

РОЗРОБКА ПРОЕКТУ МЕРЕЖІ ДОСТУПУ ЗА ТЕХНОЛОГІЄЮ FTTX

Козоріз Олена Олександрівна,
Кучугура Світлана Миколаївна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто технологію FTTx (Fiber to the x - оптичне волокно до точки X), назва якої походить від великих літер англійського виразу Fiber-to-the-build/home, що означає «оптика в кожен будинок». Цей термін застосовується для будь-якої комп'ютерної мережі, де від вузла зв'язку до певного місця (точка X) доходить оптоволоконний кабель. Широка смуга систем FTTx відкриває нові можливості надання абонентам більшої кількості нових послуг.

Технологія абонентського доступу FTTB (з англійської перекладається як «волокно до будівлі») є дуже затребуваною. Вона відрізняється безпекою, простотою узгодження при розгортанні мережі. В оптоволоконних кабелях та в розподільчих мережах вузлів другого рівня використовується мережа для передачі даних та мережа аналогового кабельного телебачення. Обладнання спеціалізоване.[1]

Її особливості:

- Висока надійність і низька ймовірність відмови;
- Простота побудови паралельних цифрових мереж;
- Простота реалізації нових цифрових технологій;
- Робота за низьких вхідних оптичних потужностей;

Топологія цієї мережі складається з вузла передачі даних, магістральної волоконно-оптичної лінії зв'язку та розподільчої мережі.

Використання FTTB технології вимагає виконання певних умов щодо забезпечення обладнання електроживленням та дотримання вимог безпеки, тому цій технології часто віддають перевагу телекомунікаційні компанії у великих та середніх містах. При проектуванні мережі широкосмугового доступу на основі FTTB технології фахівцям потрібно зробити максимально чіткі розрахунки густини абонентів, оскільки це позначається на рентабельності проектів.[2]

Література

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

4. Андрушко Л.М., Вознесенський В.А., Каток В.Б. та інші. Довінник по волоконно-оптичних лініях зв‘язку, Вінниця: ВНТУ 2005. - 225 с.

МЕТОДИКА СТВОРЕННЯ ПРОГРАМНОГО СИМУЛЯТОРА ДЛЯ МОДЕЛЮВАННЯ БАГАТОКАНАЛЬНОЇ ЦИФРОВОЇ СИСТЕМИ ЗВ'ЯЗКУ З ЧАСОВИМ РОЗПОДІЛОМ СИГНАЛІВ

Козоріз Олена Олександрівна,
Кучугура Світлана Миколаївна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто телекомунікаційні системи - це невід'ємна частина сучасного світу. Все більше різних інформаційних технологій входять в побут людства. Потреба в отриманні інформації різного роду, будь то телефонні дзвінки або ж проведення часу в глобальній мережі, призводить до постійного збільшення числа персональних пристроїв і устаткування засобів зв'язку. Одноканальні системи зв'язку втратили свою актуальність у зв'язку з тим, що вже давно вони не справляються з потоками переданих даних.

На даний момент використовуються багатоканальні системи зв'язку (БСП). Поділ інформаційних каналів в таких системах може реалізовуватися різними способами. Найбільш популярними варіантами множинного доступу з системами зв'язку є часвовий поділ каналів TDMA (Time Division Multiply Access) і кодове розділення каналів CDMA (Code Division Multiply Access). Обидва методи працюють з цифровим представленням інформації.

Цікавою областю розробки та конструювання БСП є моделювання параметрів цих систем при передачі потоків даних. В даний час існує безліч середовищ подібного моделювання. Всі вони дозволяють не тільки візуалізувати саму систему передачі даних, але і змінюючи її параметри, прогнозувати рівень зашумлення сигналу при проходженні його по каналу зв'язку з певними характеристиками, розробляти різні алгоритми підвищення перешкодозахищеності каналу і т.п. В рамках навчання студентів за напрямами, пов'язаними з інформаційно-комунікаційних системами зв'язку найбільшу популярність, придбали такі середовища моделювання як Simulink (Matlab) і LabVIEW. Ці середовища дозволяють студентам успішно моделювати канали передачі даних, займатися створенням БСП з різними видами поділу каналів, обробляти потоки інформації і застосовувати різні алгоритми кодування сигналів. Є й інші середовища-симулятори: наприклад, Scilab. Всі вони відповідають основним вимогам, що пред'являються до симуляторам фізичних процесів, дозволяють виконувати лабораторні та дослідницькі роботи, не вдаючись до створення СП на фізичному рівні. Однак у всіх у них є один недолік: для роботи в цих середовищах симуляції необхідна дорога ліцензія. У цьому ключі у пересічного студента є тільки дві можливості роботи з такими симуляторами:

- користуватися коротким проміжком часу, який надає навчальний заклад, що має ліцензію на використання і роботу з цим програмним забезпеченням;
- придбання ліцензії за власний рахунок.[1]

Перший варіант з успіхом використовується всіма студентами згаданого вище напрямки. Однак обмеження за часом роботи з симуляторами не дозволяє студенту повноцінно зануриться у вивчення систем зв'язку на рівні моделювання. Другий варіант для більшості студентів не є прийнятним через високу вартість ліцензій на подібні ПО. У зв'язку з вищесказаним бачиться актуальною задача створення повноцінної і загальнодоступною середовища симуляції фізичних процесів передачі сигналів по різним системам зв'язку.

Метою цієї роботи є розробка програмного симулятора, що візуалізує в форматі web-інтерфейсу моделювання багатоканальної цифрової системи зв'язку з часовим поділом каналів.

Завданнями роботи є:

- аналіз існуючих симуляторів передачі сигналів, який повинен бути проведений за наступними критеріями: різноманітність елементної бази і додаткових бібліотек симулятора, зручність інтерфейсу, можливості варіювання параметрів переданих потоків даних, можливості варіювання параметрів елементів систем зв'язку доступність симулятора для фізичних осіб;
- розробка архітектури симулятора в форматі web-додатки для основних браузерів;
- розробка мережевої структури множинного доступу користувачів;
- розробка та реалізація елементної бази симулятора;
- створення повноцінного користувальницького інтерфейсу для надання можливості моделювання багатоканальної системи зв'язку;
- перевірка відповідності моделювання передачі цифрового сигналу по трьохканальної системі зв'язку з часовим поділом каналів з параметрами реального сигналу, який передається за подібною БСП ВРК.[2]

Підсумком роботи має стати додаток для браузера, що дозволяє симулювати МПС з ЧПК для будь-якого виду цифрових потів даних для будь-якого числа каналів.

ЛІТЕРАТУРА

5. Бондаревский А.С., Лебедев, А.В. Имитационное моделирование: определение, применяемость и техническая реализация // Фундаментальные исследования. – 2011. – № 12-3. – С. 535-541.
6. Дьяконов В.П. MATLAB 6.5 SP1/7.0 + Simulink 5/6. Основы применения. – Litres, 2017. – 807 с.

АРХІТЕКТУРА ПОБУДОВИ ТРАНСПОРТНИХ МЕРЕЖ SDH

Ланковський Владислав Юрійович,
Михальченко Ілля Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто архітектурні рішення при проектуванні мережі SDH, можуть бути сформовані на базі використання елементарних топологій мережі як її окремі сегменти. Найчастіше використовується поєднання кільцевої та радіальної (типу «крапка-крапка») топологій або топологій послідовного лінійного ланцюга.

Архітектура типу «кільце-кільце»

Кільця в цьому з'єднанні можуть бути однакового, або різного рівнів ієрархії SDH. З'єднання двох кілець здійснюється за допомогою інтерфейсних карток. При такому з'єднанні можна використовувати необхідні оптичні триби попереднього ієрархічного рівня при переході від кільця одного рівня до іншого (наприклад, триб STM-1 при переході на кільце STM-4 і триб STM-4 при переході на кільце STM-16).

Лінійна архітектура для мережі великої довжини.

Для лінійних мереж великої протяжності відстань між термінальними мультиплексорами більша або багато більша за ту відстань, яка може бути рекомендована з точки зору максимального допустимого згасання волоконно-оптичного кабелю. У цьому випадку на маршруті (секція мультиплексування) між термінальними мультиплексорами встановлюються регенератори для відновлення оптичного оптичного сигналу (регенераційна секція). [1]

Однією з основних переваг технології SDH є можливість такої організації мережі, при якій досягається не тільки висока надійність її функціонування, зумовлена використанням волоконно-оптичного кабелю, але і можливість збереження або відновлення за дуже короткий час працездатності мережі навіть у разі відмови одного з її елементів або середовища передачі. Стосовно мереж SDH використовується термін "самовиліковна" мережа.

У принципі, існують різні методи забезпечення швидкого відновлення працездатності синхронних мереж.

ЛІТЕРАТУРА

7. Архитектурные решения сетей SDH – Режим доступу до ресурсу: https://studbooks.net/2340565/tehnika/arhitekturnye_resheniya_setey

ТИПОВІ СТРУКТУРІ МЕРЕЖ SDH

Ланковський Владислав Юрійович,
Михальченко Ілля Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто структурні рішення під час проектування мережі. Можуть бути сформовані з урахуванням елементарних топологій мережі як її окремих сегментів. З огляду на можливість самостійного використання окремих елементарних топологій ми розглянемо деякі мережі, що комбінують елементарні топології.

Радіально-кільцева структура

Ця мережа фактично побудована на основі використання двох базових топологій: «кільце» та «послідовний лінійний ланцюг». Замість останньої може бути використана простіша топологія «точка-точка». Число радіальних гілок обмежується допустимим навантаженням (загальним числом каналів доступу) на кільце.

Архітектура типу «кільце-кільце»

Кільця в цьому з'єднанні можуть бути однакового, або різного рівнів ієрархії SDH.

Каскадна схема з'єднання трьох кілець різного (по наростаючому) рівня - STM-1, STM-4, STM-16. При такому з'єднанні можна використовувати необхідні оптичні канали доступу попереднього ієрархічного рівня при переході від кільця одного рівня до іншого (наприклад, триб STM-1 при переході на кільце STM-4 і триб STM-4 при переході на кільце STM-16).

Архітектура розгалуженої мережі загального вигляду.

У процесі розвитку мережі SDH розробники можуть використовувати низку рішень, притаманних глобальних мереж. Наприклад, розгалужена мережа SDHс каскадно-кільцевою та комірчастою структурою. Остів (або опорно-магістральна мережа) цієї мережі сформований для простоти у вигляді одного мережного осередку, вузлами якого є комутатори типу SDXC, пов'язані за типом «кожен з кожним». До цього кістяка приєднані периферійні мережі SDH різної топології, які можуть бути «образами» або корпоративних мереж SDH, або сегментів інших глобальних мереж, або загальноміських мереж SDH. Ця структура може розглядатися як образ глобальної мережі SDH.

Ознайомившись з вищевикладеним матеріалом, необхідно розробити та обґрунтувати вибір тієї чи іншої структури первинної мережі ГТС на базі системи SDH.

ЛІТЕРАТУРА

8. Типовые структуры сетей sdh – Режим доступу до ресурсу: https://studfile.net/preview/2948124/page:6/

МЕТОДИКА ПОБУДОВИ МОДЕЛЕЙ РОЗПОДІЛУ РАДІОРЕСУРСІВ БЕЗДРОТОВИХ МЕРЕЖ

Романко Юлія Сергіївна,
Семіткивська Ірина Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто системи безпроводового зв'язку, які вплинули на характер взаємодії між людьми, а також між людиною та машиною, а також машина з машиною. До того ж остання має право на більшу увагу, оскільки дані технології розвиваються дуже стрімко і вимагають постійної адаптації для їх використання. Підключення яких до мережі змінить традиційне уявлення про Інтернет в цілому. Подібні пристрої можуть здійснювати передачу даних в автоматичному режимі без участі людини, тим самим генеруючи трафік міжмашинної взаємодії, для ефективного обслуговування якого в мережах бездротового зв'язку наступного покоління LTE.

До основних завдань в бездротових мережах наступного покоління відноситься оптимізація розподілу обмеженого числа частотного ресурсу серед користувачами. Рішенням завдань планування радіоресурсів, визначення пріоритетів доступу відносно типу передаючої інформації з необхідними вимогами до якості обслуговування (QoS, Quality of Service) займаються модулі управління радіоресурсами. Зважаючи на особливості M2M-трафіку, а також методи розподілу частотного ресурсу в мережах LTE, що з часом були оптимізовані для обслуговування користувачів традиційних послуг зв'язку (H2H, Human-to-Human), повинні бути доопрацьовані. Впровадження нових механізмів розподілу частотного ресурсу між чималою кількістю пристроїв, вимагає розробки нових математичних моделей, що описують особливості обслуговування M2M-трафіку.

В даний час не існує загальноприйнятого підходу з обслуговування M2M-трафіку, а саме оптимального методу для розподілу обмеженої кількості частотного ресурсу між H2H-користувачами і чималою кількістю M2M-пристроїв. таким чином існує велика кількість завдань планування і управління радіоресурсами, що робить вибрану тему актуальною.

Для виконання поставленої мети у роботі виконано наступні завдання:

- аналіз перспектив та особливостей застосування технологій M2M на базі мобільних мереж зв’язку;
- дослідження моделей розподілу радіоресурсів мобільних мереж зв’язку для мультисервисного трафіку міжмашинної взаємодії та пошук оптимального розміру діапазону радіоресурсів;
- реалізація алгоритму розрахунку розподілу ймовірностей станів моделі для M2M-трафіку, проведення аналізу показників ефективності.
- аналіз ймовірносно-часових характеристик моделі стільника мережі LTE та напрямки оптимізація схеми обслуговування M2M-трафіку.

Ступінь наукової розробки. У магістерській кваліфікаційній роботі запропоновано схему обслуговування M2M-трафіку з послідовним виділенням діапазону радіоресурсів фіксованого розміру і побудована математична модель. Для випадку однорідного M2M-трафіку розроблений рекурентний алгоритм розрахунку ЙЧХ системи і показано, що запропонована схема дозволяє забезпечувати задані параметри якості обслуговування.

Сформульовано багатокритеріальна задача пошуку оптимального розміру виділяємого діапазону радіоресурсів. Запропонований набір критеріїв і вагових коефіцієнтів не застосовувався раніше для схем обслуговування M2M-трафіку.

Практичне значення одержаних результатів. Реалізовані моделі та формули для обчислення їх ймовірносно-часових характеристик, отримані в магістерській роботі, призначені для розрахунку показників ефективності обслуговування M2M-трафіку в бездротових мережах зв'язку наступного покоління.[1]

ЛІТЕРАТУРА

1.Кучерявый Е.А. Управление трафиком и качество обслуживания сети интернет. М.: Наука и техника. 2014. - 336 с.

РОЗРОБКА ТА ВПРОВАДЖЕННЯ МЕТОДИКИ СТВОРЕННЯ МЕРЕЖ П'ЯТОГО ПОКОЛІННЯ ІЗ ЗАСТОСУВАННЯМ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ

Романко Юлія Сергіївна,
Семіткивська Ірина Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

У даній статті розглянуто мережі зв'язку "п'ятого покоління", т.зв. 5G, разом з аналізом великих даних (Big Data) та інтернетом речей (IoT) покликані стати однією з основ цифрової економіки, головною рушійною силою якої має стати штучний інтелект (II). За 40 з невеликим років змінилося чотири покоління мереж мобільного зв'язку. Якщо мережі першого покоління 1G давно зникли, то мережі 2G, 3G і 4G досі продовжують експлуатуватися. Більше того, кілька успадкованих інфраструктур мереж 3G і 4G органічно увійде до складу мобільних мереж п'ятого покоління 5G.

Розгорнуті мережі 5G забезпечують більшу швидкість і пропускну здатність для підтримки масштабного міжмашинного зв'язку та надання послуг із надмалою затримкою та високою надійністю для додатків, що нормуються за часом. Дані експлуатації різних існуючих комерційних мереж IMT-2020 свідчать про високу продуктивність у різних сценаріях, таких як густонаселені міські райони та точки доступу всередині приміщень.

Однак ці масштабні цілі, що стояли перед мережами 5G, вимагали вирішення серйозних проблем. Збільшення пропускної спроможності та швидкості передачі даних, яке забезпечили технології 5G, можуть вимагати більшого обсягу спектру та набагато більшої спектральної ефективності технологій у порівнянні з технологіями, що використовуються в системах 3G та 4G.

Частина цього додаткового обсягу спектра буде забезпечена за рахунок смуг частот вище 24 ГГц, що пов'язано зі значними труднощами. Перша проблема стосується характеристик поширення цієї частини спектра (міліметрових хвиль). Ці радіохвилі поширюються набагато менші відстані, ніж хвилі в діапазоні середніх (1-6 ГГц) і низьких (нижче 1 ГГц) частот.

Отже, покриття певної зони вимагатиме значного збільшення кількості базових станцій, що ускладнить інфраструктуру, у тому числі вимагатиме розміщення радіообладнання на вулиці, наприклад, на світлофорах, ліхтарних стовпах, опорах ЛЕП та блоках живлення.

Інша проблема стосується з'єднувальних ліній зв'язку 5G між базовими станціями та базовою мережею (транзитне з'єднання), що використовують як оптоволоконні, так і бездротові технології. Для впровадження послуг волоконно-оптичних мереж та забезпечення доступності

бездротових ліній транзитного зв'язку з достатньою пропускною здатністю, таких як мікрохвильові та супутникові лінії зв'язку та, можливо, системи станцій на висотній платформі (HAPS), потрібні значні зусилля.

Крім того, спектр є обмеженим та дуже цінним ресурсом, і на національному, регіональному та міжнародному рівнях спостерігається висока – і зростаюча – конкуренція за спектр. Оскільки радіочастотний спектр поділяється на смуги, що розподіляються різним радіослужбам, кожна смуга повинна використовуватися лише тими службами, для яких вона розподілена, а також із встановленими технічними умовами, щоб забезпечити можливість співіснування без створення шкідливих перешкод сусіднім службам.

У дослідженнях MCE-R розглядається спільне використання частот та сумісність між рухомими службами та рядом інших існуючих служб радіозв'язку, зокрема служб, що використовуються для супутникового зв'язку, метеорологічного прогнозування, моніторингу ресурсів Землі та зміни клімату, а також радіоастрономії.

У всьому світі на національному та міжнародному рівнях потрібне прийняття та застосування нормативно-правової бази, щоб уникнути перешкод між системами 5G та цими службами, створити життєздатну мобільну екосистему, розраховану на майбутнє, одночасно знизити ціни за рахунок ефекту масштабу на глобальному ринку та забезпечити функціональну сумісність та роумінг.

ЗАСОБИ ЗАХИСТУ БЕЗПРОВОДОВИХ МЕРЕЖ

Марчук Ольга Миколаївна,
Шабленко Сергій Васильович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто, як забезпечити безпеку пристрою бепроводового доступу і, відповідно, мінімізувати пов'язаний з цим видом доступу ризик. Якщо ваша безпроводова мережа не захищена, хакер може перехопити дані, що передаються по ній, отримати доступ до вашої мережі і файлів на вашому комп'ютері, а також виходити в інтернет, використовуючи ваше підключення.

Більшість сучасних комп'ютерів підтримують безпроводовий доступ до мережі. Іншими словами, вони можуть підключатися до Інтернету (і до інших пристроїв, які підтримують безпроводовий зв'язок) без кабелю мережі. Головна перевага безпроводового з'єднання – можливість працювати з інтернетом у будь-якій точці будинку або офісу (якщо дозволяє відстань між комп'ютером та пристроєм безпроводового доступу до мережі). Однак, якщо не вжити заходів щодо безпеки безпроводової мережі, можливі такі потенційно небезпечні ситуації:

- хакер може перехопити дані, що передаються або одержуються вами;
- хакер може отримати доступ до безпроводової мережі;
- Ваш канал доступу до Інтернету може бути захоплений іншою особою.[1]

Забезпечити безпеку пристрою безпроводового доступу і, відповідно, мінімізувати пов'язаний з цим видом доступу ризик можна за допомогою наступних нескладних кроків.

1. Змініть пароль адміністратора у безпроводовому пристрої. Хакеру легко з'ясувати, який пароль встановлюється за замовчуванням виробником пристрою, і використовувати цей пароль для доступу до безпроводової мережі. Уникайте паролів, які легко підібрати або вгадати.
2. Вимкніть трансляцію ідентифікатора мережі (SSID broadcasting; SSID – Service Set Identifier, ідентифікатор мережі), щоб безпроводовий пристрій не транслював в ефір інформацію про те, що він увімкнений.
3. Увімкніть шифрування трафіку: найкраще використовувати протокол WPA, якщо його підтримує (якщо ні, використовуйте WEP-шифр).
4. Змініть ідентифікатор мережі (SSID) пристрою. Якщо залишити ідентифікатор, встановлений за умовчанням виробником пристрою, зловмисник, дізнавшись цей ідентифікатор, зможе легко "засікти" вашу безпроводову мережу. Не використовуйте імена, які легко вгадати.[2]

ЛІТЕРАТУРА

1. Арсен Бандурян. Анализ угроз для беспроводных сетей. Журнал Компьютерное обозрение. № 12 (723) 2010 г.
2. Борисов В. И., Щербаков В. Б., Ермаков С. А. Спектр уязвимостей беспроводных сетей стандарта IEEE 802.11. Информация и безопасность. 2008. Т. 11. № 3.

ОСОБЛИВОСТІ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ СТРУКТУРНОЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ НАДАННЯ ПОСЛУГ МОБІЛЬНОГО ЗВ'ЯЗКУ НА ОСНОВІ МЕРЕЖ ПОСТ-NGN, 4G ТА 5G

Підгородецька Ольга Миколаївна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті досліджено питання організаційно-економічних засад надання послуг на основі мереж пост-NGN, 4G, 5G, і поклавши в основу категорії системного аналізу зосереджено увагу на структурній складності досліджуваної системи і на задачах підвищення її структурної надійності і безпеки логіко-ймовірнісними методами..

Організаційно-економічні аспекти надання послуг на основі мереж пост-NGN, 4G, 5G безсумнівно можна розглядати з позицій теорії складних систем. Такий підхід з одного боку дозволяє знаходити «слабкі» елементи складної системи, розроблювати заходи підвищення надійності цих елементів, вводячи, наприклад, структурну і часову надлишковість, застосовуючи взаємозамінюваність і відновлення для підвищення надійності всієї системи, що надає певної впевненості в відмовостійкості системи, тобто здатності продовжувати функціонувати в затвердженому стані при відмовах малої кількості її елементів. Але з іншого боку вказаний підхід не може відкидати можливості достатньо складних і багаторазових комбінацій подій, ймовірність яких дуже мала, але кількість таких «неймовірних» подій настільки суттєва, що вони в своїй сукупності не можуть не впливати на результати діяльності системи, не забезпечуючи її безпеки.

Під «складною системою» будемо розуміти систему, яку можна описати застосовуючи не менш ніж дві, в загалі кажучи, окремі математичні теорії.

Під «структурно-складними системами» будемо розуміти системи, які в процесі структурного аналізу не зводяться до послідовних паралельних та деревоподібних структур. Структурно складні системи описуються сценаріями мережевого типу з циклами і неусувною повторюваністю аргументів при їх формалізації. На сьогоднішній день розв'язуючи задачі, пов'язані з «структурно-складними» системами продуктивною виявляється теорія логіко-ймовірнісного моделювання.

Визначення 1. Функцію алгебри логіки, яка пов'язує стан елементів системи зі станом самої системи

$$y(x_1, x_2, ..., x_m) \quad X$$

будемо називати функцією структурної економічної безпеки, де системи має складну розгалуджену структуру і може знаходитись в характерних станах: в стані повної структурної економічної безпеки (y=1) і в стані небезпеки (y=0) .При цьому припускається, що стан всієї економічної системи детерміновано залежить від станів її елементів $x_1, x_2, ..., x_m$, які в свою чергу, також можуть знаходитись в одному з двох несумісних станів: або в стані економічної стабільності (x_i=1), або в стані економічного колапсу (x_i=0)[1].

Для економічних систем, в яких заміна ненадійного елемента (елемента, що відмовив, або здатний відмовити) на працездатний не може привести до відмови системи, функція структурної економічної безпеки є монотонною.

Визначення 2. Функція алгебри логіки y(x1, x2,..., xm) називається монотонною, якщо для будь-яких наборів співвідношення (a1, a2 ,..., am) і (b1,b2, ...bm) таких, що am≤bm , справджується

$$y(a1, a2 ,..., am) \leq y(b1, b2 ,..., bm).$$

Таким чином, досліджувану економічну систему надання послуг мобільного зв'язку, яка задовольняє вказаним умовам, можна називати системою з монотонною структурою або когерентною структурою. Відомо, що будь-яка функція алгебри логіки, записана через кон'юнкцію і диз'юнкцію (без заперечення), задає певну монотонну функцію.

Відомо також, що для монотонних структур введену нами функцію структурної економічної безпеки y(X) можна записати в термінах найкоротших шляхів успішного функціонування і мінімальних перетинів відмов системи. Найкоротший шлях успішного функціонування системи зображується кон'юнкцією її елементів, жодний елемент якої не можна вилучити, не порушивши функціонування системи

$$S_j = \bigwedge_{i \in K_{S_j}} x_i ,$$

де K_{S_j} – множина номерів елементів шляху.

Мінімальний перетин відмов системи, в свою чергу, можна представити кон'юнкцією заперечень станів її елементів, жоден компонент з якої не можна вилучити, не порушивши умову нефункціонування системи

$$D_j = \bigwedge_{i \in L_{D_j}} \overline{x_i} ,$$

де L_{D_j} – множина номерів, що відповідає даному перетину.

Використовуючи поняття ймовірнісної функції як ймовірності істиності функції алгебри логіки

$$P\{y(x1, x2 ,..., xm) = 1\},$$

оптимізаційну задачу для функції структурної економічної безпеки можна записати наступним чином:

$$P\{y(x_1, x_2, ..., x_m) = 1\} \to \max$$
$$f_i(x_1, x_2, ..., x_m) \geq f_i(\alpha_1^i, \alpha_2^i, ..., \alpha_m^i), i = \overline{1,m},$$

де α_j^i – наперед задані параметри (0,1) для обмеження знизу функції fi , що описує стан і-го елемента досліджуваної системи.

ЛІТЕРАТУРА

1. Надёжность и безопасность структурно-сложных систем / И.А. Рябинин. – СПб: Изд-во С.-Петерб. у-та, 2007. – 276 с

АНАЛІЗ ЗАГРОЗ, ЩО ВИНИКАЮТЬ ПІД ЧАС ПЕРЕДАЧІ ДАНИХ У БЕЗПРОВОДОВІЙ МЕРЕЖІ

Марчук Ольга Миколаївна,
Шабленко Сергій Васильович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

У даній статті розглянуто безпроводові технології, що працюють без фізичних та логічних обмежень своїх проводових аналогів, та наражають мережеву інфраструктуру і користувачів на значні ризики. Щоб зрозуміти, як забезпечити безпечне функціонування бездротових мереж, розглянемо їх докладніше.

Ризик перший - "Чужаки" (Rogues)

«Чужаками» називаються пристрої, які надають можливість неавторизованого доступу до корпоративної мережі, найчастіше в обхід механізмів захисту, визначених корпоративною безпековою політикою. Найчастіше це самі самовільно встановлені точки доступу.

Ризик другий – нефіксована природа зв'язку

Як уже зазначалося, безпроводові пристрої не «прив'язані» кабелем до розетки і можуть змінювати точки підключення до мережі безпосередньо в процесі роботи. Наприклад, можуть відбуватися «випадкові асоціації», або просто некоректно налаштований безпроводовий клієнт автоматично асоціюється і підключає користувача до найближчої безпроводової мережі. Такий механізм дозволяє зловмисникам «перемикати на себе» користувача, що нічого не підозрює, для подальшого сканування вразливостей, фішингу або атак типу Man-in-The-Middle. Крім того, якщо користувач одночасно підключений і до проводової мережі, то він стає зручною точкою входу, тобто класичним чужинцем.

Ризи третій – вразливість мереж та пристроїв

Деякі мережні пристрої можуть бути більш вразливими, ніж інші: неправильно налаштовані, використовують слабкі ключі шифрування або методи автентифікації з відомими вразливістями. Не дивно, що насамперед зловмисники атакують саме їх. Звіти аналітиків стверджують, що понад 70% успішних зламів безпроводових мереж відбулося саме внаслідок неправильної конфігурації точок доступу чи клієнтського програмного забезпечення.

Ризик четвертий – нові загрози та атаки

Безпроводові технології породили нові способи реалізації старих загроз, а також деякі нові, досі неможливі у проводових мережах. У всіх випадках боротися з атаками стало набагато важче, оскільки неможливо відстежити його фізичне розташування, ні ізолювати від мережі.

Ризик п'ятий – виток інформації з проводової мережі

Майже всі безпроводові мережі в якийсь момент з'єднуються з проводовими. Відповідно будь-яка безпроводова точка доступу може бути використана як плацдарм для атаки. Але це ще не все: деякі помилки в їхній конфігурації у поєднанні з помилками конфігурації проволової мережі можуть відкривати шляхи для витоків інформації.

Ризик шостий – особливості функціонування безпроводових мереж

Деякі особливості функціонування безпроводових мереж породжують додаткові проблеми, здатні впливати загалом на їх доступність, продуктивність, безпеку та вартість експлуатації. Для грамотного вирішення цих проблем потрібні спеціальний інструментарій підтримки та експлуатації, спеціальні механізми адміністрування та моніторингу, які не реалізовані в традиційному інструментарії управління безпроводовими мережами.[1]

Поширеність безпроводових технологій у наш час ставить під загрозу і ті мережі, де вони вже застосовуються, і ті, де ніколи не повинні використовуватися. Традиційні засоби захисту безсилі проти нових класів безпроводових загроз. При цьому ситуація ускладнюється тим, що необхідно захищати також і своїх користувачів (які можуть знаходитися і далеко від офісу), не порушуючи при цьому функціонування мереж сусідів, хоч би яким підозрілим воно не виглядало. Проте існують методи захисту від подібних загроз як безпроводових, так і проводових мереж та користувачів, що дозволяють впевнено та безпечно розгортати та використовувати безпроводові мережі.[2]

ЛІТЕРАТУРА

3. Attack on hash functions / V. D. Zyuzin, D. V. Vdovenko, V. N. Bolshakov [et al.] // EurAsian Journal of BioSciences. - 2020. - Vol. 14. - No 1. - P. 907913.
4. Кухта, А. И. Анализ методов защиты беспроводной сети Wi-fi / А. И. Кухта // Молодой исследователь Дона. - 2020. - № 2(23). - С. 41-48.

ОСОБЛИВОСТІ ТЕХНОЛОГІЇ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ OPENVPN

Шендерчук Владислав Віталійович
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій

OpenVPN - це технологія віртуальної приватної мережі (VPN), яка забезпечує безпеку та конфіденційність під час передачі даних через Інтернет. OpenVPN працює на базі відкритого коду та дозволяє забезпечити захист від перехоплення, зміни та крадіжки інформації під час її передачі. Також це означає, що програмне забезпечення може бути перевірене та аудитоване відкритою спільнотою.

Однією з переваг OpenVPN є його універсальність та сумісність з різними платформами. OpenVPN підтримується практично на всіх операційних системах, включаючи Windows, Linux, macOS, Android та iOS.

OpenVPN також відомий своєю можливістю встановлення з'єднання через різні типи мереж, включаючи Wi-Fi, Ethernet та мобільний зв'язок. Це дозволяє користувачам підключатись до мережі з будь-якого місця, навіть якщо вони знаходяться за межами своєї організації або країни.

Однією з ключових особливостей OpenVPN є його відкритий код, що означає, що програмне забезпечення може бути перевірене та аудитоване відкритою спільнотою. Це дозволяє забезпечити безпеку та надійність системи, оскільки будь-яка вразливість або помилка може бути виявлена та виправлена швидко.

Технологія OpenVPN базується на архітектурі клієнт-сервер, де сервер OpenVPN встановлюється на віддаленому сервері, а клієнт OpenVPN встановлюється на пристрої

користувача. Клієнт і сервер взаємодіють один з одним через Інтернет за допомогою протоколу OpenVPN, який забезпечує шифрування і аутентифікацію.

Основою безпеки є бібліотека OpenSSL, вона використовується для шифрування каналів передачі даних і керування. OpenSSL дозволяє виконувати всю роботу з шифрування та автентифікації, що дозволяє OpenVPN використовувати всі шифри, доступні в пакеті OpenSSL.

OpenVPN може працювати поверх протоколів User Datagram Protocol (UDP) або Transmission Control Protocol (TCP). Використання OpenVPN поширених мережевих протоколів (TCP і UDP) робить його бажаною альтернативою IPsec в ситуаціях, коли провайдер може блокувати певні VPN-протоколи, щоб змусити користувачів підписатися на більш дорогий рівень послуг "бізнес-класу". А це в свою чергу може коштувати купу грошей.

Порт 1194 - це офіційний номер порту, призначений IANA для OpenVPN.

OpenVPN пропонує два типи інтерфейсів для підключення до мережі через універсальний драйвер TUN/TAP. Він може створювати або IP-тунель (TUN) на рівні 3, або Ethernet-тунель (TAP) на рівні 2, який може передавати будь-який тип Ethernet-трафіку.

Однією з головних переваг OpenVPN є його здатність обходити брандмауери та інші мережеві обмеження. Протокол SSL/TLS забезпечує створення безпечного тунелю між клієнтом і сервером, що ускладнює виявлення і блокування трафіку брандмауерами. OpenVPN також підтримує динамічні IP-адреси, що полегшує підключення до віддаленого сервера, навіть якщо IP-адреса часто змінюється.

OpenVPN добре налаштовується, і користувачі можуть змінювати різні аспекти з'єднання, включаючи алгоритм шифрування, розмір ключа та центри сертифікації. Він також підтримує багатофакторну автентифікацію, яка забезпечує додатковий рівень безпеки з'єднання.

Список використаних джерел:

1. Eric F. Crist, Jan Just Keijser, book, "Mastering OpenVPN", Packt Publishing, 2015.

МЕТОДИКА ПОБУДОВИ КОРПОРАТИВНОЇ МЕРЕЖІ ДЛЯ ОФІСНОГО ПРИМІЩЕННЯ

Альошин Михайло Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Для сучасного офісу важливим елементом є продумано побудована та добре функціонуюча корпоративна мережа. Вона забезпечує спільне використання ресурсів, наприклад: комп'ютери, принтери, сервери та інші пристрої. Також за допомогою корпоративної мережі забезпечується зв'язок між робітниками та зовнішнім світом.

Щоб побудувати корпоративну мережу, слід прорахувати її структуру. Існують різні структури мереж, найвідоміші з них — це зірка, шина, кільце та гібридна. Однак найчастіше для офісних мереж використовують топологію "зірка". Вона представляє собою головний комутатор, який забезпечує передачу даних між кінцевими пристроями. Дана топологія вибрана через те, що вона доволі дешева, практична та зручна в використанні. Якщо розгортається мережа в великому офісі, то кількість комутаторів збільшується і вони будуються в "деревовидну" топологію, де в основі стоїть високопродуктивний комутатор.

Другий крок — вибір мережевого обладнання, яке буде використовуватися для побудови мережі, а маршрутизатори та комутатори. Вибирати слід продумано, це означає, що слід пам’ятати про розростання компанії, а з нею і мережі. Бажано, щоб всі пристрої були одного виробника, для зручності адміністрування мережі та ремонту обладнання.

Третій крок — вибір мережевих протоколів, які використовуються для передачі даних між пристроями співробітників. У корпоративній мережі використовується стек протоколів TCP/IP.

Четвертий крок — налаштування мережевих параметрів для пристроїв, що входять до складу корпоративної мережі. Для кожного пристрою, наприклад, потрібно встановити такі параметри, як IP-адреса, маска підмережі та шлюз за замовчуванням, щоб пристрої могли взаємодіяти один з одним. Також для великих компаній обов'язково потрібно налаштовувати віртуальні локальні мережі (VLAN), для розділення або ж об'єднання кінцевих пристроїв в одну мережу. Також це корисно для покращення безпеки мережі та для збільшення продуктивності мережі.

П'ятий крок — налаштування безпеки корпоративної мережі. Це включає встановлення паролів на пристроях користувачів, налаштування брандмауерів, встановлення антивірусного програмного забезпечення та інші заходи для захисту мережі від зловмисників і вірусів.

Шостий крок — тестування корпоративної мережі. На ньому можна перевірити, чи функціонує мережа, а також всі налаштування мережевих пристроїв.

Фінальний крок — підтримка та розвиток мережі компанії. Даний етап включає в себе регулярне оновлення програмного та апаратного забезпечення, перевірку мережевих помилок, підтримку мережевих протоколів та інші заходи для забезпечення безперебійної роботи мережі.

Одним словом, побудова корпоративної мережі в офісному приміщенні - це складний процес, який вимагає відповідального підходу. Застосування методів, описаних вище, забезпечить безперебійну роботу мережі та зменшить ризик перебоїв у роботі мережі. Важливо, щоб фахівці з комп'ютерних мереж мали високу кваліфікацію і використовували правильну методологію для його успішного завершення. Також важливо враховувати специфікацію офісного приміщення та потреби користувачів мережі. Застосування правильної методології та ретельне вивчення особливостей мережі забезпечить безперебійну та ефективну роботу корпоративної мережі.

Список використаних джерел:

1. Л.М. Олещенко // Організація комп'ютерних мереж / Електронне мережне навчальне видання, Київ, КПІ ім. Ігоря Сікорського 2018, 225 с.

МЕТОДИ ПРОКЛАДАННЯ ОПТОВОЛОКОННОГО КАБЕЛЮ ПІД ВОДОЮ

Наталенко Михайло Миколайович,
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
Бабенко Леонід Петрович,
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Системи підводного зв'язку за допомогою оптоволоконних кабелів стали важливим засобом передачі даних між континентами.

Згідно зі звітом, опублікованим Submarine Telecoms Forum у 2020 році, було приблизно 1,3 мільйона кілометрів (807 782 милі) підводного волоконно-оптичного кабелю, що експлуатується в усьому світі.

Крім того, у звіті зазначається, що на той час розроблялося кілька нових проектів підводного кабелю загальною довжиною приблизно 200 000 кілометрів (124 274 милі). Очікувалося, що ці проекти збільшать загальну довжину підводного волоконно-оптичного кабелю в експлуатації протягом наступних кількох років.

Проектування та прокладання оптоволоконних підводних систем зв'язку є постійним предметом досліджень та вдосконалення методів та технологій для оптимізації та підвищення продуктивності.

Існує кілька методів прокладки волоконно-оптичних кабелів під водою, і конкретний метод залежить від таких факторів, як глибина води, відстань, яку потрібно подолати, і тип морського дна.

Траншейний метод: у цьому методі траншея викопується на морському дні за допомогою плуга або траншейного інструменту. Потім волоконно-оптичний кабель укладається в траншею і засипається землею або піском. Цей метод підходить для мілководдя глибиною до 200 метрів.

Оранний метод: цей метод схожий на траншейний метод, але замість того, щоб рити траншею, плуг використовується для створення борозни на морському дні. Оптоволоконний кабель укладається в борозну і засипається піском або землею. Цей метод підходить для дрібних і помірно глибоких вод глибиною до 600 метрів.

Метод горизонтально-спрямованого буріння (ГНБ): у цьому методі використовується бурова установка для буріння отвору в морському дні від одного берега до іншого. Потім волоконно-оптичний кабель протягують через отвір і кріплять до берега. Цей метод підходить для перетину глибоких вод і часто використовується для з'єднання морських нафтових вишок з берегом.

Метод підводного плуга: цей метод використовується для прокладання волоконно-оптичних кабелів у дуже глибоких водах. Спеціально розроблений підводний плуг використовується для створення траншеї на морському дні, а волоконно-оптичний кабель прокладається в траншею та покривається осадом. Цей спосіб дорогий і трудомісткий, але є найнадійнішим способом прокладки волоконно-оптичних кабелів у глибоких водах.

Встановлення всмоктувального якоря: у цьому методі всмоктувальні якорі встановлюються на морському дні, а оптоволоконний кабель потім прокладається поверх якорів. Цей метод підходить для дрібних і помірно глибоких вод глибиною до 600 метрів і часто використовується в районах із кам'янистим морським дном.

Кожен з цих методів має свої переваги та недоліки:

Траншейний метод:

Переваги:

- підходить для мілководдя глибиною до 200 метрів.
- відносно швидкий і економічно ефективний метод.

Недоліки:

- процес копання траншей може завдати значних збурень морському дну та спичинити шкоду морським мешканцям.
- можливо, доведеться періодично обслуговувати траншею, щоб запобігти пошкодженню або оголенню кабелю.

Оранний метод:

Переваги:

- підходить для дрібних і помірно глибоких вод глибиною до 600 метрів.
- менш руйнує морське дно, ніж траншейний метод.

Недоліки:

- борозна, створена плугом, може потребувати періодичного догляду, щоб запобігти пошкодженню або оголенню кабелю.
- кабель може бути вразливим до пошкоджень іншими суднами або риболовлею.

Метод горизонтально-спрямованого буріння (ГНБ):

Переваги:

- підходить для глибоких вод і дозволяє уникнути порушення морського дна.
- кабель захищений від пошкоджень і оголення.

Недоліки:
- цей спосіб дорогий і трудомісткий.
- вимагає спеціального обладнання та досвіду.

Метод підводного плуга:

Переваги:
- підходить для дуже глибоких вод і дозволяє уникнути порушення морського дна.
- кабель захищений від пошкоджень і оголення.

Недоліки:
- дорогий і трудомісткий.
- вимагає спеціального обладнання та досвіду.

Встановлення всмоктуючого анкера:

Переваги:
- підходить для дрібних і помірно глибоких вод глибиною до 600 метрів.
- менш руйнує морське дно, ніж траншейний метод.

Недоліки:
- кабель може бути вразливим до пошкоджень іншими суднами або риболовлею.
- всмоктуючі анкери можуть порушити морське дно та морське життя під час встановлення.

Загалом, вибір конкретного способу прокладки волоконно-оптичних кабелів залежить від кількох факторів, таких як глибина води, відстань та умови навколишнього середовища. Кожен метод має свої переваги та недоліки, тому важливо ретельно всі фактори, перш ніж обирати метод.

Список використаних джерел

1. Каток В.Б., Руденко І.Е., Однорог П.М. / волоконно-оптичні системи зв’язку / посібник / 2016.

ФУНКЦІОНУВАННЯ ЛІТАЮЧИХ АПАРАТІВ НА БАЗІБЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

Бражій Петро Михайлович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

БЛА складається з декількох основних компонентів, включаючи систему керування польотом, сенсори, актуатори та комунікаційні системи. Система керування польотом відповідає за управління рухом БЛА та виконання польотних задач. Сенсори забезпечують збір даних про навколишнє середовище, такі як відео, теплові зображення, акустичні дані тощо. Актуатори використовуються для контролю руху та забезпечення стабільності польоту. Комунікаційні системи дозволяють передавати дані між БЛА та земною станцією або іншими апаратами.

Керування польотом: Керування польотом БЛА може бути здійснене за допомогою автономних або дистанційних систем. Автономне керування передбачає програмування маршруту польоту та виконання заданих завдань без прямого втручання оператора. Дистанційне керування дозволяє оператору в реальному часі контролювати рух та виконання завдань БЛА з допомогою пульта керування або комп'ютерної системи.

Сенсори та збір даних: БЛА використовує різноманітні сенсори для збору даних про навколишнє середовище. Це можуть бути відеокамери, теплові камери, радари, гіперспектральні сенсори, акустичні сенсори та інші. Сенсори забезпечують збір інформації,

необхідної для виконання зав

Обробка та аналіз даних: Після збору даних сенсорами, безпілотний літальний об'єкт виконує обробку та аналіз інформації. Це може включати виявлення об'єктів або особливостей в навколишньому середовищі, розпізнавання образів, вимірювання параметрів, класифікацію даних тощо. Аналізовані дані можуть використовуватися для прийняття рішень, наприклад, в режимі реального часу для виявлення загроз або для збирання статистичних даних для подальшого аналізу.

Комунікація та передача даних: Безпілотні літальні об'єкти можуть бути оснащені комунікаційними системами для передачі даних між БЛА та земною станцією або іншими апаратами. Це дозволяє оператору отримувати живу відеоінформацію, отримувати статусні звіти, передавати команди та отримувати дані для подальшого аналізу. Комунікаційні системи можуть використовувати бездротові технології, такі як Wi-Fi, радіо, супутникове зв'язку тощо.

Безпека та правові аспекти: Використання безпілотних літальних об'єктів також вимагає уваги до аспектів безпеки та дотримання правових вимог. Це включає забезпечення конфіденційності зібраних даних, забезпечення безпеки польоту, додержання регуляторних вимог щодо використання безпілотних систем та урахування етичних питань, пов'язаних з приватністю та безпекою.

Перспективи та майбутні напрями розвитку:

Розширення застосування БЛА в різних галузях, включаючи транспорт, моніторинг довкілля, сільське господарство, рятувальні операції та дослідження.

Розвиток більш ефективних та потужних сенсорів для збору даних, що дозволить отримувати більш точну та розширену інформацію.

Вдосконалення автономних систем керування, забезпечуючи безперебійну та безпечну роботу безпілотних літальних об'єктів.

Розвиток нових методів передачі даних та комунікаційних протоколів, що покращують швидкість і надійність зв'язку між БЛА та земною станцією.

Вирішення правових та етичних питань, пов'язаних зі збереженням приватності, безпекою та використанням безпілотних літальних об'єктів в громадських просторах.

Посилення досліджень і розвитку нових технологій, що приводить до зростання продуктивності та зниження вартості безпілотних літальних систем.

Список використаних джерел:

1. Paul G. Fahlstrom // Introduction to UAV Systems / John Wiley & Sons, 2012, 312 p.

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В БЕЗПРОВІДНИХ МЕРЕЖАХ СТАНДАРТУ IEEE 802.16

Карнасюк Андрій В'ячеславович
Державний університет телекомунікацій, м. Київ

Зростаюча популярність різноманітних мобільних пристроїв зініціювала масове поширення бездротових мереж, особливо останнім часом. На сьогодні бездротові технології отримали суттєвий розвиток і міцно ввійшли у повсякденне життя. З їх допомогою організовуються точки доступу в Інтернет, будуються локальні мережі. Наймасовішими та найперспективнішими на даний момент технологіями бездротового доступу, які можуть бути застосовані для передачі великої кількості трафіку різноманітного виду, є сімейство стандартів IEEE 802.16 для бездротових мереж міського рівня. Збільшення популярності таких мереж супроводжується тим, що вони стають суб’єктами великої кількості неправомірних вторгнень.

Для захисту даних, що транслюються через мережі, передбачено комплекс засобів безпеки, таких як аутентифікація, шифрування трафіку, прив’язка до MAC-адрес та інші. Проте далеко

не всі сучасні бездротові технології пропонують достатньо ефективні методи захисту інформації, жодна з них не знайшла глобального прийняття. Проблема полягає в оцінці великого числа існуючих рішень, які пропонуються для захисту бездротових ресурсів і у з'ясуванні напрямків дослідження інформаційної безпеки бездротових мереж.

Представлено результати досліджень та рішень щодо забезпечення захисту інформації у перспективних на сьогодні бездротових мережах стандартів 802.16, розглянуто методи захисту від загроз, характерних для бездротових мереж.

Стандарт IEEE 802.16 визначає протокол PKM (privacy and key management protocol), протокол приватності і управління ключем. Використовується алгоритм DES (Data Encryption Standard) в режимі зчеплення блока шифрів для шифрування даних. В даний час DES вважається небезпечним, тому в додаток до стандарту IEEE 802.16e для шифрування даних був доданий алгоритм AES (Advanced Encryption Standard).

Фактори уразливості стандарту IEEE 802.16:

Атаки фізичного рівня, такі як глушіння передачі сигналу, що веде до відмови доступу або лавинний наплив кадрів (flooding), що має на меті виснажити батарею станції. Ефективних способів протистояти таким загрозам на сьогодні немає.

- Самозвані базові станції, що пов'язані з відсутністю сертифіката базової станції. У стандарті проявляється явна несиметричність у питаннях аутентифікації. Запропоноване рішення цієї проблеми – інфраструктура управління ключем у бездротовому середовищі (WKMI, wireless key management infrastructure), заснована на стандарті IEEE 802.11i. У цій інфраструктурі є взаємна аутентифікація за допомогою сертифікатів X.509.

- Уразливість, пов'язана з невипадковістю генерації базовою станцією ключів авторизації. Взаємна участь базової та абонентської станції, можливо, вирішило б цю проблему.

- Можливість повторно використовувати ключі TEK (Traffic Encryption Key), термін життя яких вже закінчився. Це пов'язано з дуже малим розміром поля EKS (Encryption Key Sequence) індексу ключа TEK.

- Небезпекою використання шифрування DES, при досить великому часу життя ключа TEK та інтенсивному обміні повідомленнями можливість злому шифру становить реальну загрозу безпеці. Ця проблема була усунена з введенням шифрування AES у поправці до стандарту IEEE 802.16e. Проте велика кількість користувачів до цих пір має обладнання, що підтримує лише старий стандарт IEEE 802.16.

У таблиці 1 наведено результати порівняльного аналізу систем захисту даних у сьогоденних бездротових мережах.

Таблиця 1 Назва	Стандарт	Функції безпеки	Інші назви
WEP	802.11	RC4	Transitional Security Network (TSN)
802.1X	802.1X	EAPOL (EAP-TLS/PEAP/EAP-TTLS/Cisco-LEAP/EAP-FAST), WEP, PMK	Port-Based Security
WPA	802.11i Draft3	RC4, AES/TKIP, 802.1X/PSK	Transitional Security Network (TSN)
WPA2	802.11i	PKM, RC4, AES/TKIP, 802.1X/PSK, CCMP	Robust Security Network (RSN)
SA	802.16e	PKM, DES/3DES, AES	Data/Authorization Security Association

Висновок

Стандарт 802.11i. WEP у даний час може застосовуватися тільки в освітніх цілях – для демонстрації уразливостей цього протоколу. Однак практичні дослідження показують, що велика кількість мереж все ще покладаються на цей беззахисний протокол захисту. Недоліків у забезпеченні цілісності та конфіденційності даних, що циркулюють у мережі, не позбавлений

і WiMAX, проте більшість із них сьогодні знаходять рішення або з використанням нових алгоритмів шифрування і нового обладнання. Дослідження систем безпеки в бездротових мережах не вичерпані та потребують удосконалення.

Література

1. Ільченко, М. Ю. Сучасні телекомунікаційні системи / М. Ю. Ільченко, С. О. Кравчук.— К.: Наук. думка, 2017.— 328 с.

2. Теорія і практика управління використанням радіочастот□ного ресурсу: навч. посібник / [П. В. Слободянюк, В. Г. Сайко, Т. М. Наритник, В. Г. Благодарний].— К.: ДУІКТ, 2018.— 596 с.

3. Fazel, K. Multi-carrier and spread spectrum systems: from OFDM and MC-CDMA to LTE and WiMAX / K. Fazel, S. Kaiser.— 2nd ed., 2020.

4. Беркман, Л. Н. Багатоканальні модеми: монографія / [Л. Н. Беркман, І. С. Щербина, О. І. Чумак, Л. В. Рудик]; за наук. ред. С. Є. Захаренка.— К.: Зв'язок, 2014.— 149 с

УДК 004.8

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ТА ТЕХНОЛОГІЯХ

Корягіна Дар'я Олександрівна

Київський національний економічний університет імені Вадима Гетьмана

Штучний інтелект (ШІ) - це сукупність алгоритмів та технологій, що дозволяють комп'ютерам самостійно навчатися та приймати рішення на основі аналізу великих обсягів даних. У 2020-2022 роках ШІ став все більш популярним та використовується в різних галузях, зокрема в інформаційних системах та технологіях. У даному науковому дослідженні розглянуті переваги та недоліки використання ШІ та особливості його використання у галузях вітчизняної економіки.

Однією з найбільш важливих галузей застосування ШІ є інформаційні системи (ІС). ШІ дозволяє створювати ІС, що можуть самостійно збирати, обробляти та аналізувати великі обсяги даних, що дозволяє значно покращити якість прийнятих рішень та оптимізувати роботу систем [1] .

Одним з прикладів використання ШІ в ІС є система управління виробництвом. Завдяки аналізу даних від сенсорів, ШІ може передбачити поломки обладнання та запобігти їм, що дозволяє підвищити ефективність виробництва та зменшити витрати .

Ще одним прикладом є ІС для фінансових установ, яка може аналізувати дані про транзакції та виявляти шахраїв та шахрайські схеми, що дозволяє зменшити кількість крадіжок та збільшити довіру до банківської системи [3].

ШІ також знаходить застосування в технологіях. Одним з найбільш відомих прикладів є голосові асистенти, такі як Siri від Apple, Alexa від Amazon та Google Assistant, що дозволяють користувачам взаємодіяти зі своїми пристроями за допомогою голосових команд.

Ще одним прикладом використання ШІ в технологіях є автономні автомобілі. Системи ШІ дозволяють автомобілям самостійно приймати рішення та реагувати на змінні умови дорожнього руху, що зменшує кількість аварій та підвищує безпеку на дорозі [2].

Так як ШІ використовують вже у багатьох компаній, можна виділити низку переваг його використання. Зокрема:

- Збільшення продуктивності. AI системи можуть автоматизувати рутинні завдання, такі як редагування зображень або відео, дозволяючи працівникам зосередитися на більш стратегічній роботі.

- Персоналізований досвід клієнтів. Алгоритми штучного інтелекту можуть використовуватися для персоналізації контенту для клієнтів. Наприклад, індивідуальні рекомендації продуктів, що призводить до покращення залученості клієнтів і збільшення продажів.
- Підвищення креативності. AI рішення підсилюють креативність, надаючи нові інструменти та методи для дослідження та експериментів художникам, дизайнерам і письменникам.
- Зменшення витрат. Технології на базі генеративного штучного інтелекту знижують витрати, автоматизуючи завдання та оптимізуючи робочі процеси.
- Покращений досвід користувачів. Використання генеративного штучного інтелекту допомагає підприємствам створювати персоналізований контент і досвід, який відповідає потребам клієнтів. Це призводить до збільшення лояльності та задоволення клієнтів.
- Підвищена масштабованість. Генеративний штучний інтелект дозволяє масштабувати виробництво контенту відповідно до попиту, дозволяючи підприємствам швидко та економічно вигідно виробляти великі обсяги високоякісного контенту.
- Вища конкурентоспроможність. Системи з генеративним штучним інтелектом забезпечують конкурентну перевагу, дозволяючи підприємствам створювати унікальний та оригінальний контент, який виділяє їх серед конкурентів.

Одним з найбільших недоліків використання ШІ є можливість зловживання та порушення приватності. Наприклад, системи відеоспостереження, що використовують ШІ для розпізнавання обличь, можуть порушувати приватність людей та збирати їхні дані без їхньої згоди [4].

Крім того, системи ШІ можуть бути не досконалими та допускати помилки, що може призвести до серйозних наслідків. Наприклад, система ШІ для виявлення раку на зображеннях мамографії може неправильно діагностувати хворобу, що може призвести до затримки в лікуванні та погіршення стану пацієнта.

Штучний інтелект став все більш популярним та використовується в різних галузях, зокрема в інформаційних системах та технологіях. Використання ШІ дозволяє покращити якість прийнятих рішень та оптимізувати роботу систем. Однак, використання ШІ може також призвести до порушення приватності та допущення помилок. Для успішного використання ШІ в інформаційних системах та технологіях необхідно бути уважними та здійснювати додаткові заходи для захисту приватності та запобігання помилкам.

Загалом, використання ШІ у сфері інформаційних систем та технологій є великим кроком вперед у розвитку цих галузей. Використання ШІ дозволяє підвищувати продуктивність та ефективність роботи систем, що призводить до покращення якості послуг та задоволеності користувачів. Однак, необхідно пам'ятати про можливі негативні наслідки використання ШІ та дотримуватись відповідних заходів для їх запобігання.

Список використаних джерел:

1. "Artificial Intelligence and Machine Learning." The National Institute of Standards and Technology (NIST), 20 January 2021.URL: https://www.nist.gov/artificial-intelligence
2. "Artificial Intelligence and the Future of Autonomous Vehicles." TechEmergence, 11 June 2021. URL: https://www.techemergence.com/artificial-intelligence-autonomous-vehicles-future/
3. "Artificial Intelligence in Banking: Transforming Financial Services." Emerj, 29 September 2020. URL:https://www.academia.edu/74719782/Banking_on_AI_mandating_a_proactive_approach_to_AI_regulation_in_the_financial_sector

4. United Nations. The Role of Artificial Intelligence in Achieving the Sustainable Development Goals. (2019)
URL: https://www.itu.int/en/ITU-T/climatechange/resources/Pages/topic-003.aspx

МЕТОДИ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ

Ігнатенко Анастасія Сергіївна
Державний університет телекомунікацій
м. Київ

Беручи до уваги значну інформатизацію суспільства, необхідність у мобільності користувачів мережі Інтернет, на сьогодні, все більшої популярності набувають бездротові мережі. На разі розвиток бездротових мереж дає змогу встановлювати з'єднання такої ж якості, як і мережі з використанням фізичного середовища передачі даних, але кількість користувачів в рази більша, ніж раніше. Але зі збільшенням кількості користувачів зростає необхідність захисту переданої інформації в таких типах мереж, тобто використання методів та механізмів шифрування та захисту даних. Так як на сьогоднішній день загрози інформаційним ресурсам є значними та катастрофічними. Тому дослідження методів захисту бездротових мереж та підвищення ефективності даних механізмів є актуальним.

Щоб проводити дослідження, доцільно проаналізувати можливі загрози та визначити наслідки їх впливу та проаналізувати методи захисту від них.

Базовим стандартом, який визначає набір протоколів для передачі даних в бездротових мережах є IEEE 802.11. Цей стандарт постійно доповнюється та оновлюється, таким чином його нові версії були опубліковані в 1999, 2007, 2012 роках, а також наступна очікується ще в 2016 році.

Існує декілька методів захисту бездротових мереж, а саме основні та допоміжні.

Використання шифрування даних є одним з найефективніших методів захисту бездротових мереж. Воно дозволяє зашифрувати передачу інформації між пристроями, забезпечуючи конфіденційність даних.

Існує кілька протоколів безпеки для бездротових мереж, таких як WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) і WPA2 (Wi-Fi Protected Access II). Вони забезпечують аутентифікацію та шифрування даних, зменшуючи ризик несанкціонованого доступу до мережі.

Найкращим вирішенням проблем безпеки мережі є реалізація протоколу WPA2. Поряд з тим доповненням до основних рекомендацій можуть бути такі:

– Вимкнення мовчки ідентифікатора мережі (SSID) може забезпечити додатковий рівень захисту. Це робить мережу менш помітною для потенційних зловмисників, оскільки її ім'я не відображатиметься у списку доступних мереж.

– Важливо встановити сильний пароль на бездротовий маршрутизатор для обмеження доступу до мережі. Рекомендується використовувати комбінацію букв, цифр і символів та регулярно змінювати пароль.

– Мережеві брандмауери можуть фільтрувати трафік і блокувати несанкціонований доступ до мережі. Вони можуть виявляти та блокувати спроби зламати мережу, забезпечуючи додатковий рівень захисту.

– Важливо регулярно оновлювати програмне забезпечення бездротових пристроїв і маршрутизаторів. Це дозволяє виправити вразливості та уразливі пункти безпеки, які можуть бути використані зловмисниками для несанкціонованого доступу до мережі.

– MAC-фільтрація дозволяє обмежити доступ до бездротової мережі, дозволяючи лише підключення пристроїв з визначеними MAC-адресами. Це додатково ускладнює несанкціонований доступ до мережі.

Засновуючись на наведеному про методи захисту бездротових мереж, можна зробити висновки. Безпека бездротових мереж вимагає комплексного підходу. Використання одного методу захисту може бути недостатнім, тому рекомендується комбінувати кілька методів для забезпечення максимального рівня безпеки. Ефективна захист бездротових мереж вимагає постійного вдосконалення та відстеження нових загроз. Технології та методи зламу безпеки постійно розвиваються, тому важливо слідкувати за оновленнями та застосовувати найсучасніші методи захисту. Важливо враховувати індивідуальні потреби та вимоги при виборі методів захисту бездротових мереж. Різні типи мереж (домашні, корпоративні, громадські) вимагають різних рівнів захисту, тому необхідно адаптувати методи захисту під конкретні потреби і ситуації.

Загалом, забезпечення безпеки бездротових мереж є постійним процесом, який вимагає поєднання технічних, організаційних та свідомих підходів. Шлях до надійної бездротової мережі полягає в усвідомленні загроз, використанні надійних методів захисту та постійному підвищенні рівня безпеки.

ТРАНСФОРМАЦІЯ ТЕЛЕКОМУНІКАЦІЙНОГО СЕКТОРУ В ЕПОХУ ЦИФРОВОЇ КОМУНІКАЦІЇ

Сюрвасєв Владислав Валерійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

1. Теза: "Розширення бездротових технологій сприяє мобільності та підвищує доступність телекомунікаційних послуг".

Розвиток бездротових технологій, таких як мобільний зв'язок і Wi-Fi, відіграє ключову роль у зміні телекомунікаційного сектору. Ці технології дають користувачам можливість залишатися підключеними та отримувати доступ до телекомунікаційних послуг незалежно від їх місця перебування. Одним з головних переваг бездротових технологій є мобільність. Завдяки їм, ми можемо мати доступ до інтернету та телекомунікаційних послуг на руху, незалежно від обмежень проводових підключень. Це дозволяє нам комунікувати, обмінюватися інформацією та користуватися послугами там, де це зручно для нас, будь то у місті, в селі або навіть під час подорожей.

Розширення бездротових технологій також сприяє підвищенню доступності телекомунікаційних послуг. Раніше, у віддалених районах або місцях з обмеженим проводовим покриттям, доступ до швидкого та стабільного Інтернету та зв'язку був обмежений. Однак, завдяки розширенню бездротових мереж, ці області тепер можуть отримати доступ до телекомунікаційних послуг і вигоди цифрового світу. Бездротові технології також грають важливу роль у забезпеченні підключення в екстремальних умовах, таких як надзвичайні ситуації чи віддалені регіони, де проводове покриття може бути недоступним або пошкодженим. В цих випадках бездротовий зв'язок може забезпечити зв'язок та допомогти з координацією дій для надання допомоги та забезпечення безпеки.

Таким чином, розширення бездротових технологій сприяє мобільності та підвищує доступність телекомунікаційних послуг, роблячи їх доступними в будь-який час і в будь-якому місці. Це відкриває нові можливості для спілкування, розвитку бізнесу та поліпшення якості життя.

2. Теза: "Швидкість передачі даних та пропускна здатність мереж стають все важливішими у цифровому суспільстві".

У цифровому суспільстві, яке характеризується постійним зростанням обсягу та складності передаваної інформації, швидкість передачі даних та пропускна здатність мереж стають все важливішими факторами. Це обумовлено зростаючою потребою у швидкому та

безперервному доступі до інформації, великому обсягу передаваних даних, а також розвитком інтерактивних сервісів, які вимагають широкополосного з'єднання. Забезпечення високої швидкості передачі даних є ключовим для ефективної комунікації, спільної роботи, стрімінгу мультимедійного контенту та розробки нових сервісів. Швидкі телекомунікаційні мережі дозволяють користувачам швидко обмінюватися інформацією, переглядати відео високої якості, користуватися хмарними сервісами та використовувати передові технології, такі як віртуальна реальність і штучний інтелект.

Проблемою в цьому контексті є те, що зростання вимог до швидкості передачі даних нерідко перевищує можливості існуючих телекомунікаційних інфраструктур. Це створює потребу у постійному розвитку та модернізації мереж, впровадженні нових технологій (наприклад, 5G), а також вирішенні питань ефективного управління смугою пропускання. Забезпечення високої швидкості передачі даних та великої пропускної здатності мереж стає важливим завданням для забезпечення ефективної цифрової комунікації та розвитку сучасного суспільства.

3. Теза: "Технології Internet of Things (IoT) відкривають нові можливості для підключення різних пристроїв до мережі телекомунікацій".

Технології Internet of Things (IoT) представляють собою систему, в якій різні фізичні пристрої, обладнані сенсорами та здатні до збору та обміну даними, підключаються до мережі телекомунікацій. Це відкриває широкі перспективи для розвитку телекомунікаційного сектору. За допомогою IoT, пристрої можуть взаємодіяти між собою та обмінюватися даними в реальному часі. Наприклад, розумні прилади вдома, автомобілі з підключенням до Інтернету, медичні пристрої та інші розумні пристрої можуть передавати інформацію про свій стан, виконувати взаємодію з користувачами та надавати нові сервіси.

Це має велике значення для розвитку індустрії, містобудування, охорони здоров'я та багатьох інших сфер. Наприклад, в індустрії IoT дозволяє впроваджувати системи моніторингу та управління, що підвищує ефективність виробничих процесів. У містобудуванні IoT допомагає впроваджувати розумні системи управління освітленням, транспортним рухом та інфраструктурою. У галузі охорони здоров'я IoT може забезпечувати моніторинг пацієнтів, надавати телемедицинські послуги та покращувати діагностику та лікування.

Проте, разом зі зростанням IoT постають і проблеми, такі як забезпечення безпеки та конфіденційності даних, сумісність між пристроями та стандартами, а також вирішення питань енергоефективності та життєвого циклу пристроїв. Вирішення цих проблем стає важливим завданням для подальшого розвитку IoT та телекомунікаційного сектору.

РОЗРОБКА СИСТЕМИ БЕЗПЕКИ ВЕБ-САЙТУ З ПРОДАЖУ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ: ЗАХИСТ ВІД КІБЕРАТАК ТА ВИКРАДЕННЯ ДАНИХ

Сергієнко Роман Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

В часи високого рівня розвитку інтернет мереж, створення та розробка мережевого веб ресурсу є необхідністю для будь-якого бізнесу, в тому числі для постачальників телекомунікаційного обладнання. Однак, лише наявності зручного та конкурентного ресурсу не достатньо. У сучасному світі, тим паче в реаліях війни, коли на велику кількість економічно, культурно та системно важливих українських ресурсів щоденно здійснюються кібератаки – важливим стає забезпечення безпеки ресурсу.

Загалом, кібератаки використовують 2 типи вразливостей: людський фактор та вразливості програмно-апаратних потужностей. Найбільш поширеними видами атак є: 1. DoS або DDoS атаки: ці атаки спрямовані на перевантаження сервера, щоб заборонити користувачам отримувати доступ до веб-сайту. У DoS (Denial of Service) атаки використовується лише один комп'ютер, тоді як у DDoS (Distributed Denial of Service) атаки використовується багато комп'ютерів, які є частиною ботнету (мережі заражених вірусом комп'ютерів). 2. Фішинг: ці атаки спрямовані на отримання конфіденційної інформації від користувачів, наприклад, їх логінів і паролів, шляхом створення фальшивих веб-сайтів, які схожі на оригінальні. 3. SQL-ін'єкції: ці атаки використовуються для зламування баз даних веб-сайту, щоб здобути конфіденційну інформацію. 4. Крадіжка ідентифікаторів сесій: ці атаки спрямовані на крадіжку унікального коду, що генерується веб-додатком та використовується для ідентифікації користувача під час сеансу роботи з додатком, щоб мати доступ до облікових записів користувачів. 5. Malware (віруси) - шкідливі програми, які можуть бути використані для отримання доступу до системи та викрадення конфіденційної інформації [1].

Частину захисту програмно-апаратних потужностей веб-ресурсу можуть взяти на себе послуги хостинг-компаній, що надають обчислювальні потужності, котрими зазвичай послуговуються при розробці веб-сайту. Це дозволяє зменшити витрати на обладнання та захист на апаратному та мережевому рівні (охорона об'єкту та фільтрація трафіку через фаєрвол, системи проникнення IDS/IPS для виявлення фактів проникнення в мережу). Важливо також потурбуватися про програмну безпеку веб-сервера, який використовується для розміщення сайту, в інтернеті, навіть якщо він орендований у хостинг-провайдера. Для цього слід встановити необхідне програмне забезпечення для захисту та налаштувати його згідно з рекомендаціями виробника, проводити регулярні оновлення та аудит безпеки. Хорошою практикою є використання методології ризик-менеджменту, моніторингу роботи системи, що дозволяє ідентифікувати потенційні ризики чи спроби атак та визначати шляхи їх запобігання. Щодо вирішення проблем з перехопленням даних користувачів, необхідно забезпечити шифрування даних, що передаються, та їх цілісність. Для цього необхідно використовувати мережеві протоколи, що передають дані виключно у зашифрованому вигляді. Для поліпшення рівня безпеки, відмово стійкості, швидкодії ресурсу та шифрування можливо делегувати роботу, використовуючи послуги «DNS захисту» у таких компаній як "Cloudflare". Даний захист є «додатковим фільтром» перед веб-ресурсом завдяки великій кількості серверів по всьому світу, які розташовані ближче до потенційних користувачів та зберігають DNS-запити й перенаправляють трафік в разі необхідності, та моніторингу трафіку, за допомогою чого DoS або DDoS атаки, перехоплення даних чи пере направлення запитів на сервер зловмисника стають вкрай складними та невигідними [2].

Розглядаючи загрози, пов'язані з людським фактором, необхідно підтримувати високий рівень знать про кібербезпеку та інформаційну гігієну у працівників, надавати мінімально необхідний, обмежений доступ до роботи з даними. Також важливо допомагати користувачам у безпечному користуванні ресурсом: хорошою практикою є нагадування користувачеві про перевірку правильності адреси сайту в адресному рядку, щоб убезпечитись від знаходження на «фальшивому сайті», котрий шахраї можуть скопіювати з цільового у найменших деталях та вкрасти дані. Необхідно поставити вимоги до створення та використання облікових записів користувача, наприклад, вимоги до складності паролів та двофакторну автентифікацію (з використанням смс-повідомлення чи електронного листа) з кодом доступу обмеженого часу дії, котрий необхідно вводити разом з паролем.

Використовуючи дані методики захисту мережевого ресурсу, продаж телекомунікаційного обладнання стає безпечнішим для обох сторін – замовника та продавця. Додатково, якщо хостингова компанія не надає за умовами договору автоматичне резервне

копіювання даних чи використовуються власні потужності – регулярне примусове резервне копіювання допоможе не хвилюватися за дані навіть в разі виходу обладнання з ладу.

Список використаних джерел:

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— Київ: ДУТ, 2015.— 288 с.
2. Посібник з налаштування Cloudflare [Електронний ресурс] // Hostiq. – 2022. – Режим доступу до ресурсу: https://hostiq.ua/wiki/ukr/dns-hosting-cloudflare/.

ТЕХНІЧНІ АСПЕКТИ ПОБУДОВИ МЕРЕЖІ ДОСТУПУ НА ОСНОВІ ТЕХНОЛОГІЙ 5G

Швець Валерія Валеріївна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

5G – стандарт п'ятого покоління мобільної мережі, на основі стандартів 5G/IMT-2020 для радіо інтерфейсів в області телекомунікацій, наступник 4G мережі. Технологія стільникової мережі, в якій зона обслуговування поділяється на невеликі географічні райони – стільники або соти. Всі безпровідні пристрої 5G в соті підключені до мережі Інтернет і мобільного зв'язку за допомогою радіохвиль, через локальну антену. Основною перевагою нової мережі є те, що вона має більшу пропускну здатність, забезпечуючи таким чином більш високу швидкість завантаження, з часом, планується збільшення швидкості до 20 Гбіт\с.

Технологія 5G відкриває нові можливості для створення мережі доступу з високою швидкістю передачі даних та мінімальним часом затримки. Побудова мережі на основі 5G передбачає використання ряду нових технологій, таких як масивні мімо-системи, віртуалізація мережі та хмарні технології.

Архітектура технології 5G представляє значні переваги за технологію 4G LTE (long-term evolution), яка з’явилась слідом за 3G і 2G. Завжди існує період часу, протягом якого існує кілька поколінь мережі одночасно. Як і його попередники, 5G має співіснувати з попередніми мережами з двох важливих причин:

1. Розробка та розгортання нових мережевих технологій потребує величезної кількості часу, інвестицій і співпраці основних організацій і операторів.
2. Перші користувачі завжди бажають отримати нові технології якнайшвидше, тоді як ті, хто зробив значні інвестиції у великі розгортання існуючих мережевих технологій, таких як 2G, 3G і 4G LTE, хочуть скористатися ними якомога довше, і, звичайно, поки нова мережа не стане повністю життєздатною.

Мережна архітектура мобільної технології 5g значно вдосконалена в порівнянні з минулими архітектурами. Великі мережі з щільністю стільникового зв’язку забезпечують величезні стрибки продуктивності. Крім того, архітектура мереж 5G забезпечує кращий рівень безпеки порівняно з сучасними мережами 4G LTE.

Підсумовуючи, технологія 5G пропонує три основні переваги:

- Більш висока швидкість передачі даних.
- Більша ємність, що забезпечує величезну кількість пристроїв підключених до Інтернету на квадратний кілометр.
- Менша затримка, аж до однозначних мілісекунд, що є критично важливим у таких додатках, до як підключені транспортні засоби та автономні транспортні засоби, де необхідна майже миттєва відповідь. [2]

Технічна архітектура мережі 5G складається з таких головних компонентів: мережі радіодоступу (RAN) та Обчислення на межі мультидоступу (MEC). Мережа доступу є

ключовою складовою мережі 5G, оскільки вона забезпечує бездротове з'єднання між мобільними пристроями та базовими станціями (BS), які підключені до ядрової мережі.

5G створює динамічну, узгоджену та гнучку структуру передових технологій для підтримки різноманітних програм. 5G використовує більш інтелектуальну архітектуру з мережами радіодоступу (RAN), які більше не обмежені близькістю базових станцій або складною інфраструктурою. 5G прокладає шлях до дезагрегованої, гнучкої та віртуальної RAN з новими інтерфейсами, які створюють додаткові точки доступу до даних.

Multi-Access Edge Computing (MEC) є важливим елементом архітектури 5G. MEC — це відгалуження хмарних обчислень, яке переносить програми з централізованих центрів обробки даних на край мережі, ближче до кінцевих користувачів та їхніх пристроїв. По суті, це створює ярлик у доставці вмісту між користувачем і хостом, минаючи міжміський мережевий шлях, який колись розділяв їх. Ця технологія не є ексклюзивною для 5G, але, безумовно, є невід'ємною частиною її ефективності.

- Характеристики MEC включають низьку затримку, високу пропускну здатність і доступ до інформації RAN у реальному часі, що відрізняє архітектуру 5G від її попередників.
- Мережі 5G на основі специфікацій 3GPP 5G є ідеальним середовищем для розгортання MEC. Ці специфікації визначають механізми периферійних обчислень, що дозволяє MEC і 5G спільно маршрутизувати трафік.
- Розподіл обчислювальної потужності забезпечує великий обсяг підключених пристроїв, властивих розгортанню 5G та Інтернету речей (IoT), на додаток до переваг затримки та пропускної здатності.
- Конвергенція RAN і базових мереж вимагатиме від операторів використання нових

Технологія 5G створює нові можливості для швидкого та надійного бездротового зв'язку на великій території з високою мобільністю. Це означає, що технічна архітектура мережі 5G повинна бути розроблена з урахуванням високої пропускної здатності, низької затримки, високої мобільності та різноманітних вимог до ресурсів. [1]

Таким чином, побудова мережі доступу на основі технології 5G є складним завданням, яке вимагає використання нових технологій та розробки ефективних рішень для вирішення викликів, пов'язаних з ємністю, безпекою та ефективністю мережі. Однак, з використанням нових технологій, мережа 5G може стати потужним інструментом для забезпечення швидкого та надійного зв'язку у майбутньому.

Список використаних джерел:

1. What is 5G Architecture? [Електронний ресурс] – Режим доступу: https://www.viavisolutions.com/en-us/what-5g-architecture

2. What Is 5G Network Architecture? [Електронний ресурс] – Режим доступу: https://www.digi.com/blog/post/5g-network-architecture

ПЕРЕВАГИ ВИКОРИСТАННЯ СИСТЕМ ВІДДАЛЕНОГО ДОСТУПУ ТА МОНІТОРИНГУ У МЕДИЦИНІ

Щеглова Олена Андріївна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Remote Patient Monitoring (RPM) – це система віддаленого доступу та моніторингу, яка дозволяє медичним працівникам відстежувати початок захворювання та прогресування

симптомів, дистанційно спілкуватися з пацієнтами, щоб змінити плани догляду та надати навчання самообслуговуванню на основі змін у стані хворого.

Рішення RPM обіцяють зіграти вирішальну роль у полегшенні лікування хронічних захворювань, які зростають у Європі та створюють навантаження на системи охорони здоров'я. Крім того, рішення RPM можуть бути потенційно використовуватися для підтримки діагностики та скринінгу. Що наштовхує на думку про доцільність використання даного рішення.

Вперше це було обговорено на початку COVID-19, адже через стрімкий розвиток хвороби чисельність хворих зростала у геометричній прогресії. Країна за країною зіштовхувалися з проблемою у неспроможності забезпечити належний догляд за хворими. Через високі ризики зараження традиційні методи лікування довелося оновити. Так зустрічі віч-на-віч було замінено на відеоконференції, що економило час та не шкодило здоров'ю.

Наразі рішення RPM можуть принести такі переваги пацієнтам:

- Забезпечення своєчасного втручання.

Віддалений моніторинг забезпечує більш простий обмін інформацією між пацієнтами та медичними працівниками, що призводить до більш ретельного спостереження за станом пацієнта, а також помічалися більш точні та своєчасні клінічні та технічні втручання. Таким чином, прискорюючи втручання, рішення RPM можуть сприяти кращим результатам для пацієнтів, включаючи якість життя, шляхом запобігання погіршенню стану їхнього здоров'я. Це особливо актуально для хронічних захворювань, адже як виявили спеціалісти: достатньо лише декілька основних вимірювань, тобто конкретних параметрів здоров'я, і постійний моніторинг стану здоров'я аби запобігти погіршення стану або навіть летальні випадки.

- Збільшення обізнаних пацієнтів.

За дослідженням кількість прихильників до самоконтролю та своєчасного лікуванню лише збільшилася з моменту використання системи RPM.

- Покращення доступу до медичної допомоги.

Сама система доступна через мобільний додаток, що дозволяє пацієнтам записуватися на прийоми, своєчасно приймати ліки або відслідковувати стан здоров'я не виходячи з дому. Особливо це стало у нагоді для таких груп населення, які стикаються з обмеженнями у доступі медичних центрів через географічну відстань, вік, фізичний стан або часові обмеження. Окрім пандемії, дослідження 2014 року показало, що активація протоколу RPM, який запровадив онлайн консультації та спостереження у медичних працівників, скоротило транспортування швидкої допомоги на 56%.

- Зменшення витрат на медичні послуги.

При своєчасному втручанню, можна виявити зародки хвороб, аби після прийняти необхідні заходи для їх попередження та лікування.

- Автоматизовані повідомлення для хронічних захворювань.

Завдяки RPM, при виявленні будь-яких аномалій у показниках здоров'я, система негайно надсилає сигнали тривоги медичному персоналу. Це дозволяє спеціалістам швидко реагувати та вживати необхідні заходи для зупинки подальшого розвитку хвороби або уникнення серйозних ускладнень.

Наприклад, якщо RPM виявляє відхилення у серцевому ритмі пацієнта, які можуть свідчити про можливий інфаркт, система негайно повідомляє про це медичний персонал. Лікар може швидко зв'язатися з пацієнтом, надати рекомендації та навіть надіслати швидку допомогу на місце. Таким чином, RPM допомагає запобігти летальному розвитку хвороби та забезпечує негайне лікування, що може врятувати життя пацієнта.

Крім того, система також надсилає сповіщення пацієнту про будь-яке погіршення його стану. Це дає можливість пацієнту вчасно звернутися до лікаря або дотримуватися рекомендацій, що зменшує ризик ускладнень і покращує результати лікування.

Загальні висновки про використання технології віддаленого моніторингу пацієнтів (RPM) полягають у покращенні якості та ефективності медичної допомоги завдяки постійному моніторингу показників здоров'я, ранньому виявленню змін у стані пацієнта та негайній реакції медичного персоналу. Використання RPM сприяє покращенню результатів лікування, зниженню витрат на охорону здоров'я та забезпеченню зручності та комфорту для пацієнтів, забезпечуючи зародження хвороб, своєчасне лікування та запобігання ускладнень.

АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ВИМІРЮВАННЯ МАГНІТНОЇ ТА ДІЕЛЕКТРИЧНОЇ ПРОНИКНОСТЕЙ МАТЕРІАЛІВ

Дмитраков Тарас Сергійович
Державний університет телекомунікацій

Аналіз існуючих методів вимірювання магнітної та діелектричної проникнень матеріалів може бути досить широким, після чого існує багато різних методик і технік для визначення цих фізичних параметрів. Нижче наведено огляд деяких з них:

Магнітна проникність:

1. Метод магнітного відвідування (вимірювання магнітної проникності): Цей метод виконується у вимірюванні магнітної індукції в матеріалі при певному магнітному полі. З використанням цих даних можна застосувати магнітну проникність матеріалу.
2. Метод тороїдальних ядресонансів (toroidal core resonator method): Цей метод вимірює зміну індуктивності тороїдального ядра при прикладанні магнітного поля. За допомогою цих даних можна розмістити магнітну проникність матеріалу.

Діелектрична проникність:

1. Метод капсульного резонатора (cavity resonator method): Цей метод вимірює зміну резонансної частоти капсульного резонатора при введеній діелектриці. За допомогою цих даних можна налаштувати матеріал діелектричної проникності.
2. Метод вимірювання мікрохвильової перетини (вимірювання мікрохвильової передачі): Цей метод вимірює зміну передавальної здатності мікрохвильової хвилі при проходженні через діелектричний зразок. За допомогою цих даних можна налаштувати матеріал діелектричної проникності.

Варто зауважити, що існує багато інших методів вимірювання магнітної та діелектричної проникнень матеріалів, таких як методи на основі використання світла, акустичні методи, методи на основі магнітного резонансу тощо. Кожен метод має свої переваги, обмеження і особливості застосування, і вибір конкретного методу залежить від властивостей матеріалу, точності, доступності обладнання та інших факторів.

ОСНОВНІ ПЕРЕВАГИ ТА ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ВОЛОКОННО-ОПТИЧНИХ СИСТЕМ ПЕРЕДАЧІ

Герасименко-Вакуленко Н.О.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м.Київ

Оптичне волокно в даний час вважається найдосконалішою фізичним середовищем для передачі інформації, а також самої перспективним середовищем для передачі великих потоків інформації на значні відстані. Сьогодні волоконна оптика застосовується практично у всіх сферах, пов'язаних з передачею інформації. Стало допустимим підключення робочих станцій до інформаційної мережі з використанням волоконно-оптичного кабелю.

У нинішній час перевага для організації зв'язку по волоконно-оптичним лініям, надаються цифровим системам передачі (ЦСП). Це зумовлено не тільки загальними перевагами ЦСП у порівнянні з аналоговими системами передачі (АСП), але й особливостями роботи та побудови волоконно-оптичних систем передачі (ВОСП).

Розглянемо основні особливості. Для одержання необхідної якості передачі інформації в АСП потрібні спеціальні засоби приймання та обробки оптичних сигналів. ЦСП забезпечують необхідну якість передачі інформації при відношенні сигнал/шум на 30-40 дБ менше, ніж АСП. Тому реалізація ВОСП з використанням ЦСП значно простіша у порівнянні з АСП. Переваги ЦСП: висока завадозахищеність, стійкість до нелінійних спотворень, незалежність якості передачі від довжини лінії зв'язку, стабільність параметрів каналу зв'язку та інші.

Розглянемо головні елементи організації ВОСП. Як і системи, що використовують традиційні кабелі з мідними провідниками, волоконно-оптичні системи передачі є проводовими, бо сигнали оптичного діапазону передаються по направляючій системі – волоконним світловодам. Тільки середовище передачі та форма сигналів в лінії ВОСП відрізняють від традиційних проводових ліній передачі. Тому побудова ВОСП аналогічна побудові будь-якої проводової багатоканальної системи передачі, в складі якої є кінцеві та проміжні станції, з'єднанні безперервною направляючою системою. На (рисунку 1.1) наведена узагальнена структура ВОСП (для одного напрямку передачі).

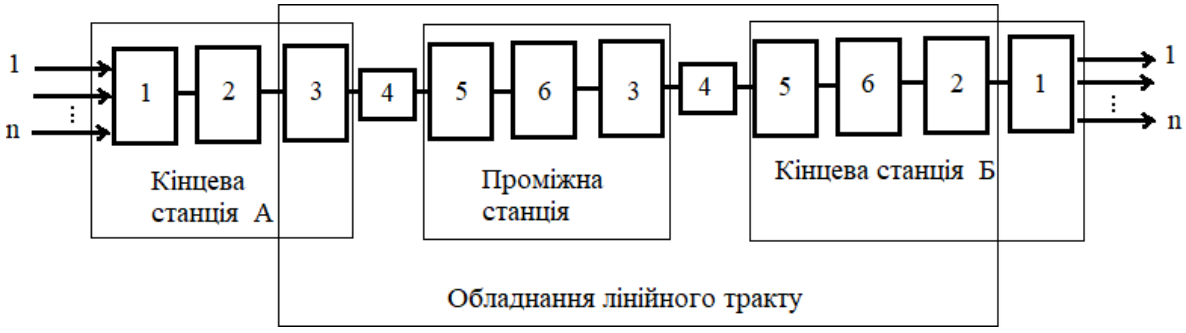


Рисунок 1.1 Узагальнена структура схема ВОСП (для одного напряму передачі)

1. Типова кінцева апаратура багатоканальної схеми передачі;
2. Апаратура спряження;
3. Передавальний оптоелектронний модуль (ПрОМ);
4. Оптичний кабель;
5. Приймальний оптоелектронний модуль(ПОМ);
6. Електронний генератор.

На передавальній кінцевій станції А первинні сигнали тональної частоти (ТЧ) надходять на кінцевій тональну апаратуру, де об'єднуються в груповий сигнал, що подається на апаратуру спряження.

В ній електронний сигнал перетворюється у форму, необхідну для передачі по волоконно-оптичному лінійному тракту, тобто формується лінійний сигнал. Після цього в ПОМ здійснюється модуляція потужності несучої лінійним електричним сигналом і оптичний сигнал надходить в ОК. При розповсюдженні по кабелю оптичний сигнал послаблюється і спотворюється. Для збільшення дальності зв'язку через певні відстані вздовж лінії встановлюються проміжні станції (регенератори), що відновлюють форму сигналу і компенсують загасання (послаблення) в лінії.

В сучасних ВОСП у регенераторі проводиться обробка (підсилення, корекція, регенерація) електричного сигналу.

Тому на проміжній станції електричний сигнал на вході перетворюється в електричний, зворотнє перетворення відбувається на виході. Ці перетворення здійснюються в ПрОМ та ПОМ відповідно.

Проводяться розробки оптичних регенераторів на основі лазерних підсилювачів та оптичних транзисторів, в яких будуть відсутні проміжні перетворення оптичних сигналів в електричні та навпаки.

На приймальній кінцевій станції Б здійснюється перетворення оптичного сигналу в електричний, його регенерація, підсилення, відновлення до вигляду первинного сигналу на вході кінцевої станції А.

Відмінність ВОСП від традиційних проводових систем передачі, яка випливає з розглянутої структурованої схеми, полягає у тому, що інформація передається за допомогою оптичних сигналів, що супроводжується встановленням спеціальних додаткових приладів (ПОМ та ПрОМ на кінцевих та проміжних станціях і апаратури спряження на кінцевих станціях).

Сучасні ВОСП являють собою поєднання оптичного лінійного тракту, який містить ПОМ, ПрОМ, ОК з уніфікованою каналоутворюючою апаратурою та апаратурою групоутворення ЦСП різних ступенів ієрархії.

Тому вони мають уніфіковані параметри стику, що дозволяє легко організувати лінії передачі з застосуванням інших середовищ розповсюдження.

Застосування ВОСП доцільно, економічно і ефективно на всіх ділянках Єдиної Національної мережі зв'язку України. Це не тільки підвищує техніко-економічні показники галузі зв'язку, але й забезпечує можливість поетапного переходу до цифрових мереж інтегрального обслуговування.

Список використаних джерел

1. Каток В.Б., Руденко І.Е., Ранський Є.Г., Однорог П.М. Волоконно-оптичний зв'язок : посіб. Київ : Логос 2015. 383 с.

2. Ковальчук В.К. Волоконно-оптичні системи передачі : навч. посіб. Харків : ХІРЕ 2000. 212 с.

3. Осадчук В.С., Осадчук О.В. Волоконно-оптичні системи передачі : навч. посіб. Вінниця : ВНТУ 2005. 225 с.

ДОСЛІДЖЕННЯ ТА АНАЛІЗ МЕТОДІВ ПОБУДОВИ СУЧАСНИХ VPN-МЕРЕЖ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ПРИВАТНОСТІ В КОМУНІКАЦІЙНИХ СИСТЕМАХ

Москаленко Данило Олексійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Забезпечення безпеки та приватності в комунікаційних системах стає все більш актуальним завданням у світі, де цифрові технології використовуються на всіх рівнях життя. З ростом кількості загроз та кібератак, потреба у надійних методах захисту даних та забезпечення конфіденційності стає необхідною. Одним з найефективніших засобів захисту є використання віртуальних приватних мереж (VPN), що дозволяють забезпечити безпеку та приватність комунікаційних систем.

Дослідження та аналіз методів побудови сучасних VPN-мереж вимагає уваги до різних аспектів, включаючи протоколи шифрування, аутентифікацію, маршрутизацію трафіку та управління ключами.[2] Одним з ключових аспектів є вибір протоколу шифрування. Наприклад, протоколи IPSec, SSL/TLS та OpenVPN є найпоширенішими протоколами шифрування, які забезпечують безпеку передачі даних у VPN-мережах.

Для забезпечення аутентифікації та контролю доступу до VPN-мереж використовуються різні методи, такі як шифрування паролями, сертифікатами або двофакторною аутентифікацією. Вибір правильного методу аутентифікації є важливим для забезпечення безпеки мережі та захисту від несанкціонованого доступу.Окрім цього, ефективна маршрутизація трафіку в VPN-мережах грає важливу роль у забезпеченні безпеки та ефективності комунікаційної системи. Вибір правильних алгоритмів маршрутизації, таких як статична маршрутизація, динамічна маршрутизація (наприклад, OSPF або BGP) чи комбінація обох, залежить від потреб користувачів та характеристик мережі. Управління ключами також є важливим аспектом побудови VPN-мережі. Ефективне та безпечне управління ключами дозволяє забезпечити конфіденційність та цілісність даних у мережі. Для цього використовуються різні протоколи обміну ключами, такі як IKE (Internet Key Exchange), які дозволяють сторонам установити безпечне з'єднання та обмінуватися ключами для шифрування.

Використання сучасних методів побудови VPN-мереж значно покращує безпеку та приватність в комунікаційних системах. За допомогою шифрування, аутентифікації та інших заходів захисту, VPN-мережі забезпечують захищену передачу даних, унеможливлюючи їх перехоплення або розкриття несанкціонованим особам.[1] Віртуальні приватні мережі також дозволяють користувачам маскувати свою реальну IP-адресу, що сприяє приватності та анонімності в мережі.

Дослідження та аналіз методів побудови сучасних VPN-мереж для забезпечення безпеки та приватності в комунікаційних системах показує, що вони є ефективним засобом захисту даних у сучасному цифровому світі. Вибір правильних протоколів шифрування, методів аутентифікації, алгоритмів маршрутизації та протоколів обміну ключами допомагає побудувати надійну та безпечну VPN-мережу. Використання віртуальних приватних мереж дозволяє забезпечити конфіденційність та цілісність даних, а також зберегти приватність користувачів у комунікаційних системах. Отже, розуміння та використання цих методів є важливими для будь-якої організації чи користувача, які прагнуть забезпечити безпеку та приватність своїх даних у цифровому світі.

Література

1. Deka, G. C. (2018). Virtual Private Networks: A Secure Connection to the Internet. CRC Press.
2. Patel, N. (2019). Virtual Private Networks (VPNs): Everything You Need to Know. Packt Publishing.

ПІДВИЩЕННЯ СТІЙКОСТІ СТЕГАНОГРАФІЧНОГО МЕТОДУ З КОДОВИМ УПРАВЛІННЯМ ВБУДОВУВАННЯМ ДОДАТКОВОЇ ІНФОРМАЦІЇ ДО АТАК ЗАШУМЛЕННЯМ

А.В. Соколов, Д.О. Гулід
Національний університет «Одеська політехніка»

Збільшення кількості мультимедійного контенту, що генерується та передається у сучасних інформаційно-телекомунікаційних системах призводить до зростаючої необхідності застосування стеганографічних методів при проектуванні та імплементації сучасних систем захисту інформації. До таких методів висуваються жорсткі критерії ефективності, які передбачають забезпечення їх достатньої пропускної спроможності, стійкості до атак проти вбудованого повідомлення, забезпечення надійності сприйняття, а також низької обчислювальної складності. Останнє є особливо важливим через повсюдне впровадження та застосування ресурсообмежених пристроїв, насамперед, мобільних пристроїв, пристроїв Internet of Things, пристроїв Internet of Battlefield Things тощо.

У роботі [3] представлено ідею забезпечення ефективності стеганографічних методів у просторовій області, яка отримала свій розвиток у роботі [1], де представлено стеганографічний метод з кодовим управлінням вбудовуванням додаткової інформації (ДІ), що передбачає адитивне вбудовування ДІ, яка зазнає попереднього кодування за допомогою кодових слів, що здійснюють цілеспрямований вплив на задану трансформанту перетворення Уолша-Адамара. Численні експерименти представлені в роботі [1] дозволили підтвердити значний рівень стійкості стеганографічного методу з кодовим управлінням вбудовуванням ДІ до різноманітних атак проти вбудованого повідомлення, зокрема, атак стисненням, зашумленням та розмиттям. Тим не менш, особливості забезпечення функціонування стеганографічного методу з кодовим управлінням вбудовуванням ДІ в умовах атак зашумленням потребують подальших досліджень.

Метою роботи є підвищення стійкості до атак зашумленням стеганографічного методу з кодовим управлінням вбудовуванням ДІ.

Незважаючи на те, що найбільш розповсюдженим видом атак проти вбудованого повідомлення в умовах функціонування сучасних інформаційних систем є атаки стисненням (наприклад, алгоритмом JPEG), атаки зашумленням із метою знищення вбудованої ДІ у стеганоповідомленні лишаються можливими і мають бути досліджені. У даній роботі розглядаються варіанти зашумлення стеганоповідомлення двома найбільш розповсюдженими видами шуму: адитивним білим гаусовим шумом (АБГШ) з математичним очікуванням $M[X]=0$ та дисперсією $D[X]$, а також шумом типу «Salt and Pepper» з дисперсією $D[X]$. Для кожного з зазначених видів шуму розроблені обґрунтовані рекомендації щодо вибору параметрів стеганографічного методу з кодовим управлінням вбудовуванням ДІ для забезпечення його ефективності в умовах атак зашумленням зазначеними видами шуму.

Розглянемо спочатку випадок АБГШ. Оскільки даний вид шуму характеризується рівномірною спектральною щільністю, обґрунтованим є висування гіпотези про те, що стійкість стеганографічного методу з кодовим управлінням вбудовуванням ДІ до атак зашумленням АБГШ не залежатиме від обраного кодового слова. Проведені масштабні експерименти для всіх кодових слів порядків $\mu=4,8,16$, що вибірково впливають на задану трансформанту перетворення Уолша-Адамара, тобто характеризуються елементарною структурою $\{\mu(1),0(\mu-1)\}$, на вибірці з 500 зображень з бази NRCS. Проведені дослідження дозволили встановити, що розкид значень відсотку помилок при атаці проти вбудованого повідомлення зашумленням АБГШ з різними значеннями дисперсії для різних кодових слів (за винятком кодового слова, що впливає на постійну складову) з елементарною структурою $\{\mu(1),0(\mu-1)\}$ становить: до 0.2% помилок для $\mu=4$, до 0.1% помилок для $\mu=8$ та до 0.3%

помилок для $\mu = 16$. При цьому, при застосуванні кодового слова, що впливає на постійну складову, відсоток помилок при декодуванні в умовах атаки зашумленням в середньому більший на 0.7% для $\mu = 4$, на 0.9% для $\mu = 8$ і на 1.9% для $\mu = 16$. Зростання стійкості стеганографічного методу з кодовим управлінням вбудовуванням ДІ спостерігалося лише при застосуванні багаторівневих кодових слів [2] при зростанні їх енергії E, інваріантно до трансформанти перетворення Уолша-Адамара, на яку вони здійснюють зосереджений вплив (за винятком постійної складової).

Таким чином, зважаючи на результати проведеного експерименту сформулюємо наступні рекомендації щодо застосування стеганографічного методу з кодовим управлінням вбудовуванням ДІ в умовах його застосування у каналах з атаками зашумленням АБГШ:

1. за аналогією із вибором сигнальних конструкцій для роботи у каналах зв'язку, що зашумлені АБГШ, більша стійкість стеганографічного методу до атак зашумленням проти вбудованого повідомлення може бути забезпечена через збільшення енергії E кодового слова шляхом застосування багаторівневих кодових слів;
2. задля забезпечення найбільшої надійності сприйняття стеганоповідомлення, зважаючи на рівний степінь стійкості кодових слів до атак зашумленням АБГШ (за винятком постійної складової), може бути рекомендоване застосування кодових слів, що впливають на найбільш високочастотні складові, наприклад, на трансформанту Уолша-Адамара (2,2). У разі застосування багаторівневих кодових слів вибір даної трансформанти для вбудовування ДІ також нівелює проблему знаходження максимальних за амплітудою елементів по краям кодового слова, що дозволить уникнути виникнення проблеми найбільшого перепаду яскравості на границях блоків та підвищити надійність сприйняття стеганоповідомлення.

У разі застосування стеганографічного методу з кодовим управлінням вбудовуванням ДІ у каналах із шумом типу «Salt and Pepper», зважаючи на природу та особливості даного шуму, рівень стійкості стеганоповідомлення до таких атак може бути підвищений за рахунок додавання операції обмеження амплітуди елементів матриць Δ_i на *Кроці 2* стеганографічного методу з кодовим управлінням вбудовуванням ДІ рівнем максимальної амплітуди кодового слова, яка для випадку бінарних кодових слів складає $\{\pm 1\}$. Зазначений спосіб вилучення ДІ побудований за аналогією з відомим методом ШОВ (BAN, широка полоса □ обмежувач □ вузька полоса), який є ефективним для боротьби із імпульсними завадами. Застосування обмеження по амплітуді матриць Δ_i перед їх подальшою обробкою дозволяє практично повністю позбутися помилок під час атак зашумленням із $PSNR \geq 8$дБ, таким чином підвищення стійкості стеганографічного методу з кодовим управлінням вбудовуванням ДІ для виду шуму «Salt and Pepper» має місце на рівні до 48% (рис.) для випадку кодового слова порядку $\mu = 8$, що впливає на трансформанту Уолша-Адамара (1,5).

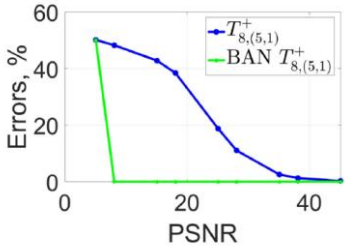


Рис. Графіки залежності числа помилок при вилученні ДІ від рівня зашумлення шумом «Salt and Pepper»

Висновки. У роботі проведено дослідження можливостей підвищення стійкості стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації. Запропоновано рекомендації щодо роботи даного методу в умовах зашумлення каналу АБГШ, а також застосування обмеження по амплітуді елементів матриць Δ_i, яке дозволило зменшити рівень помилок при вилученні ДІ на рівні до 48%.

Література

1. Кобозева А. А., Соколов А.В. Устойчивый стеганографический метод с кодовым управлением внедрением информации. Проблемы Региональной Энергетики. 2021. №. 4 (52). С. 115-130.

2. Kobozeva A.A., Sokolov A.V. Theoretical foundations for constructing effective codewords for the code-controlled information embedding steganographic method. Radiotekhnika. 2021. 4(207). P. 27-39.

3. Костырка О.В. Анализ преимуществ пространственной области цифрового изображения-контейнера для стеганопреобразования. Інформатика та математичні методи в моделюванні. 2013. № 3. С. 275-282.

АНАЛІЗ СПОСОБІВ ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ ВОЛОКОННО-ОПТИЧНИХ ЛІНІЙНИХ ТРАКТІВ

Герасименко-Вакуленко Н.О.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м.Київ

Актуальною проблемою, що потребує систематичного вирішення при модернізації існуючих та розбудові нових волоконно-оптичних ліній зв'язку (ВОЛЗ), є попередній вибір лінійного оптичного волокна (ОВ) з потрібними передавальними характеристиками. Поставник пропонує різні типи одномодових ОВ, які істотно різняться за своїми характеристиками та вартістю. При виборі ОВ потрібно враховувати не тільки дисперсійні характеристики волокна але й такі характеристики, як діаметр поля моди та ефективну площу, коефіцієнт згасання оптичної потужності та локальні втрати потужності сигналу за рахунок оптичного випромінення на макровигинах волокна.

Як відомо, одним із способів збільшення пропускної здатності однохвильового волоконно-оптичного каналу, організованого за технологією TDM розділення різних сигналів в часі (Time Division Multiplexing – накладання розділене в часі), є збільшення швидкості передавання даних, значення якої обмежується дисперсійними явищами у волоконно-оптичному світловоді (дисперсія хроматична і дисперсія поляризованої моди) та швидкодією електронних компонент системи передачі. У технології WDM (Wavelength Division Multiplexing – ущільнення за довжинами хвиль, або спектральне ущільнення каналів передачі), немає багатьох обмежень і технологічних труднощів, властивих технології TDM. Для підвищення пропускної здатності, замість збільшення швидкості передавання в однохвильовому каналі, як це реалізовано в технології TDM, в технології WDM збільшують число каналів (кожний канал на своїй довжині хвилі), які використовують для одночасного передавання різних сигналів по одному і тому самому волокну. Отже, на кожній носійній довжині хвилі в системі WDM може передаватися ТДМ-сигнал. Системи передачі, побудовані за цим принципом, називаються гібридними системами TWDM.

Система WDM багато в чому схожа на традиційну систему TDM. Сигнали різних довжин хвиль, що генеруються декількома оптичними передавачами, об'єднуються оптичним мультиплексором (ОМ – Optical Multiplexer, MUX (Multiplexer)) в багатоканальний груповий оптичний сигнал. При великих відстанях передачі групового сигналу, на лінії зв'язку встановлюється один або декілька оптичних підсилювачів. Демультиплексор DEMUX (Demultiplexer) приймає об'єднаний сигнал, виділяє з нього початкові канали різних довжин хвиль і спрямовує їх на відповідні фотоприймачі. На проміжних вузлах деякі канали можуть бути додані або виділені з об'єднаного сигналу за допомогою мультиплексорів введення/виведення.

Для підвищення пропускної здатності ліній зв'язку замість збільшення швидкості передачі у оптичному каналі, як це робиться в системах TDM, в системах WDM йдуть шляхом збільшення числа каналів (котрі передаються на різних довжинах хвиль), що застосовуються у

системах передачі. Технологія WDM дозволяє суттєво збільшити пропускну здатність лінії зв'язку, дає можливість організувати двухсторонню передачу даних по одному волокну, причому нарощування пропускної здатності може відбуватись на вже існуючому волоконно-оптичному кабелі. Зазначу, що можливості й переваги технології WDM, у ще більшому ступені розкриваються в складних мережах зв'язку, що містять багато різних вузлів. На проміжних вузлах спектральні канали можуть бути додані або виділені зі складеного сигналу за допомогою мультиплексорів введення/виводу, а інші канали проходять через вузол без перетворення в електричний сигнал. Всі розглянуті компоненти, дозволяють виконати поставлене завдання.

Список використаних джерел

1. Власов О. М. Підвищення пропускної спроможності волоконно-оптичних лінійних трактів на одномодових світловодах. *Сучасні тенденції розвитку технологій в інфокомунікаціях та освіті* : матеріали наук. конф., м. Харків, 25–26 лист. 2010 р . Харків, 2010. С. 132–137.

2. Каток В.Б., Руденко І.Е., Ранський Є.Г., Однорог П.М. Волоконно-оптичний зв'язок : посіб. Київ : Логос 2015. 383 с.

СУЧАСНІ ВИМОГИ ДО ОБРОБКИ ВЕЛИКИХ ОБСЯГІВ ДАНИХ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Андрійчук Владислав Вікторович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Зростання обсягів даних у телекомунікаційних мережах є актуальною проблемою, яка вимагає ефективної обробки для забезпечення надійності та якості послуг, проведено аналіз сучасних вимог до обробки великих обсягів даних у телекомунікаційних мережах та розглянуто приклади їх застосування.

Аналітики компанії IBS «весь світовий обсяг даних» оцінили такими величинами:

– 2003 г. – 5 ексабайт даних (1 ЕБ = 1 млрд гігабайтів)

– 2008 г. – 0,18 зетабайта (1 ЗБ = 1024 ексабайти)

– 2015 г. – більше 6,5 зетабайт – 2021 г. – 44–48 зетабайта (прогноз)

– 2025 г. – цей об'єм збільшується ще у 10 разів.

Великі дані – це сукупність технологій, покликаних здійснювати три операції: – Обробляти більші, у порівнянні зі «стандартними» сценаріями, об'єми даних. – Уміти працювати з даними, що швидко надходять у дуже великих об'ємах. Тобто даних не просто багато, а їх постійно стає все більше й більше. – Вміти працювати зі структурованими і мало стуктурованими даними паралельно і у різних аспектах.

Аналіз зростання кількості користувачів

За останні роки спостерігається стрімкий розвиток телекомунікаційних послуг, що призводить до збільшення кількості користувачів. Наприклад, застосунки для спілкування, соціальні медіа, онлайн-торгівля та інші платформи залучають мільйони людей. Це створює потребу у швидкій та ефективній обробці даних для задоволення потреб користувачів.

Розвиток нових послуг.

З'явлення нових телекомунікаційних послуг, таких як стрімінгове відео, віртуальна реальність та Інтернет речей, призводить до значного збільшення обсягів даних, що потребують обробки. Наприклад, стрімінгові платформи, такі як Netflix та YouTube, генерують велику кількість даних через потікове відтворення відео в реальному часі.

Технологічні прориви

Впровадження нових технологій, зокрема 5G, сприяє зростанню пропускної здатності мереж та, відповідно, збільшенню обсягів даних. Нові послуги, які використовують велику пропускну здатність, наприклад, відеозв'язок високої якості або геймінг у хмарі, вимагають обробки великих обсягів даних у реальному часі.

Вимоги до обробки великих обсягів даних у телекомунікаційних мережах

Швидкодія

Обробка даних у реальному часі стає все важливішою для забезпечення безперебійного функціонування та задоволення потреб користувачів. Вимагаються швидкі алгоритми та системи, які здатні ефективно обробляти великі обсяги даних у найкоротші терміни.

Масштабованість

Системи обробки даних повинні бути масштабовані, тобто здатні працювати зі зростаючими обсягами інформації без втрати продуктивності. Потрібні архітектури, що можуть розширюватися горизонтально та вертикально, а також розподілені системи для оптимального використання ресурсів.

Збереження та архівування

Великі обсяги даних потребують ефективних методів їх збереження та архівування. Важливо забезпечити не тільки надійне збереження даних, але й швидкий доступ до них для подальшого аналізу та обробки.

Технології які найчастіше використовуються для роботи з базами даних

NoSQL. Серед NoSQL-рішень, що застосовуються, виділяються: MongoDB — кросплатформова документо-орієнтована система керування базами даних з підтримкою JSON та динамічних схем, Apache Cassandra — масштабована база даних, орієнтована на стійкість до відмов.

Hadoop. Apache Hadoop. Серед програмного забезпечення, що пов'язано з Hadoop, виділяють: Apache Ambari — інструмент для управління та моніторингу Hadoop кластерів, Apache Avro — система серіалізації даних, Apache Hive — інфраструктура сховища даних, яка забезпечує агрегацію даних, Apache Pig — високорівнева мова потоків даних і програмний каркас для паралельних обчислень, Apache Spark — високопродуктивний рушій для обробки даних, що зберігаються в кластері Hadoop та ін.

Зростання кількості користувачів, розвиток нових послуг та впровадження нових технологій призводять до збільшення обсягів даних. Для ефективної обробки цих даних необхідно враховувати вимоги щодо швидкодії, масштабованості та збереження. Дослідження та впровадження відповідних технологій та методів можуть сприяти оптимальній обробці великих обсягів даних у телекомунікаційних мережах.

Список використаних джерел:

1. Johnson, A., & Brown, C. (2020). Handling Big Data in Telecommunications Networks. International Journal of Communication Systems.
2. Smith, J. (2018). Big Data in Telecommunications: Challenges, Opportunities, and Future Perspectives. Telecommunications Journal.

ВПРОВАДЖЕННЯ СИСТЕМИ ФУНКЦІОНУВАННЯ ЛІТАЮЧИХ АПАРАТІВ НА БАЗІ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

Москаленко Данило Олексійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Літаючі апарати на базі бездротових сенсорних мереж (БСМ) є одним з передових напрямків розвитку технологій в сучасному світі. Їх потенціал використання в різних сферах діяльності є значним і варіативним. Аналізуючи цей потенціал, можна зрозуміти, що розробка та впровадження системи функціонування літаючих апаратів на базі БСМ має велику важливість для досягнення ефективності та прогресу у різних галузях.

Однією зі сфер, в яких літаючі апарати на базі БСМ можуть мати значний вплив, є геодезія та картографія. [1]Вони можуть використовуватись для високоточного зйомки територій, мапування складних рельєфів та моніторингу змін у природному середовищі. Завдяки бездротовим сенсорним мережам, такі апарати можуть збирати велику кількість даних, що дозволяє зробити картографування більш точним та швидким.

У сфері транспорту та логістики літаючі апарати на базі БСМ можуть бути використані для виконання розвідки маршрутів, контролю над дорожнім рухом та навігації. Вони можуть допомагати зменшити транспортні затори, покращити безпеку дорожнього руху та забезпечити більш ефективне використання ресурсів.

Літаючі апарати на базі БСМ також можуть знайти застосування в сільському господарстві.[2] Вони можуть виконувати моніторинг стану посівів, виявляти погодні умови та шкідливих комах, що сприяє підвищенню врожайності та оптимізації використання ресурсів.

Крім того, літаючі апарати на базі БСМ можуть мати важливе застосування в пошуках та рятувальних операціях, моніторингу стану навколишнього середовища, виявленні пожеж та відстеженні змін клімату. Вони можуть допомагати у прогнозуванні природних катастроф та вчасному реагуванні на них.

Отже, аналізуючи можливості літаючих апаратів на базі бездротових сенсорних мереж, їх розробка та впровадження системи функціонування виявляються важливими для покращення ефективності та прогресу в різних галузях діяльності. Впровадження цих систем може мати значний вплив на геодезію, транспорт, сільське господарство, пошуки та рятувальні операції, а також на збереження природи та сталий розвиток.

Література

1. Smith, J. D., & Johnson, A. B. (2018). Wireless Sensor Networks: Principles and Practice. CRC Press.

2. Sharma, R., & Kumar, V. (Eds.). (2019). Applications of Wireless Sensor Networks in the Industry. Springer.

АНАЛІЗ ПРАВОВОГО РЕГУЛЮВАННЯ СФЕРИ ЛІЦЕНЗУВАННЯ ТА СЕРТИФІКАЦІЇ ВИКОНАННЯ РОБІТ В ТЕЛЕКОМУНІКАЦІЙНІЙ СФЕРІ ЄС

Тишик Вікторія Віталіївна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій

Законом України від 16.09.2014 р. №1678-VII [1] **ратифіковано Угоду про асоціацію між Україною, з однієї сторони, та Європейським Союзом (ЄС), Європейським співтовариством з атомної енергії і їхніми державами-членами**, з іншої сторони. Відповідно до ст. 117 цієї Угоди сторони мають забезпечувати можливість застосування ліцензій для вирішення питань щодо розподілу номерів та частот. В доповненні XVII-3 «Правила, що застосовуються до телекомунікаційних послуг» до цієї Угоди Україна взяла на себе зобов'язання забезпечити поступове приведення свого законодавства у відповідність до законодавства ЄС.

Правове регулювання в сфері ліцензування та сертифікації виконання робіт в телекомунікаційній сфері постійно змінюється і адаптується до змін технологій та вимог ринку, тому дослідження досвіду сертифікації та ліцензування в телекомунікаційній сфері ЄС допоможе краще зрозуміти вектор розвитку української телекомунікаційної мережі в на шляху вступу України до ЄС, окреслити тенденції розвитку та сприятиме вдосконаленню національного правового регулювання у сфері телекомунікаційних послуг.

Ліцензування та сертифікація робіт і проектів в телекомунікаційній сфері ЄС є важливими елементами правового регулювання для забезпечення безпеки, якості та надійності телекомунікаційних послуг. Процедури ліцензування та сертифікації можуть відрізнятись між різними країнами ЄС, оскільки регуляторні рамки можуть бути встановлені на рівні національного законодавства або на рівні ЄС. Ліцензія дозволяє компаніям надавати телекомунікаційні послуги, тоді як сертифікат підтверджує відповідність продукту або системи технічним стандартам.

Ліцензування в телекомунікаційній сфері ЄС передбачає процес отримання дозволу від національних регуляторів або інших компетентних органів для надання телекомунікаційних послуг. Ліцензія є офіційним документом, виданим відповідним національним регулятором телекомунікацій, який надає компанії або оператору право на надання телекомунікаційних послуг у відповідній країні-члені ЄС. Ліцензія може включати обмеження, умови та вимоги, які компанія має виконувати для забезпечення якості та безпеки послуг, а також для дотримання відповідних правил і законодавства. Ліцензія надає компанії право використовувати певні радіочастоти та ресурси, необхідні для надання телекомунікаційних послуг. В ЄС ліцензію в сфері телекомунікацій можуть отримувати як юридичні особи, так і фізичні особи, якщо вони відповідають вимогам, установленим законодавством країни-члена ЄС, в якій вони подають заявку на отримання ліцензії. Ліцензування телекомунікаційної діяльності в ЄС здійснюється на рівні кожної окремої країни-члена, відповідно до національного законодавства та директив ЄС. ЄС встановлює загальні рамки та принципи, які країни-члени мають враховувати при ліцензуванні. Процедура може включати подання заявки на отримання ліцензії, представлення документів, перевірку відповідності та сплату відповідних зборів. Вимоги до отримання ліцензії в ЄС можуть варіюватися в залежності від країни-члена, але в основному вони включають інформацію про заявника, його фінансову стабільність, технічні здібності, плани розвитку мережі та спектральну політику.

Вимоги щодо отримання ліцензії можуть варіюватися в залежності від країни та конкретних умов. Зазвичай, для отримання ліцензії в сфері телекомунікацій юридичній або фізичній особі потрібно відповідати вимогам:

- фінансовим - заявник повинен мати достатні фінансові ресурси для забезпечення надійного та стабільного функціонування телекомунікаційних послуг;

- щодо технічної компетентності - заявник повинен мати достатній рівень технічної експертизи та знань, що дозволяють надавати телекомунікаційні послуги;

- безпеки та конфіденційності - заявник повинен дотримуватися стандартів безпеки та конфіденційності, які встановлюються відповідними органами регулювання;

- дотримання вимог законодавства - заявник повинен дотримуватися всіх вимог, встановлених відповідними національними і європейськими законодавчими актами, що регулюють сферу телекомунікацій;

- в окремих випадках можуть бути встановлені додаткові вимоги, такі як наявність ліцензованих спеціалістів у складі команди або виконання певних обов'язкових процедур.

Для отримання статус ліцензованого спеціаліста в сфері телекомунікацій в ЄС, зазвичай, потрібно пройти певний процес ліцензування, який організовує національний регулятор телекомунікацій відповідної країни-члена ЄС. Наприклад, в Німеччині це Federal Network Agency, у Франції - Агентство зв'язку ARCEP, в Іспанії - Комісія з ринку телекомунікацій і поштових послуг Comisión Nacional de los Mercados y la Competencia, в Італії - Агенція з регулювання телекомунікацій та поштових послуг Autorità per le Garanzie nelle Comunicazioni.

Сертифікація в телекомунікаційній сфері ЄС спрямована на підтвердження відповідності обладнання, програмного забезпечення та послуг встановленим стандартам та вимогам. Часто це пов'язано з технічною безпекою, електромагнітною сумісністю та якістю обслуговування. Органи сертифікації проводять оцінку відповідності та тестування продуктів, підтверджуючи їх відповідність вимогам європейських стандартів. В ЄС існують регуляторні рамки та стандарти, що встановлюють вимоги до якості, безпеки та сумісності проектів в телекомунікаційній сфері. Розробники проектів повинні враховувати ці стандарти при підготовці своїх робіт.

Для проведення процесу **сертифікації розробників проектів** використовуються незалежні сертифікаційні органи, які оцінюють та перевіряють відповідність проектів встановленим стандартам та вимогам. Ці органи виконують аудити, тести та інші процедури для підтвердження відповідності розробок вимогам сертифікації. Процес сертифікації включає подання заявки на сертифікацію до відповідного сертифікаційного органу, перевірку документації та виконання необхідних тестів та аудитів. Результатом успішної сертифікації є отримання сертифікату, який підтверджує відповідність проекту вимогам та стандартам. Розробники проектів в телекомунікаційній сфері повинні мати систему управління якістю, яка включає процеси контролю якості, забезпечення безпеки та відповідності стандартам. Ця система також може бути піддана сертифікації для підтвердження її ефективності та відповідності вимогам. Після отримання сертифікату розробники проектів повинні імплементувати рекомендації та вимоги сертифікації у свої роботи. Регуляторні органи та сертифікаційні органи також здійснюють контроль та аудити для перевірки дотримання встановлених стандартів.

Сертифікат розробника проектів з телекомунікацій в ЄС можна отримати через акредитовані сертифікаційні органи, які мають повноваження видачі сертифікатів відповідності. Ці органи зазвичай мають незалежний статус і підтверджують відповідність розроблених проектів встановленим стандартам та вимогам. Процедури та вимоги для отримання сертифікату можуть варіюватися в залежності від країни ЄС та обраного сертифікаційного органу. Для отримання сертифікату проектувальника телекомунікаційної мережі на території ЄС треба звернутись до відповідних професійних організацій або асоціацій, які здійснюють акредитацію та сертифікацію фахівців у галузі телекомунікацій, наприклад, таких як Європейська Федерація Інженерів Телекомунікацій (European Federation of Telecommunications Engineers), Європейська Асоціація Комунікаційних Інженерів (European Association of Communications Engineers) або подібних національних асоціацій відповідних країн ЄС. Такі організації зазвичай мають програми сертифікації та акредитації для фахівців у

сфері телекомунікацій. Вони можуть проводити оцінку знань, навичок і досвіду, а також вимагати пройти спеціальні курси або навчання для отримання сертифікату.

Виконавець телекомунікаційного проекту в ЄС може мати як сертифікат, так і ліцензію, або обидва залежно від конкретних вимог та правил країни-члена ЄС де проектується та реалізується проект. Сертифікат, зазвичай, стосується відповідності продукту, системи або обладнання технічним стандартам та вимогам безпеки, що дозволяє їх використання на ринку ЄС. Сертифікат може бути виданий відповідним органом або організацією з сертифікації, які мають повноваження здійснювати оцінку відповідності. Ліцензія надає право на надання телекомунікаційних послуг у відповідній країні-члені ЄС і видається відповідним національним регулятором телекомунікацій та може містити умови та вимоги, які оператор має виконувати для забезпечення якості та безпеки послуг.

Порівнюючи процес сертифікації та ліцензування робіт виконуваних в сфері телекомунікаційній в ЄС та в Україні можна зробити висновок, що основні принципи та етапи виконання даних робіт в цих країнах схожі, однак існують відмінності в законодавстві та в регуляторних політиках кожної країни.

Список використаних джерел:

1. Закон України «Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони» Електронний ресурс: https://zakon.rada.gov.ua/laws/show/1678-18#Text

2. Офіційний сайт ЄС Електронний ресурс: https://eur-lex.europa.eu/homepage.html?locale=en

ЕВОЛЮЦІЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ У СУЧАСНІЙ ВОЄННІЙ СИТУАЦІЇ

Христевич Олександр Сергійович
Державний університет телекомунікацій

Сучасна воєнна ситуація ставить перед нами унікальні виклики, які вимагають інноваційних підходів до телекомунікаційних систем. У цьому розділі вводиться контекст і визначається значимість розвитку міцних комунікаційних мереж, а також описуються цілі дослідження.

Розширена архітектура мереж

Для забезпечення ефективного зв'язку під час воєнних дій, телекомунікаційні системи повинні бути адаптивними, масштабованими і здатними підтримувати різноманітні пристрої та сервіси. У цьому розділі розглядається розвиток розширеної архітектури мереж, такої як мережі з програмно-визначеною архітектурою (SDN) та віртуалізація функцій мережі (NFV), що пропонують гнучкість, централізоване керування та поліпшену розподіл ресурсів.

Техніки управління спектром

Недостатність спектру та електромагнітні перешкоди становлять великі виклики для телекомунікаційних систем у сучасних воєнних діях. У цьому розділі досліджуються нові техніки управління спектром, включаючи динамічний доступ до спектру, мережі когнітивного радіо та стратегії спільного використання спектру. Ці підходи оптимізують використання спектру, зменшують взаємовплив та забезпечують ефективне співіснування різних систем зв'язку.

Інтеграція нових технологій

Інтеграція нових технологій має великий потенціал для покращення телекомунікаційних систем у сучасних воєнних діях. У цьому розділі розглядається впровадження технологій,

таких як штучний інтелект (AI), Інтернет речей (IoT) та мережі 5G. Досліджується, як ці технології можуть покращити ситуаційну обізнаність, забезпечити автономне прийняття рішень та підтримувати використання розумних та підключених пристроїв на полі бою.

Виклики та перспективи майбутнього

Незважаючи на значний прогрес у розвитку телекомунікаційних систем для сучасних воєнних дій, виникають нові виклики. У цьому розділі обговорюються можливі перешкоди, такі як вразливості безпеки, проблеми взаємодії та етичні аспекти. Також висвітлюються майбутні напрямки дослідження, зокрема дослідження квантового зв'язку, супутникових констеляцій та мереж на основі маршрутизації у вигляді мережі з масштабованою топологією.

Висновки

Розвиток телекомунікаційних систем і мереж у сучасних воєнних умовах вимагає постійної інновації та адаптації. Ця дисертація досліджує основні аспекти розширеної архітектури мереж, технік управління спектром та інтеграції нових технологій, пропонуючи оригінальну перспективу щодо поліпшення можливостей зв'язку на полі бою в умовах постійно змінюваної динаміки воєнних дій.

ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ 5G У РОЗУМНИХ БУДИНКАХ: НОВІ МОЖЛИВОСТІ ТА ПЕРЕВАГИ

Шмельов Михайло Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

5G - це п'яте покоління мобільних мереж, яке відкриває нові можливості для швидкого та надійного бездротового зв'язку. Україна також активно розвиває і впроваджує 5G технологію, щоб забезпечити населенню передові можливості зв'язку.

Україна розпочала підготовку до впровадження 5G ще у 2018 році, коли проведена аукціонна торгівля по дозвільних документах для використання радіочастотного ресурсу. У наступні роки проводилися експерименти та тестування нової технології.

В 2020 році розпочалося комерційне впровадження 5G мереж в Україні. Поступово оператори зв'язку почали пропонувати послуги 5G в окремих містах країни. Перший етап впровадження орієнтований на основні міські центри та промислові райони.

Технологія 5G дозволяє передавати дані з надзвичайно високою швидкістю та низькою затримкою, що сприяє покращенню якості зв'язку, швидкості завантаження та передачі даних. Вона також підтримує підключення великої кількості пристроїв, що є важливим аспектом для розвитку Інтернету речей та розумних технологій.

Впровадження 5G в Україні дозволяє розширити можливості мобільного зв'язку, покращити швидкість та якість передачі даних, забезпечити інноваційні послуги та прискорити розвиток цифрової інфраструктури. Це відкриває нові перспективи для економіки, науки, медицини, транспорту та багатьох інших галузей.

Завдяки появі технології 5G, розумний будинок входить в нову еру і надає безліч нових функцій та переваг. Ця передова технологія, яка пропонує високу швидкість та низьку затримку, відкриває безмежні можливості для власників будинків. Деякі з цих нововведень включають:

- Швидкісне бездротове підключення: 5G забезпечує швидке та стабільне бездротове підключення по всьому будинку. Це означає, що власники зможуть насолоджуватися швидким Інтернетом та завантажувати великі файли миттєво.
- Дистанційне керування: Завдяки 5G, власники розумного будинку зможуть дистанційно керувати різними системами та пристроями в будинку. Це означає, що вони

зможуть включати та вимикати світло, регулювати температуру, контролювати безпеку та багато іншого, навіть коли вони не знаходяться вдома.

- Розширена реальність (AR): 5G відкриває нові можливості для використання розширеної реальності в розумному будинку. Власники зможуть використовувати AR для створення інтерактивних візуалізацій, додавання віртуальних елементів до свого оточення та сприяння більшій зручності та ефективності.
- Розумні аудіосистеми: 5G дозволяє створювати розумні багатокімнатні аудіосистеми, які синхронізуються між кількома приміщеннями. Власники можуть насолоджуватися високоякісним звуком, який заповнює кожну кімнату, та легко керувати відтворенням з мобільного.
- Розумна енергія та ефективність: За допомогою 5G, розумні будинки можуть використовувати енергію більш ефективно. Наприклад, системи керування енергією можуть автоматично регулювати використання електроприладів залежно від потреб, що допомагає знизити споживання енергії та економити кошти.
- Розумна безпека: 5G розширює можливості розумної безпеки в будинку. Завдяки швидкому та надійному зв'язку, власники можуть отримувати миттєві повідомлення про потенційні небезпеки, які сприяють покращенню безпеки будинку та захисту майна.

Список використаних джерел:

1. TS2// Marcin Frąckiewicz // The impact of 5G on smart homes// [https://ts2.space/en/the-impact-of-5g-on-smart-homes/]

2. УНІАН//Роман Хіміч // 5G для України: туман розсіюється // [https://www.unian.ua/economics/other/5g-dlya-ukrajini-tuman-rozsiyuyetsya-12010437.html]

СЕКЦІЯ 2

Інформаційні системи та технології

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ СТАНДАРТУ ПЕРЕДАЧІ ДАНИХ AMQP

Бацак Артем Олексійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

AMQP (Advanced Message Queuing Protocol) - це протокол передачі повідомлень, який був розроблений з метою стандартизації та поліпшення комунікації між різними системами та пристроями. Він був спеціально розроблений для вимогливих до надійності та ефективності сценаріїв, включаючи системи Інтернету речей (IoT).

Основні особливості AMQP:

1. Надійна доставка повідомлень: AMQP забезпечує гарантовану доставку повідомлень від одного пристрою до іншого. Це важливо в сценаріях, де критично важлива точність та повнота обміну даними.

2. Розширена маршрутизація повідомлень: AMQP підтримує різні способи маршрутизації повідомлень між пристроями. Це дозволяє гнучко керувати тим, як повідомлення будуть доставлені та оброблені.

3. Багатопартнерськість: AMQP підтримує багатопартнерськість, що дозволяє використовувати його для комунікації між різними системами, включаючи пристрої, які використовують різні мови програмування та операційні системи.

4. Відкритість та стандартизація: AMQP є відкритим протоколом, розробленим відповідно до стандартів, що підтримуються міжнародними організаціями. Це дозволяє різним розробникам та виробникам пристроїв використовувати його у своїх системах.

5. Розширюваність: AMQP має гнучку архітектуру, яка дозволяє розширювати його функціональність та використовувати додаткові можливості, такі як шифрування повідомлень або управління потоком.

AMQP широко використовується у сценаріях, де важлива надійна комунікація між системами та пристроями, таких як фінансові послуги, телекомунікації, логістика та, звичайно, Інтернет речей.

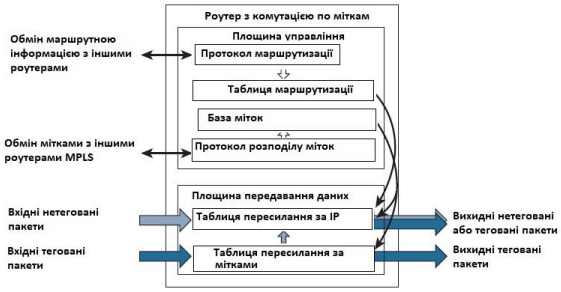
Було розглянуто особливості функціонування стандарту передачі даних AMQP (Advanced Message Queuing Protocol) у контексті сучасних мереж Інтернету речей (IoT).

AMQP є потужним протоколом, який забезпечує надійну та ефективну комунікацію між різними пристроями та системами в IoT-екосистемі. Він пропонує стандартизований підхід до передачі повідомлень, використовуючи модель клієнт-сервер та механізми черги повідомлень.

ТЕХНОЛОГІЯ MPLS В МАРШРУТИЗАТОРАХ CISCO

Мантула Р.А.
Державний університет телекомунікацій, м. Київ

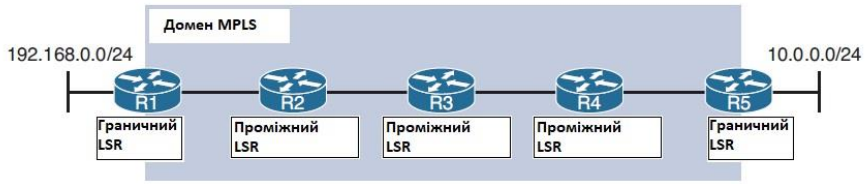
Багатопротокольна комутація по міткам (MPLS) — це метод пересилання пакетів, який приймає рішення про пересилання на основі міток, а не на рівні 3 адресата пакета. MPLS був розроблений для підтримки багатьох різних протоколів рівня 3. Мітки можна використовувати замість IPv4-адреси призначення — для пересилання IP-пакетів. В сучасних маршрутизаторах MPLS не набагато швидший за традиційну IP-маршрутизацію. Основна перевага MPLS в тому, що ця технологія підтримує численні служби, такі як одноадресна маршрутизація, багатоадресна маршрутизація, VPN, Traffic Engineering (TE), QoS і Any Transport Over MPLS (AToM). Таким чином, MPLS є дуже ефективним і гнучким.



Малюнок 1. Структура роутера MPLS.

На малюнку 1 позначено, що площина керування маршрутизатора з підтримкою MPLS відповідає за обмін мітками з іншими маршрутизаторами з підтримкою MPLS за допомогою протоколу розподілу міток на додаток до обміну інформацією про маршрутизацію за допомогою протоколів маршрутизації для заповнення таблиці маршрутизації IP (Routing Information Base - RIB). Після обміну мітками інформація про мітки використовується для заповнення LIB (Label Information Base), а потім найкраща інформація про мітки може бути використана для заповнення інформаційної бази пересилання (Forwarding Information Base - FIB), щоб можна було позначати пакети без міток і LFIB (Label Forwarding Information Base), щоб можна було позначати пакети з мітками. пересилаються або мітки можуть бути видалені, коли пакети потрібно пересилати FIB.

На малюнку 2 розглянуто структуру мережі MPLS. Маршрутизатори від R1 до R5 є частиною домену MPLS. Вони відомі як маршрутизатори з комутацією міток (LSR), оскільки підтримують MPLS. У цьому випадку R1 і R5 вважаються граничними LSR, а R2, R3 і R4 вважаються проміжними LSR. Граничний LSR знаходиться на краю домену MPLS і додає мітки до пакетів, які входять до домену MPLS (відомий як вхідний LSR), видаляє мітки з пакетів, які будуть залишати домен MPLS (відомий як вихідний LSR), і навіть пересилає пакети за потреби на основі міток або відсутності мітки. Проміжний LSR знаходиться в домені MPLS і переважно пересилає пакети, використовуючи інформацію про мітку.



Малюнок 2. Домен MPLS.

Шлях з комутацією міток (LSP) — це послідовність маршрутизаторів, яку тегований пакет проходить через домен MPLS. Це односпрямований шлях. На шляху кожен

маршрутизатор перевіряє мітку, щоб прийняти рішення про переадресацію, видаляє мітку, додає нову мітку, якщо потрібно , а потім пересилає пакет.

Щоб MPLS працював, до пакета потрібно додати мітку. Мітка додається як додатковий заголовок між заголовком кадру рівня 2 і заголовком пакета рівня 3. Роутер MPLS автоматично додає мітку для кожної відомої йому мережі.

Щоб побудувати LSP, мітки потрібно спільно використовувати/розповсюджувати з безпосередньо підключеними LSR. Це робиться за допомогою протоколу розповсюдження міток, наприклад протоколу розповсюдження міток (LDP), який є найпоширенішим протоколом, який використовується під час спільного використання/розповсюдження міток для префіксів IPv4. Після ввімкнення MPLS на інтерфейсі пакети привітання LDP надсилаються через інтерфейс на цільову багатоадресну адресу 224.0.0.2 (групова адреса всіх маршрутизаторів), використовуючи UDP-порт 646. Будь-який пристрій на цьому ж каналі, у якому також увімкнено MPLS, формує сеанс LDP TCP із використанням порту 646 із сусіднім пристроєм, щоб можна було обмінюватися інформацією про мітки.

Кожний MPLS роутер за допомогою міток, отриманих від LDP-сусідів, формує LIB. У відповідності з інформацією, що міститься в таблиці маршрутизації та LIB, роутер формує LFIB та FIB.

Список використаних джерел:

4. Vivek Alwayn. “Advanced Mpls Design and Implementation”. Cisco Systems. 2001.

5. CCNP Enterprise Advanced Routing ENARSI 300-410 official cert guide. Cisco Systems, 2020

SMS FRAUD REALIZATION AND RECOGNITION METHODS

Sahaidak Viktor
Educational-scientific Institute of Telecommunications
State University of Telecommunications
Kyiv, Ukraine

Telecommunications market was never an exception for fraudsters. Due to carrier network telecom fraud can vary based on different realization methods, that can be combined to achieve fraudster’s goal. Let’s take a look on most common SMS fraud types.

Smishing/SMS Phishing is the practice of sending mass SMS in order to obtain personal information from the person who receives the messages. A simple system for monitoring signups and transactions coming from the B2B service should be enough to ensure telco company isn’t helping a smishing business.

SMS hacking - criminals can hack an operator’s SMS center or even take control of it at the signaling level and use it to send malicious traffic all over the world. This traffic could solicit consumers to make calls to premium numbers or even contain viruses or other malware that could infect the recipient’s phone.

Malware SMS based fraud. The most popular of such fraud realization was FluBot. First spotted in December 2020, FluBot has gained traction in 2021 and compromised a huge number of devices worldwide, including significant incidents in Spain and Finland. The malware was installed via text messages which asked Android users to click a link and install an application to track to a package delivery or listen to a fake voice mail message. Once installed, the malicious application, which actually was FluBot, would ask for accessibility permissions. The hackers would then use this access to steal banking app credentials or cryptocurrency account details and disable built-in security mechanisms. This strain of malware was able to spread like wildfire due to its ability to access an

infected smartphone's contacts. Messages containing links to the FluBot malware were then sent to these numbers, helping spread the malware ever further.

SMS Bypass is a practice where unscrupulous SMS aggregators use unauthorized or even illegal routes to deliver SMS messages at the lowest possible cost. This practice harms operators, depriving them of their legitimate termination revenues. To understand it, let's look at a scenario with two operators in different countries:

1) A customer of Operator A sends an SMS to a customer of Operator B.
2) Operator A charges its customer a fee.
3) Operator B charges Operator A a fee for providing the SMS to its customer.

That last charge, where the SMS terminates, is the termination rate. These rates vary wildly depending on the contracts between the two operators. Some of them are expensive, others are close to 0. This is where a fraudulent operator comes into the picture. They reroute these international SMS using a SIM box or GSM gateway, effectively hijacking the connection to achieve cheaper termination rates. They are essentially making long-distance services much cheaper, but the sender pays the same price – so the fraudster telco pockets the difference.

A common symptom of SMS fraud is abnormal spikes in SMS traffic volumes from one operator to another. In a recent instance, an Australian operator, suddenly began receiving huge volumes of SMS traffic from an African country. The daily SMS volumes, which were typically in the hundreds, went up to 145,000 messages per day, costing the Australian operator €10,000 per day in SMS termination fees that could not be invoiced. If the case had gone undetected, the Australian operator would have lost €300,000 to SMS fraud in just one month.

References:

1. BICS [online]// Understanding international telecoms fraud – Available - https://www.bics.com/wp-content/uploads/2022/02/Telco-Fraud-Whitepaper.pdf
2. EUROPOL [online]// Takedown of SMS-based FluBot spyware infecting Android phones – Available - https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones
3. SEON [online]// 11 Types of Telecommunications Fraud: How to Detect & Prevent It – Available - https://seon.io/resources/telecommunications-fraud-detection-and-prevention/

ФРЕЙМВОРКИ ДЛЯ АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Гакман Дмитро Віталійович,
Державний університет телекомунікацій,
Навчально-науковий інститут інформаційних технологій

Постановка проблеми: Автоматизоване тестування є важливою складовою процесу розробки програмного забезпечення в будь-яких сферах, в тому числі і телекомунікаційних системах. Тестується все: від інтерфейсів доступу, які можуть мати вигляд веб-сайту, мобільного додатку чи CLI інтерфейсу, до функціонування окремих частин телекомунікаційної системи чи її робота в цілому. Автоматизоване тестування дозволяє підвищити його продукту та пришвидшити розробуку і випуск нових версій. Одним із ключових елементів автоматизованого тестування є використання фреймворків. Та водночас постає проблема їх вибору під кожен окремий набір задач та питань.

Мета дослідження: Полегшення процесу підбору фреймворку, розгляд переваг та недоліків кожного з них та огляд існуючих технологій в даній сфері.

Результат дослідження: Сучасні та найбільш популярні фреймворки можна розбити на 3 категорії. При плануванні тестування в першу чергу варто визнпчити яку категорію можна застосувати під даний проєкт, та відштовхуватись саме від цієї інформації.

Першою категорією є фреймворки загального призначення. Вони призначені для найбільш широкого кола задач і при адаптації та поєднанні зі іншими інструментами можуть покривати будь-які сфери. Найкраще вони підходять для розробки автоматизації функціональних, інтеграційних та системних тестів. Використовуючи дані фреймворки, можна з легкістю налаштувати під'єднання до пристрою що буде тестуватись використовуючи, до прикладу SSH чи UART з'єднання та виконувати рзіні набори тестів без участі людини. Серед лідерів можна виділити RobotFramework та pytest.

Robot Framework є одним з найбільш популярних фреймворків для автоматизованого тестування. Він базується на використанні ключових слів і може бути використаний для тестування різних типів програмного забезпечення, включаючи веб-додатки, мобільні додатки та та десктопні додатки. Robot Framework підтримує різні мови програмування, такі як Python, Java, C# та інші, що дозволяє програмістам працювати з фреймворком у зручному для них середовищі. Крім того, Robot Framework є відкритим програмним забезпеченням та підтримується активною спільнотою. Robot Framework має розширену документацію та активну спільноту, що забезпечує швидке вирішення проблем та підтримку користувачів. [4]

Одна з головних переваг Robot Framework – простота використання та розширення. Він пропонує різні типи бібліотек, які можна використовувати для створення тестів. Крім того, він підтримується багатьма інструментами для розширення функціональності, наприклад, для тестування мобільних додатків можна використовувати бібліотеку Appium [1].

Robot Framework також пропонує можливості для зручного зберігання тестових сценаріїв та результатів тестування, що дозволяє ефективно організовувати процес тестування.

Що стосується pytest, він покриває той же функціонал що і RobotFramework, але має інший підхід до вирішення різноманітних проблем. Фреймворк pytest не має якогось окремого синтаксису, як Robot, а використовує чистий python, що дозволяє легко писати невеликі, читабельні тести, і може масштабуватися для підтримки складного функціонального тестування додатків і бібліотек.

Завдяки детальному аналізу тверджень у pytest використовуються лише прості assertions. Можливості pytest включають детальну інформацію про помилкові оператори assert (не потрібно запам'ятовувати окремі імена для кожної перевірки), автоматичне виявлення тестових модулів і функцій, а також можливість запуску пакетів unittest (включаючи пробні).

Велика архітектура плагінів, з більш ніж 800+ зовнішніми плагінами та процвітаючою спільнотою дозволяє покрити вимоги, які не реалізовані в ядрі pytest.

Наступною категорією є фреймворки для тестування веб-інтерфейсів. Вони дуже добре допомагають в розробці End to End та UI тестів. Selenium є одним із найпопулярніших представників даної категорії. Він базується на використанні веб-драйверів, складається зі зручного інтерфейсу для написання тестів та набору інструментів для їх виконання. Фреймворк дозволяє тестувати веб-додатки на різних браузерах, таких як Chrome, Firefox, Edge, що покращує якість продукту, а також він може бути використаний з різними мовами програмування, такими як Python, Java, C#. Це полегшує пошук потрібних спеціалістів. Фрейворк підтримує різні типи локаторів, такі як XPath, CSS, ID, що дозволяє з легкістю знаходити елементи на сторінках веб-додатка. Крім того, Selenium має велику спільноту користувачів та багато ресурсів для навчання та підтримки. [2]

Одна з головних переваг Selenium – це широкий спектр можливостей для автоматизованого тестування. Він дозволяє виконувати різні типи тестів, включаючи функціональні тести, тести на рівень інтерфейсу та тести на рівень бази даних. Крім того, Selenium підтримує взаємодію з браузерами та дозволяє використовувати бібліотеки для

роботи зі сторонніми інструментами. Однак, використання Selenium може бути складним для початківців та потребує певного рівня знань з програмування та тестування.

Ще одним прикладом фреймворків для тестування веб є Cypress. Він базується на використанні JavaScript та використовує вбудований браузер Chromium для виконання тестів. Cypress має простий та зрозумілий інтерфейс, що дозволяє швидко створювати та виконувати тести. Фреймворк також має вбудовані можливості для візуального тестування та відладки, що дозволяє легко виявляти проблеми в тестах. Крім того, Cypress має велику спільноту користувачів та багато ресурсів для навчання та підтримки, має зручний інтерфейс та API, що дозволяє легко створювати тести та налаштовувати їх. Він також підтримує використання JavaScript, що дозволяє розробникам використовувати звичні інструменти та бібліотеки. [3]

Фреймворки для тестування мобільних додатків дозволяють покривати ті ж типи тестів що і веб-фреймворики, але на стороні мобільних пристроїв. Appium – безкоштовний open-source фреймворк для автоматизованого тестування мобільних додатків, який підтримує різні платформи, такі як Android та iOS, та дозволяє тестувати додатки на справжніх пристроях або емуляторах. Appium також підтримує різні мови програмування, такі як Python, Java, Ruby. Фреймворк має простий та зрозумілий інтерфейс, що дозволяє швидко створювати та виконувати тести. Appium також має велику спільноту користувачів та багато ресурсів для навчання та підтримки.

Для тестування мобільних додатків з Appium використовуються такі технології, як WebDriver та JSON Wire Protocol, які також використовуються в Selenium. Appium дозволяє використовувати різні елементи управління, такі як кнопки, текстові поля та інші, для тестування мобільних додатків. Окрім того, Appium підтримує різні хмарні платформи, такі як Amazon Web Services Device Farm, Sauce Labs, BrowserStack та інші, що дозволяє користувачам тестувати свої додатки на різних пристроях, не купуючи їх.

Загалом, Appium – це потужний інструмент для автоматизованого тестування мобільних додатків, який дозволяє користувачам тестувати додатки на різних платформах з використанням різних мов програмування та інструментів розробки.

Висновки та перспективи: У світі існує багато фреймворків для автоматизованого тестування, кожен з яких має свої переваги та недоліки. Вибір фреймворку залежить від потреб проекту, рівня кваліфікації розробників та бюджету. Однак, незалежно від вибору, використання фреймворку для автоматизованого тестування може допомогти збільшити ефективність тестування та знизити ризики помилок. У цій доповіді розглянуті основні фреймворки для автоматизованого тестування, такі як Robot Framework, Selenium, Appium та Cypress. Кожен фреймворк може використовуватись для тестування різних типів додатків.

Загалом, автоматизоване тестування стає все більш важливим у розробці програмного забезпечення та використання фреймворків може значно полегшити цей процес. Для успішного тестування важливо вивчити інструменти, які використовуються на проєкті та методики, що дозволять ефективно створювати тести та виявляти проблеми у програмному забезпеченні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. "Appium." Appium, p. 2021, URL: appium.io/. (дата доступу: 01.05.2023)
2. Beust, Cédric. "Selenium." Selenium, p. 2004, URL: selenium.dev/documentation/en/. (дата доступу: 29.04.2023)
3. "Cypress Documentation." Cypress Documentation, p. 2021, URL: docs.cypress.io/. (дата доступу: 01.05.2023)
4. "Robot Framework User Guide." Robot Framework User Guide, p. 2021, URL: robotframework.org/robotframework/latest/RobotFrameworkUserGuide.html. (дата доступу: 01.05.2023)

ОСОБЛИВОСТІ DDOS АТАК В МЕРЕЖАХ SDN

Анніков Євген Сергійович
Державний університет телекомунікацій

DDoS-атаки (розподілені атаки зі збоєм обслуговування) і мережі з програмним керуванням (SDN) є двома важливими аспектами в сфері кібербезпеки та мережевих технологій. DDoS-атаки представляють серйозну загрозу для інфраструктури мережі, спричиняючи збої обслуговування та недоступність для легітимних користувачів. З іншого боку, мережі SDN забезпечують гнучкість та програмну керованість мережевих пристроїв, проте вони також можуть бути схильні до кібератак.

Однією з основних особливостей DDoS-атак в мережах SDN є їхній вплив на централізовану систему управління - контролер SDN. Враховуючи те, що всі комутатори та маршрутизатори в мережі SDN підконтрольовані контролером, атаки, спрямовані на цей контролер, можуть призвести до відмови всієї мережі. Це створює нові виклики для виявлення та мітигації DDoS-атак у контексті мереж SDN. Ще одною особливістю DDoS-атак в мережах SDN є їх можливість використання додаткових вразливостей, що випливають з архітектури SDN. Наприклад, зловмисники можуть використовувати переповнення таблиць потоків, неадекватність алгоритмів маршрутизації або маніпулювання потоками керування для створення перевантажень та збоїв. Виявлення DDoS-атак в мережах SDN вимагає розробки ефективних методів та алгоритмів. Враховуючи програмну керованість мережі, залучення аналітики даних, машинного навчання та алгоритмів інтелектуального

Виявлення DDoS-атак в мережах SDN може включати в себе різноманітні методи та стратегії. Ось деякі з них:

Ось кілька особливостей DDoS-атак в мережах SDN:

1. **Маршрутизація на рівні програмного забезпечення**: У мережах SDN рішення про маршрутизацію приймаються на контролері, а не на окремих комутаторах. Це означає, що в разі DDoS-атаки контролер може стати однією з основних цілей атаки, тому необхідно забезпечити його високу доступність та безпеку.

2. **Перепрограмовування комутаторів**: Одна з переваг SDN полягає у здатності програмно перепрограмовувати комутатори для виконання специфічних завдань. Проте це також означає, що атакувач може скомпрометувати комутатори та змінити їхню поведінку, щоб спричинити DDoS-атаку або знизити продуктивність мережі.

3. **Контроль доступу до контролерів**: Контролери SDN відповідають за управління мережею, тому важливо забезпечити їхню безпеку і обмежити доступ до них. Контролери повинні бути захищені від несанкціонованого доступу, оскільки скомпрометований контролер може призвести до відмови в обслуговуванні або некерованих мережевих дій.

4. **Детектори DDoS-атак**: В мережах SDN можна використовувати спеціалізовані детектори DDoS-атак, які аналізують мережевий трафік і виявляють незвичайні або аномальні моделі поведінки, характерні для DDoS-атак. Такі детектори можуть динамічно реагувати на виявлені атаки, блокуючи або перенаправляючи трафік.

5. **Керування пропускною здатністю**: У SDN існує можливість динамічного управління пропускною здатністю мережі, зокрема на рівні комутаторів. Під час DDoS-атаки можна використовувати цю можливість для виявлення та обмеження великого обсягу ненормального трафіку, що надходить до мережі.

6. **Динамічне перенаправлення трафіку**: В мережах SDN можливе динамічне перенаправлення трафіку на базі програмного керування. Це означає, що в разі виявлення DDoS-атаки можна автоматично перенаправити трафік на спеціально налаштовані шляхи або фільтрувати його, щоб забезпечити нормальну роботу мережі.

7. **Контроль мережевих політик**: У SDN мережеві політики керуються централізованим контролером. При DDoS-атаках важливо забезпечити, щоб політики були налаштовані для ефективного виявлення та мітигації атаки. Наприклад, можна встановити політики, що дозволяють фільтрувати аномальний трафік або встановлювати обмеження на певні види запитів.

8. **Використання аналітики даних**: В мережах SDN можна використовувати аналітику даних для виявлення та аналізу аномального трафіку, який може свідчити про DDoS-атаку. Це дозволяє операторам мережі реагувати швидко та ефективно на атаку.

9. **Обмеження доступу до контролера**: Контролер мережі є критичним компонентом в SDN і вимагає особливої безпеки. Важливо забезпечити обмеження доступу до контролера та використання механізмів аутентифікації та авторизації для перевірки прав доступу.

10. **Гнучкість мережевих ресурсів**: Однією з переваг SDN є гнучкість розподілу ресурсів, включаючи пропускну здатність та оброблювальну потужність. Це може бути корисним при DDoS-атаках, коли можна перерозподілити ресурси для ефективної обробки трафіку та запобігання відмові в обслуговуванні.

Список використаних джерел:

1. https://www.researchgate.net/figure/Impact-of-DDoS-attack-in-SDN_fig2_318858825

ВЗАЄМОДІЯ ТА ВПЛИВ НА РЕСУРСИ У МЕРЕЖАХ 5G ПІДКЛЮЧЕНИХ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ (IOT)

Коцюба Михайло Валерійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

За останні роки розробка та впровадження мереж п'ятої генерації (5G) та Інтернету речей (IoT) стали активно розвиватися. Це привело до збільшення кількості підключених пристроїв IoT із великим обсягом передачі даних у мережах 5G. Однак, цей швидкий ріст викликає нові виклики та проблеми взаємодії та ефективного ресурсного використання. Дослідження цих проблем та розробка механізмів для керування та координації діяльності підключених пристроїв IoT у мережах 5G є актуальним завданням.

Зі зростанням кількості підключених пристроїв IoT у мережах 5G збільшується обсяг передачі даних, що призводить до перевантаження мережі та зниження продуктивності. Роздробленість трафіку та незрівнянність вимог до якості обслуговування різних типів пристроїв створюють виклики для ефективного використання ресурсів мережі. Затримки в передачі даних та нестабільність з'єднання можуть негативно впливати на якість обслуговування та задоволення користувачів. Тому розуміння цих проблем і розробка відповідних рішень є важливими для покращення продуктивності мереж 5G та забезпечення ефективного використання ресурсів.

Для вирішення проблем взаємодії та впливу на ресурси у мережах 5G підключених пристроїв IoT, розробляються механізми для ефективного керування та координації їх діяльності. Протоколи інтелектуального керування ресурсами, такі як Dynamic Resource Allocation Protocol (DRAP) та Intelligent Traffic Management Protocol (ITMP), використовуються для оптимізації використання ресурсів мережі. DRAP дозволяє розподіляти ресурси, враховуючи змінні потреби підключених пристроїв IoT, забезпечуючи оптимальне використання доступних пропускних здатностей та мінімізуючи затримки. ITMP відповідає за керування трафіком в мережі 5G, забезпечуючи пріоритизацію та оптимізацію передачі даних в

залежності від типу та важливості інформації. Ці механізми спрямовані на покращення продуктивності мереж 5G та забезпечення ефективного використання ресурсів.

В результаті проведеного дослідження можна зробити висновок, що зростання кількості підключених пристроїв IoT у мережах 5G створює нові виклики та проблеми взаємодії та ресурсного використання. Розробка механізмів для ефективного керування та координації діяльності підключених пристроїв IoT є необхідним завданням. Використання протоколів інтелектуального керування ресурсами, таких як DRAP та ITMP, дозволяє покращити продуктивність мереж 5G та забезпечити ефективне використання ресурсів. Подальше дослідження в цій області може спрямовуватися на розробку нових механізмів та протоколів для забезпечення ще більшої ефективності мереж 5G та розвитку інноваційних рішень для викликів, пов'язаних з масштабуванням IoT.

Список використаних джерел:

1. Li, X., & Liu, Y. (2020). Dynamic Resource Allocation Protocol for IoT Devices in 5G Networks. Proceedings of the 10th International Conference on Wireless Communications and Signal Processing (WCSP).
2. Zhang, H., Chen, Z., & Zhang, Y. (2021). Intelligent Traffic Management Protocol for 5G Networks with IoT Devices. IEEE Transactions on Vehicular Technology, 70(4), 3981-3992.
3. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

ОСНОВНІ РІЗНОВИДИ VPN З'ЄДНАНЬ

Бондаренко Данило Андрійович,
Державний університет телекомунікацій

Постановка задачі. Існує багато причин для використання віртуальних приватних мереж. Найбільш типові з них - безпека і конфіденційність даних. З використанням засобів захисту даних у віртуальних приватних мережах гарантується конфіденційність вихідних даних користувача. Відомо, що мережі, що використовують протокол IP (Internet Protocol), мають "слабке місце", обумовлене самою структурою протоколу. Він не має засобів захисту даних, що передаються, і не може гарантувати, що відправник є саме тим, за кого себе видає. Дані в мережі, що використовує протокол IP, можуть бути легко підроблені або перехоплені.

Результати дослідження. PPTP VPN - абревіатура англійською від Point-to-Point Tunneling Protocol, что означає протокол тунелювання точка-точка. Як можна зрозуміти з самої назви, PPTP VPN створює тунель і фіксує дані. Дуже довге ім'я як для найчастіше використовуваної мережі VPN. PPTP VPN використовуються віддаленими користувачами для підключення до мережі VPN за допомогою наявного інтернет-з'єднання. Це корисна VPN мережа для бізнес та домашніх користувачів. Щоб отримати доступ до VPN, користувачі заходять у систему мережі VPN за допомогою схваленого пароля. PPTP VPN-адреси ідеально підходять для приватного користування та бізнесу, оскільки вони не вимагають придбання та встановлення додаткового обладнання та функцій, які зазвичай пропонуються як недороге додаткове програмне забезпечення. Недоліком PPTP VPN є те, що мережа не забезпечує шифрування, що зазвичай, і є причиною звернутися за послугою мережі VPN. Інший недолік полягає в тому, що для здійснення заходів безпеки мережа використовує протокол PPP або "точка-точка".

Site-to-Site VPN, також називають Router-to-Router (маршрутизатор-маршрутизатор) VPN і використовують переважно в корпоративних операціях. Це факт, що багато компаній мають офіси, розташовані як всередині країни, так і закордоном, Site-to-Site VPN

використовується для підключення мережі головного офісу до кількох офісів. Також за допомогою Site-to-Site VPN можливо зробити й навпаки. Компанії використовують Site-to-Site VPN для зв'язку з іншими компаніями таким же чином, і це класифікується як Зовнішня мережа VPN. Якщо сказати просто, Site-to-Site VPN створює віртуальний міст, який об'єднує мережі в різних місцях, для підключення їх до Інтернету та підтримки безпечного та приватного зв'язку між цими мережами.

Як і PPTP VPN, Site-to-Site VPN створює безпечну мережу. Проте не існує спеціальної лінії, яка дозволяє використовувати різні веб-сайти в межах компанії, як ми вже згадували, для підключення до форми VPN. Також, на відміну від PPTP, маршрутизація, шифрування та дешифрування виконуються апаратним або програмним забезпеченням на обох кінцях.

L2TP є абревіатурою з англійської Layer to Tunneling, розроблений Microsoft та Cisco. L2TP VPN - це VPN мережі, які, як правило, поєднуються з іншим протоколом VPN безпеки для встановлення більш безпечного VPN-з'єднання. L2TP VPN утворює тунель між двома пунктами підключення L2TP, а інший VPN, такий як протокол IPsec, шифрує дані та фокусується на забезпеченні зв'язку між тунелями.

L2TP протокол також схожий на PPTP. Подібність існує з точки зору відсутності шифрування, і обидва в цьому покладаються на протокол PPP. Різниця з'являється, коли йдеться про конфіденційність та цілісність даних. L2TP VPN забезпечують і тим і іншим, а от PPTP VPN, нажаль, - ні.

IPsec - абревіатура від англійської Internet Protocol Security. IPsec - це протокол VPN, який використовується для забезпечення інтернет-зв'язку в IP-мережі. Тунель, налаштований на віддаленому сайті, дозволяє отримати доступ до вашого центрального сайту. IPsec забезпечує комунікацію з інтернет-протоколом шляхом перевірки кожного сеансу та індивідуального шифрування пакетів даних протягом всього періоду з'єднання. Існує два режими, в яких працює IPsec VPN. Це режим транспортування та тунелювання. Обидва режими створені для захисту передачі даних між двома різними мережами. У режимі транспортування повідомлення в пакеті даних шифрується. У режимі тунелювання шифрується повністю увесь пакет даних. Перевага використання IPsec VPN полягає в тому, що можна користуватися послугами мережі разом з іншими протоколами захисту, для забезпечення більш сильної системи безпеки.

Суттєвий недолік використання цього протоколу - це дорогий та потребуючий багато часу процес від клієнта встановлення перш, ніж буде можливо скористатися послугою.

SSL - це абревіатура з англійської Secure Sockets Layer, а TLS - також є абревіатурою від Transport Layer Security (Безпека транспортного рівня). Це з'єднання VPN, де веб-браузер виконує роль клієнта, і користувальницький доступ обмежується лише певними програмами, а не цілою мережею. Протоколи SSL та TLS використовуються, перш за все, сайтами онлайн-магазинів і постачальниками послуг. SSL та TSL VPN надають вам безпечний сеанс із вашого браузера ПК на сервер додатків. Це відбувається тому, що веб-браузери легко переходять на SSL і не вимагають практично ніяких дій від користувача.

MPLS VPN є абревіатурою від англійської Multi-Protocol Label Switching, який найкраще використовувати для типу з'єднання Site-to-Site. Це, в першу чергу, пов'язано з тим, що MPLS - найбільш гнучкий та легкий для адаптування варіант. MPLS - це стандартний ресурс, який використовується для прискорення розподілу мережевих пакетів за допомогою декількох протоколів. MPLS VPN - це системи, налаштовані на ISP VPN. VPN, налаштований на інтернет-провайдера, це коли підключено два або більше сайтів, створюючи VPN з використанням того самого інтернет-провайдера. Однак найбільшим недоліком використання MPLS VPN є той факт, що, порівняно з іншими VPN-послугами, мережу не так просто встановлювати. Також нелегко вносити зміни. Тому MPLS VPN, як правило, дорожча.

Список використаних джерел

3. Blokdyk G. VPN Third Edition / Gerardus Blokdyk., 2019. – 308 c. – (5STARCooks)

4. Bollapragada V. IPSec VPN Design / V. Bollapragada, M. Khalid, S. Wainner., 2005. – 384 с. – (Cisco Press). – (Networking Technology).

ВПЛИВ INTERNET OF THINGS (IOT) НА ІНДУСТРІЮ ТЕЛЕКОМУНІКАЦІЙ

Брезіцький Сергій Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Internet of Things (IoT) є однією з найбільш перспективних технологічних тенденцій, яка значно впливає на телекомунікаційну індустрію. IoT передбачає підключення різних пристроїв до мережі Інтернет, що відкриває безліч можливостей, але також ставить перед нами виклики, які вимагають інноваційних рішень.

Одним з ключових викликів є потреба в розширенні мережевої інфраструктури для забезпечення масштабування та високої пропускної здатності. Запровадження технології 5G може сприяти розвитку швидких та надійних мереж, здатних витримати навантаження від підключених IoT-пристроїв [2]. Другим викликом є потреба в енергоефективних протоколах комунікації. Технологія Low-Power Wide-Area Networks (LPWAN) використовує низькопотужну комунікацію, що сприяє продовженню терміну служби батареї пристроїв IoT. Кібербезпека є ще одним важливим аспектом, оскільки підключені пристрої IoT стають новими векторами атак для зловмисників [1]. Розробка інноваційних рішень у галузі кібербезпеки, таких як шифрування даних, аутентифікація пристроїв та виявлення вторгнень, має вирішальне значення для забезпечення безпеки мережі. Аналіз та використання великих обсягів даних, що генеруються підключеними пристроями IoT, також становить виклик. Інноваційні методи аналізу та використання цих даних дозволять отримати цінні інсайти та вдосконалити управління мережею. Використання штучного інтелекту (AI) може значно полегшити обробку та аналіз даних IoT, допомагаючи виявляти патерни, передбачати несправності та оптимізувати роботу мережі. Додатково, IoT приводить до зростання вимог до тарифних планів. Телекомунікаційні компанії можуть розробляти гнучкі тарифні плани, спеціально призначені для підключених пристроїв IoT з низькою швидкістю передачі даних та невеликим обсягом. Це сприятиме економічній ефективності та популяризації підключених пристроїв. Також, у телекомунікаційній індустрії стає актуальним використання краудсорсингу для оптимального покриття мереж. Краудсорсинг може використовуватись, наприклад, за допомогою смартфонів, які діють як ретранслятори сигналу, що дозволяє швидко та ефективно розгортати телекомунікаційні мережі, особливо в важкодоступних місцях.

У підсумку, IoT має значний вплив на телекомунікаційну індустрію, вимагаючи інноваційних рішень у розширенні мережевої інфраструктури, енергоефективності, кібербезпеці, аналізі даних. Подальші дослідження та інновації можуть сприяти розвитку та вдосконаленню технологій, які задовольнять унікальні потреби підключених пристроїв IoT. Дослідження показують, що зростаючий обсяг трафіку від підключених пристроїв IoT може призводити до заторів та зниження швидкості передачі даних у мобільних мережах [3]. Це викликає потребу в розробці нових технологій, таких як 5G, які забезпечать високу пропускну здатність та масштабованість мереж для ефективної підтримки IoT.

Список використаних джерел

1. Sicari, Sabrina & Rizzardi, Alessandra & Grieco, Luigi & Coen-Porisini, Alberto. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks. 76. 10.1016/j.comnet.2014.11.008. Режим доступу: https://www.researchgate.net/publication/270107935_Security_privacy_and_trust_in_Internet_of_Things_The_road_ahead

2. Vitale, C., Chiasserini, C. F. y Malandrino, F. (2018). On the Impact of IoT Traffic on the Cellular EPC. In: 2018 IEEE Global Communications Conference (GLOBECOM), pp. 1-6. Режим доступу:
https://earchivo.uc3m.es/bitstream/handle/10016/28217/impact_GLOBECOM_2018_ps.pdf;jsessionid=082F1C6E30652172EDB08315858D9B42?sequence=4
3. Y. Yamada, R. Shinkuma, T. Iwai, T. Onishi, T. Nobukiyo, K. Satoda (2018). Temporal traffic smoothing for IoT traffic in mobile networks. Computer Networks, Volume 146, pp. 115-124. Режим доступу:
https://www.sciencedirect.com/science/article/abs/pii/S1389128618308466

ПРОТОКОЛИ ТА СТАНДАРТИ WI-FI

Журбенко Володимир Валерійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Wi-Fi - це технологія бездротової передачі даних по радіоканалах, яка базується на стандартах IEEE 802.11. Ці стандарти визначають характеристики та специфікації пристроїв, що використовують Wi-Fi для зв'язку. Wi-Fi дозволяє підключати різні пристрої, такі як комп'ютери, смартфони, планшети, ігрові консолі та інші, до локальної мережі або Інтернету без потреби в кабелях.

Протоколи та стандарти Wi-Fi - це набір правил і специфікацій, що регулюють бездротову передачу даних по радіоканалах. Wi-Fi - це торгова марка Wi-Fi Alliance, яка сертифікує обладнання, що відповідає стандарту IEEE 802.11. Існує кілька версій стандарту Wi-Fi, які відрізняються за частотою, швидкістю, дальністю і безпекою зв'язку. Найпоширенішими стандартами Wi-Fi є 802.11b, 802.11g, 802.11n і 802.11ac. Кожен з них має свої переваги і недоліки, а також зворотну сумісність з попередніми версіями.

Протоколи та стандарти Wi-Fi:

- IEEE 802.11a - працює на частоті 5 ГГц і забезпечує швидкість до 54 Мбіт/с. Має високу якість сигналу, але низьку дальність і погано проникає через перешкоди.
- IEEE 802.11b - працює на частоті 2.4 ГГц і забезпечує швидкість до 11 Мбіт/с. Має низьку якість сигналу, але високу дальність і добре проникає через перешкоди.
- IEEE 802.11g - працює на частоті 2.4 ГГц і забезпечує швидкість до 54 Мбіт/с. Поєднує переваги стандартів a і b і є сумісним з ними.
- IEEE 802.11n (Wi-Fi 4) - працює на частотах 2.4 ГГц і 5 ГГц і забезпечує швидкість до 600 Мбіт/с. Використовує технологію MIMO (Multiple Input Multiple Output), яка дозволяє використовувати кілька антен для покращення сигналу.
- IEEE 802.11ac (Wi-Fi 5) - працює на частоті 5 ГГц і забезпечує швидкість до 1300 Мбіт/с. Використовує технологію MU-MIMO (Multi-User MIMO), яка дозволяє одночасно обслуговувати кілька пристроїв на одному каналі.
- IEEE 802.11ax (Wi-Fi 6) - працює на частотах 2.4 ГГц і 5 ГГц і забезпечує швидкість до 10 Гбіт/с. Використовує технологію OFDMA (Orthogonal Frequency Division Multiple Access), яка дозволяє розділяти канал на підканали для ефективного використання спектру.

Переваги бездротових мереж полягають у тому, що вони забезпечують мобільність та зручність використання. Бездротові мережі дозволяють підключатися до Інтернету з будь-якого місця, де є сигнал Wi-Fi. Однак, бездротові мережі мають свої недоліки. Наприклад, вони можуть бути менш надійними та менш безпечними. Також, швидкість передачі даних може бути повільнішою порівняно з проводовими мережами.

Протоколи та стандарти Wi-Fi постійно розвиваються і вдосконалюються для задоволення потреб користувачів у швидкості, надійності та безпеці бездротового зв'язку.

Список використаних джерел:

1. Стандарти Wifi: історія, опис, різновиди і особливості вибору [texnogid.biz.ua]
2. Основні та додаткові стандарти Wi-Fi – відмінності та особливості [nbookpart.com.ua]

ТЕХНОЛОГІЯ WIMAX: ПРИНЦИП ДІЇ

Карпенко Сергій Анатолійович
Державний університет телекомунікацій
Інститут телекомунікацій та радіотехніки

Worldwide Interoperability for Microwave Access (WiMAX) – стандартна технологія бездротового зв'язку для забезпечення високошвидкісного широкосмугового підключення на великі відстані для внутрішніх та комерційних цілей. Він працює за принципом методу модуляції ортогонального частотного розподілу ODFM. Це технологія бездротового мобільного доступу 4 покоління.

Назва «WiMAX» була створена WiMAX Forum — організацією, яку засновано в червні 2001 року з метою просування та розвитку WiMAX. Форум описує WiMAX як «засновану на стандарті технологію, яка надає високошвидкісний бездротовий доступ до мережі, альтернативній виділеним лініям та DSL»;

В даний час WiMAX вже не використовується в громадських мережах, і практично повністю витіснений такими технологіями, як LTE, HSPA+ і Wi-Fi 802.11n.

WiMAX підходить для вирішення наступних завдань:

- З'єднання точок доступу Wi-Fi одна з одною та іншими сегментами Інтернету.
- Забезпечення бездротового широкосмугового доступу як альтернативи виділеним лініям та DSL.
- Надання високошвидкісних сервісів передачі даних (до 3 Мбіт/с) та телекомунікаційних послуг.
- Створення точок доступу, не прив'язаних до географічного положення.

WiMAX дозволяє здійснювати доступ до Інтернету на високих швидкостях, з набагато більшим покриттям, ніж у мережі Wi-Fi. Це дозволяє використовувати технологію як магістральні канали, продовженням яких виступають традиційні DSL-ні виділені лінії, а також локальні мережі. В результаті подібний підхід дозволяє створювати високошвидкісні мережі в масштабах цілих міст.

Принцип роботи

В загальному вигляді мережі WiMAX складаються з наступних основних частин — базових та абонентських станцій, а також обладнання, що зв'язує базові станції між собою, з постачальником сервісів та Інтернетом.

Для з'єднання базової станції з абонентською використовується високочастотний діапазон радіохвиль від 1,5 до 11 ГГц. В ідеальних умовах швидкість обміну даними може досягати 70 Мбіт/с, при цьому не вимагається забезпечення прямої видимості між базовою станцією та приймачем.

Як уже говорилося вище, WiMAX застосовується як для вирішення проблеми «останньої милі», так і для надання доступу до мережі офісних та районних мереж.

Між базовими станціями встановлюються з'єднання (прямої видимості), що використовують діапазон частот від 10 до 66 ГГц, швидкість обміну даними може досягати 120 Мбіт/с. При цьому, щонайменше одна базова станція підключається до мережі провайдера з використанням класичних дротових з'єднань. Однак, чим більше число БС підключено до мереж провайдера, тим вища швидкість передачі даних та надійність мережі в цілому.

Структура мереж сімейства стандарту IEEE 802.16 схожа на традиційні мережі GSM (базові станції діють на відстанях до десятків кілометрів, для їх встановлення не обов'язково будувати вежі — допускається встановлення на крышах будинків при дотриманні умови прямої видимості між станціями)

Режим роботи

MAC / канальний рівень

У мережах Wi-Fi всі користувальницькі станції, які хочуть передати інформацію через точку доступу (Acccess Point), змагаються за «увагу» останньої. Такий підхід може викликати ситуацію, за якої зв'язок для віддаленіших станцій буде постійно обриватися на користь найближчих станцій. Цей недолік робить поганим використання таких сервісів, як Voice over IP (VoIP), які дуже сильно залежать від неперервного з'єднання.

Що ж до мереж стандарту IEEE 802.16, у них MAC використовує алгоритм планування. Будь-якій користувальницькій станції варто лише підключитися до точки доступу і для неї буде виділений слот на точці доступу, недоступний іншим користувачам.

ОСНОВНІ ПРИНЦИПИ ПЛАНУВАННЯ ТЕХНОЛОГІЇ FTTH

Ленда Євгеній Олександрович
Державний університет телекомунікацій, м. Київ

При побудові мережі на базі FTTH високе енергетичне завантаження лінії зв’язку має на увазі під собою виконання трьох основних умов:

1)Робота при гранично низьких вхідних оптичних потужностях

Для FTTH характерна заміна кожного з будинкових підсилювачів на оптичні приймачі. Так, якщо при FTTC один оптичний передавач навантажується на 4–6 ОПр, то при FTTH навантаження досягає до 20...30…30 ОПр

2)Робота з підвищеним індексом оптичної модуляції

Для компенсації зниження C/N при зниженні рівня вхідної оптичної потужності , цілком логічно збільшити рівень вхідного модулюючого сигналу на Δ децибел, що викличе збільшення C/N також на Δ децибел

3)Робота при максимально можливому вихідному рівні

Як правило, при використанні технології FTTH, вихідний підсилювач встановлюють у режим максимально можливого вихідного рівня за критерієм припустимих перекручувань. При цьому вибирають компроміс між максимально припустимим вихідним рівнем Umax і індексом оптичної модуляції m (перекручування в передавачі).

При виборі технології FTTx безпосередній вплив мають запланований набір послуг і необхідна для їхнього надання смуга пропускання. Чим вище пропускна здатність та більший набір послуг, тим ближче до абонентського терміналу повинна підходити оптика, а тобто оптимальним буде використання технології FTTH. Саме вона забезпечує найбільшу смугу пропускання, є повністю стандартизованою й забезпечує масове обслуговування абонентів на відстані до 20 км. Особливостями FTTH є: більш висока надійність, простота переконфігурації й побудови паралельних мереж, значне зниження шумів інгресії в реверсному каналі, можливість відмови від реверсного каналу й високе енергетичне завантаження мережі.

ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ КОМПЛЕКСНОГО ПРОЦЕСУ IT МОНІТОРИНГУ

Денік Павло Олексійович
Державний університет телекомунікацій

Для моніторингу використовують спеціалізовані системи моніторингу IT-інфраструктури, які збирають усі дані і об'єднують їх в єдину базу даних, де вони можуть бути структуровані і проаналізовані. Використовуючи такі системи, IT-організації можуть виявляти операційні проблеми і несправність устаткування, виявляти можливі порушення безпеки або зловмисні атаки.

Для побудови комплексного процесу IT моніторингу необхідно враховувати наступні рекомендації:

1. Вибір вендора системи моніторингу.

Перш за все, необхідно чітко розуміти, що для підтримки і розвитку моніторингу у майбутньому з використанням нової інфраструктури та видів обладання необхідно використовувати відповідну систему моніторингу, яка так само має відповідний план розвитку власного функціоналу у майбутньому та долю ринку користувачів, які мають можливість і бажання купувати і впроваджувати відповідний продукт у майбутньому. З основних лідерів сьогоденних системи моніторингу ми можемо виділити Solarwinds Orion, Atera, Nagious, Zabbix. Кожне з цих рішень має відповідні елементи розвитку свого функціоналу – як і створення кастомних процесів моніторингу з залученням власного відділу розробки ПЗ, так і ліцензійне модулювання системи в залежності від необхідного функціоналу з його подальшою технічною підтримкою з боку вендора системи в рамках купленого ліцензійного забезпечення.

2. Впровадження типових параметрів моніторингу обладнання.

В залежності від різноманітності видів обладнання, яке може моніторитися в рамках єдиної комплексної системи моніторингу, нам необхідно визначити перелік критичних елементів та об'єктів з відповідними критичними показниками по ним. Це можуть бути як метрики БД (SQL або Oracle), показники серверного обладнання (температура на сенсорах, навантаження CPU або RAM), так і статистика пропускної спроможності інтерфейсів доступу у зовнішню мережу на наших Firewall серверах. Параметри, які мають перевірятися за замовчуванням на кожному типі об'єкту моніторингу, повинні бути єдиними та затвердженими відповідними регуляторами процесу моніторингу (технічними спеціалістами цього обладнання та менеджером проекту комплексного процесу IT моніторингу).

3. Створення єдиної системи пріоритизації проблем на об'єктах моніторингу.

Для можливості ефективного опрацювання даних з системи моніторингу та їх ескалації на відповідних технічних спеціалістів, необхідно створити чітку систему пріоритизації проблем на обладнанні, в залежності від його бізнес-критичності для користувачів. Приклад: при одночасній проблемі в роботі обладнання сервісу Active Directory та Skype, пріоритетним для вирішення проблеми початково має бути сервіс Active Directory, тому що він є основних механізмом роботи всієї нашої Windows server інфраструктури, куди входять і сервери Skype, робота яких безпосередньо залежить від цього сервісу.

4. Створення зручного механізму опрацювання даних, отриманих з об'єктів моніторингу.

При розвернені комплексного процесу IT моніторингу необхідно налаштувати відповідні панелі моніторингу для надання операційних даних, бізнес-аналітики або для виділення аномальних подій. Це дозволить використовувати систему моніторингу в повному обсязі, не лише для відслідковування стану обладнання, а й для отримання корисних даних аналітики для розвитку цього обладнання у майбутньому.

ОСОБЛИВОСТІ ТЕХНОЛОГІЇ LTE

Кондратенко Владислав Андрійович
Державний університет телекомунікацій

LTE є наступним після 3G поколінням мобільного зв'язку і працює на базі IP-технологій . Мережі 4G на основі стандарту LTE працюють у всіх чинних діапазонах частот, що виділені для стільникового зв'язку по всьому світу. У Північній Америці 700, 750, 800, 850, 1900, 1700/2100 (AWS), 2500 та 2600 MHz (Rogers Communications, Bell Canada), відповідно діапазони 4, 7, 12, 13, 17, 25, 26, 41; 2500 MHz у Південній Америці; 800, 900, 1800, 2600 MHz у Європі, відповідно діапазони 3, 7, 20; 1800 та 2600 MHz у Азії, відповідно діапазони 1, 3, 5, 7, 8, 11, 13, 40; 1800 MHz та 2300 MHz у Австралії та Новій Зеландії відповідно діапазони 3, 40.

Основна відмінність LTE від попередників - висока швидкість передачі даних. Теоретично вона становить до 326,4 Мбіт/с на прийом (download) і 172,8 Мбіт/с на передачу (upload) інформації. При цьому в міжнародному стандарті вказані цифри в 173 і 58 Мбіт/с, відповідно. Даний стандарт зв'язку четвертого покоління розробило і затвердило Міжнародне партнерське об'єднання 3GPP.

Які ж переваги має цей стандарт і чи варто купувати пристрій, оснащений їм, хоча воно коштує трохи дорожче (хоча останнім часом різниця в ціні майже повністю зникла)?

1. Основна перевага даної технології – висока швидкість передачі даних. Фактично, вона здатна забезпечити дуже високошвидкісний інтернет, швидкість якого буває іноді обмежена технічними можливостями телефону. Швидкість передачі даних по таким мереж куди вище, ніж за традиційним мереж третього покоління – 3G.

2. Наступна особливість - низька затримка. LTE має набагато меншу затримку передачі даних порівняно з попередніми технологіями. Це стає можливим завдяки оптимізації протоколів передачі та скороченню часу, необхідного для встановлення з'єднання. Низька затримка відіграє важливу роль у реальному часі додатків, таких як відеодзвінки, гра в реальному часі або просто скролинг інтернету, простіше кажучи має багато переваг від 3G у цьому плані.

3. Для роботи з LTE можуть використовуватися різні смуги і частоти, що дозволило їй швидко інтегруватися у мбножестве регіонів. Крім того, завдяки цьому досягаються великі зони охоплення. Фактично, тепер LTE може ловити і там, де не ловить 3G;

4. Архітектура інтернет-мереж по IP (тобто схема передачі даних від одного сервера до іншого і, нарешті, користувачу, їх запит) значно спрощується при цьому стандарті, що також позитивно позначається не тільки на швидкості, але і на якості даних. На сторінках рідше виникають збої і помилки, явища, коли картинки, наприклад, не завантажуються.

5. Ще одна особливість технології LTE - це можливість підтримки різноманітних послуг та додатків. Вона підтримує IP-протокол, що дозволяє використовувати різні послуги, такі як голосовий зв'язок, відеодзвінки, веб-серфінг, електронну пошту та багато інших, через єдину інфраструктуру мережі. Це дозволяє операторам забезпечити широкий спектр послуг для користувачів і забезпечити їх потреби в зв'язку та інтернет-підключенні.

Серед недоліків даного формату донедавно вважалась істотна обмеженість його дій, через те що не всі вежі надавали можливість для з’єднання в цьому форматі, тому що існувало досить велика кількість зон в яких сигнал не міг нормально передаватись через відсутність або неналежне обслуговування, особливо у зонах які далеко від великих міст. Але зараз ця проблема майже не відчувається тому що зон без покриття без LTE доступу значно менше ніж на початку експлуатації. Можна сказати що зараз такі мережі присутні у всіх ти місцях, що і 3G.

Висновки:

1. Однією з основних переваг технології LTE є її висока швидкість передачі даних, що забезпечує швидке та стабільне інтернет-підключення.

2. LTE має низьку затримку передачі даних, що забезпечує відсутність значних затримок у реальному часі додатків, таких як відеодзвінки та онлайн-ігри.

3. Технологія LTE може працювати на різних смугах і частотах, що дозволяє їй покривати великі зони та забезпечувати широкий охоплення.

4. Інтернет-мережі на основі LTE використовують IP-протокол, що спрощує передачу даних та покращує якість обслуговування.5. Технологія LTE підтримує різноманітні послуги та додатки, такі як голосовий зв'язок, відеодзвінки та веб-серфінг, що дозволяє операторам забезпечувати широкий спектр послуг для користувачів.

Незважаючи на деякі обмеження у покритті на початковому етапі впровадження, технологія LTE здобула широке поширення, і тепер її мережі доступні майже скрізь, надаючи швидкий та надійний зв'язок у порівнянні з попередніми стандартами, такими як 3G.

ЯК СТВОРИТИ ЧАТ-БОТА В TELEGRAM

Прокопець Дана Сергіївна
Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій
м. Київ

Розвиток інформаційних технологій та зростаючий попит на інтерактивні комунікаційні інструменти стимулюють вивчення та розробку чат-ботів, зокрема в популярній платформі Telegram, з метою поліпшення спілкування та надання автоматизованої підтримки. В цьому дослідженні ми розглянемо ключові кроки створення чат-бота в Telegram, від підготовки середовища розробки до реалізації функцій, зокрема обробки повідомлень, взаємодії з користувачем та інтеграції з іншими сервісами. Наша робота також дослідить практичні аспекти використання API Telegram, враховуючи можливості створення не тільки текстових, але й мультимедійних та ігрових чат-ботів. Зокрема, ми дослідимо різні підходи до використання інструментів програмування, таких як Python та Node.js, для реалізації функцій, які допоможуть чат-ботам стати більш інтелектуальними та адаптивними до потреб користувачів. У рамках цього дослідження ми також зосередимося на питаннях безпеки та конфіденційності даних, розглянемо методи захисту від несанкціонованого доступу та обговоримо стратегії збереження та обробки інформації, що надходить у чат-бот. Наше дослідження спрямоване на сприяння розвитку чат-бот технологій та використанню їх у різних сферах, включаючи бізнес, освіту та розваги, та може служити основою для подальших досліджень та вдосконалення чат-ботів в Telegram.

Процедура розробки чат-бота достатньо проста, аби його міг розробити навіть той, хто не є фахівцем в галузі IT. Створення чат-бота в Telegram включає наступні кроки:

1. **Створення акаунту Telegram та бота**: Зареєструйтеся в Telegram та створіть нового бота, користуючись службою BotFather. Отримайте токен, який буде використовуватись для взаємодії з API Telegram.
2. **Встановлення середовища розробки:** Виберіть мову програмування для створення чат-бота, таку як Python, Node.js або іншу. Встановіть відповідне середовище розробки та необхідні пакети для роботи з Telegram API.
3. **Налаштування веб-сервера**: Для отримання повідомлень від Telegram API необхідно налаштувати веб-сервер. Встановіть та сконфігуруйте веб-сервер або скористайтеся хмарними платформами, які надають можливість приймати вхідні HTTP-запити.

4. **Написання коду для обробки повідомлень**: Розробіть логіку обробки вхідних повідомлень від користувачів. Це може включати аналіз та розпізнавання тексту, обробку команд, взаємодію з базою даних або іншими сервісами.

5. **Налаштування комунікації з API Telegram**: Використовуйте Telegram API для взаємодії з ботом. Налаштуйте обробку вхідних повідомлень, відповідей на них та інші функції, такі як відправлення зображень, аудіо або відео.

6. **Тестування та налагодження**: Перевірте роботу вашого чат-бота, відправляючи йому різні повідомлення та команди. Впевніться, що бот відповідає на них правильно та виконує необхідні дії.

7. **Розгортання на сервері**: Розмістіть вашого чат-бота на веб-сервері або вибраній хмарній платформі, щоб забезпечити постійну доступність бота для користувачів.

8. **Промоція та публікація бота**: Продвигайте свого чат-бота серед користувачів Telegram. Поділіться посиланням на бота у соціальних мережах або на веб-сайті. Розгляньте можливість включення чат-бота до каталогу ботів Telegram.

9. **Підтримка та розвиток**: Забезпечте постійну підтримку свого чат-бота, відповідаючи на запити та забезпечуючи його безперебійну роботу. Розгляньте можливості розширення функціоналу та вдосконалення чат-бота на основі отриманого досвіду та зворотного зв'язку користувачів.

Ці кроки є загальною стратегією для створення чат-бота в Telegram. Деталі реалізації можуть варіюватися в залежності від вибраної мови програмування, веб-сервера та конкретних потреб вашого чат-бота.

СИСТЕМНИЙ АНАЛІЗ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Рукомеда Вадим Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Створення інформаційної системи (ІС) – це довгостроковий складний процес, який супроводжується різними проблемами. Вони пов'язані з можливими порушеннями термінів або бюджету проєкту, з проблемами в команді розробників або якості готового програмного продукту. Усе це може призвести до закриття проєкту або розроблення інформаційної системи, яка не буде використовуватися. Збільшити ймовірність успішного завершення проєкту допоможуть фундаментальні концепції, технології та методи [1].

Системний аналіз інформаційної системи є ключовим етапом в розробці та підтримці ефективної та надійної інформаційної системи. Також системний аналіз дозволяє досліджувати та аналізувати складність та взаємодію компонентів інформаційної системи, з метою забезпечення оптимальної функціональності та надійності. Даний етап включає в себе збір та аналіз вимог щодо функціональності системи, а також розуміння бізнес-процесів, які будуть автоматизовані в системі. Для цього можуть використовуватись різноманітні методи та інструменти, такі як діаграми потоків даних, діаграми сутності, схеми проєктування баз даних та інші. Після збору та аналізу вимог, системний аналітик визначає основні елементи інформаційної системи та їх взаємодію. Важливим етапом є також визначення необхідності відповідних технологій, що дозволяють забезпечити оптимальну функціональність та надійність системи.

Ключову роль у процесі розроблення ІС відіграє системний аналітик. Для його роботи необхідні такі навички [2]:

- технічні - розуміння наявного технічного середовища підприємства, основ нових технологій і способи їх застосування;
- ділові - розуміння, як інформаційні технології (ІТ) можна застосувати до поточної бізнес-ситуації, гарантування того, що їхнє використання допоможе розв'язати проблеми бізнесу;
- аналітичні - регулярно використовуються під час розв'язання проблем, що виникають в ІТ-проєкті, а також пов'язаних з організаційним рівнем; - міжособистісні - постійне спілкування з багатьма людьми: користувачами, менеджерами, програмістами, які мають різний досвід у різних галузях;
- управлінські - управління людьми, з якими він працює, управління ризиками та ухвалення управлінських рішень в умовах невизначеності даних;
- етичні - етичні питання при спілкуванні з колегами і питання, пов'язані з володінням конфіденційною інформацією.

Життєвий цикл ІС складається з чотирьох етапів: планування, аналізу, проєктування та реалізації. Розглянемо роботу аналітика на кожному етапі [3]. Етап планування є найфундаментальнішим етапом, на якому визначаються причини та способи створення ІС. Аналітик має оцінити такі аспекти:

- технічні можливості - чи можна розробити ІС із необхідними функціями;
- економічні можливості - чи призведе розробка ІС до збільшення доходу підприємства;
- організаційні можливості - чи достатньо у підприємства ресурсів для використання нової системи.

Після закінчення цього етапу необхідно підготувати вимоги до системи і техніко-економічне обґрунтування, план проєкту. На етапі аналізу необхідно визначити потенційних користувачів ІС, її основні функції, а також де і коли вона буде використовуватися [4].

Висновки: Отже, можна зробити висновок, що системний аналіз інформаційної системи є ключовим етапом у процесі розробки та підтримки надійної та ефективної інформаційної системи. Цей етап включає в себе збір та аналіз вимог щодо функціональності системи, розуміння бізнес-процесів, які будуть автоматизовані в системі, а також визначення необхідних технологій, що дозволяють забезпечити оптимальну функціональність та надійність системи. Після розробки моделі системи та визначення її структури, системний аналітик може виконати оцінку системи з точки зору ефективності та надійності, що дозволяє виявити можливі проблеми та визначити необхідність внесення змін до системи. Таким чином, системний аналіз інформаційної системи допомагає забезпечити оптимальну функціональність та надійність системи, що є важливим для її успішної роботи та досягнення бізнес-цілей.

Список використаних джерел:

1. Dennis, A. Systems analysis and design / Alan Dennis, Barbara Ha- ley Wixom, Roberta M. Roth. — 5th ed.— Wiley : [Б. и.], 2012. — 363 p. — ISBN 978-1-1180576-2-9.
2. Чорней Н. Б. Теорія систем і системний аналіз: Навч. посіб. для студ. вищ. навч. закл. – К.: МАУП, 2005. – 256с.
3. Сурмін Ю.П. Аналітична діяльність: Посібник для аналітика неприбуткової організації. – К.: Центр інновацій та розвитку, 2002. – 96 с
4. Henderson J. Strategic Alignment: Leveraging information tech- nology for transforming organizations / J. Henderson, N. Venkatra- man // IBM Systems Journal.— 1993.— Vol. 32, no 1. — P. 4–16.

ОСОБЛИВОСТІ ТЕХНОЛОГІЇ WIMAX

Сержанський Станіслав Станіславович
Державний університет телекомунікацій

Worldwide Interoperability for Microwave Access (WiMAX) – стандартна технологія бездротового зв'язку для забезпечення високошвидкісного широкосмугового підключення на великі відстані для внутрішніх та комерційних цілей. Він працює за принципом методу модуляції ортогонального частотного розподілу ODFM. Це технологія бездротового мобільного доступу 4 покоління.

Принцип роботи WiMAX аналогічний принципу Wi-Fi. Комп'ютер або ноутбук, оснащені WiMAX, отримуватимуть дані від станції, що передає, використовуючи зашифровані ключі даних. Система WiMAX складається з вежі (базової станції) та приймача WiMAX. Базова станція може забезпечити покриття великої площі, в той час як приймач WiMAX може бути ноутбуком або карткою PCMCIA, який приймає сигнали від БС. Станція на вежі може бути підключена безпосередньо до Інтернету з використанням високошвидкісної смуги пропускання, проводового з'єднання або іншої базової станції з WiMAX.[1,с.1]

Передусім через значно більшу вартість, WiMAX не є заміною технологій Wi-Fi або бездротових точок доступу. Проте в цілому дешевше реалізувати WiMAX замість стандартних дротових апаратних засобів, таких як DSL. Тим не менш, глобальна телекомунікаційна індустрія вирішила інвестувати повністю в інші можливості, такі як LTE, залишаючи майбутню життєздатність Інтернет-послуг WiMAX, про яку йде мова. Устаткування WiMAX існує у двох основних формах: базова станція, встановлена постачальниками послуг для розгортання технології в зоні покриття; і приймачі, встановлені в клієнтах.

WiMAX розробляється консорціумом промисловості, під наглядом групи, що називається WiMAX Forum, який засвідчує обладнання WiMAX, щоб забезпечити його відповідність технічним умовам. Його технологія базується на стандарті IEEE 802.16 стандартів широкосмугового зв'язку.

WiMAX має великі переваги, коли мова йде про мобільність, але це саме там, де його обмеження видно.

Плюси WiMAX:

WiMAX користується популярністю завдяки своїй низькій вартості та гнучкості. Він може бути встановлений швидше, ніж інші інтернет-технології, оскільки він може використовувати більш короткі вежі та меншу кабельну підтримку, навіть підтримуючи нелінійний вигляд (NLoS) охоплення по всьому місту чи країні.

Окрім доступу до Інтернету, WiMAX може забезпечити можливості передачі голосу та відео, а також доступ до телефону. Оскільки передавачі WiMax можуть проходити на відстані декількох миль із швидкістю передачі даних, що досягають 30-40 мегабіт на секунду (Mbps) (1 Гбіт / с для стаціонарних станцій), легко зрозуміти його переваги, особливо в тих областях, де дротовий Інтернет неможливий або теж витрати на реалізацію.

WiMAX підтримує кілька моделей використання мереж:

Засіб для передачі даних через мережу Інтернет-провайдерів, зазвичай називається зворотний тракт.

Форма фіксованого бездротового широкосмугового доступу до Інтернету, що замінює супутниковий Інтернет.Форма мобільного доступу до Інтернету, яка безпосередньо конкурує з технологією LTE. Інтернет-доступ для користувачів у надзвичайно віддалених місцях, де прокладка кабелю буде занадто дорогою.

WiMAX мінуси:

Оскільки WiMAX є бездротовим за своїм характером, чим далі від джерела, який отримує клієнт, тим повільніше їх зв'язок стає. Це означає, що в той час як користувач може

знизити 30 Мбіт / с в одному місці, віддаляючись від сайту комірки, ця швидкість може скоротитись до 1 Мбіт / с або поруч із нічим.

Подібно до того, коли підключення до одного маршрутизатора з'єднується з кількома пристроями, багато користувачів в одному секторі радіо WiMAX зменшать продуктивність для інших.

Wi-Fi набагато популярніший, ніж WiMAX, тому вбудовані більше Wi-Fi пристроїв, ніж WiMAX. Тим не менше, більшість реалізацій WiMAX включають в себе апаратне забезпечення, яке дозволяє цілому домашньому господарству, наприклад, користуватись послугою через Wi-Fi, подібно до того, як бездротовий маршрутизатор забезпечує Інтернет для декількох пристроїв.[2,с.1]

АНАЛІЗ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ У СФЕРІ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

Глущенко Олексій Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Штучний інтелект на основі нейронних мереж на теперішній час стає все більш поширеним у всіх галузях життя людини. У роботі розглянуто можливі варіанти застосування нейронних мереж у сфері електронних комунікаційних мереж та сформовано ряд задач, які потребують вирішення.

На теперішній час через постійно зростаючу складність електронних комунікаційних мереж (ЕКМ) внаслідок збільшення кількості користувачів та їх вимог постає питання більш ефективного вирішення задач за призначенням цих мереж. Водночас зростає потужність та функціональність систем штучного інтелекту (ШІ) на основі нейронних мереж (НМ) у всіх галузях життя людини. Застосування ШІ дозволяє зробити техніку, що оточує людину не тільки більш функціональною, а й більш зручною для користувачів. Тож галузь ЕКМ також переживає трансформацію через дедалі ширше використання штучного інтелекту (ШІ).

Технології ШІ використовуються в різноманітних програмах, від обслуговування клієнтів до оптимізації продуктивності мережі. В основі функціонування систем ШІ закладено нейронні мережі.

Нейронні мережі – це математичні моделі, що імітують роботу людського мозку, в якому нейрони взаємодіють один з одним за допомогою зв’язків, що передають сигнали. НМ зазвичай складаються з безлічі шарів нейронів, які є штучними системами, що імітують роботу біологічного нейрону, кожен з яких обробляє вхідний сигнал і передає результати наступному шару. НМ є одним із ключових інструментів у машинному навчанні та штучному інтелекту.

Далі розглянуто основні поняття НМ:

1) архітектура мережі – у залежності від кількості шарів нейронів може бути одношарова побудова або багатошарова, між різними шарами існують взаємозв’язки;

2) функція активації – визначає, яким чином нейрон реагує на вхідні дані;

3) функція витрат – використовується для оцінки різниці між прогнозованими та фактичними результатами;

4) алгоритм навчання – метод або математична модель, яка підвищує продуктивність штучної НМ, і, як правило, застосовується багаторазово для поновлення ваг і рівнів упередженості мережі;

5) регуляризація – поняття, яке характеризує ряд функцій, які запобігають перенавчанню моделі.

НМ мають низку можливих застосувань у галузі електронних комунікацій, це такі як:

розпізнавання мови – системи голосового керування і голосового пошуку; автоматичний переклад; прогнозування трафіку – прогнозування обсягу трафіку в ЕКМ, що дає змогу операторам ефективніше розподіляти ресурси та підвищувати якість послуг; виявлення шахрайства – запобігання шахрайства в фінансових операціях, наприклад, у платіжних системах і банках; управління мережами – оптимізація управління ЕКМ, наприклад, для автоматичного управління частотами, зміни потоків даних і підтримки стабільної роботи мережі. Також НМ можуть використовуватись для аналізу великих обсягів даних, тим самим частково замінивши людину. Ще один з варіантів застосування ШІ на основі НМ – написання системного програмного забезпечення для пристроїв, на основі яких побудуються ЕКМ.

Проте, при впровадження НМ в галузі ЕКМ виникає ряд задач, які є невирішеними натепер. Наприклад, доволі високі вимоги до апаратного та програмного забезпечення ЕКМ, висока вартість готових програмних продуктів із ШІ, та необхідний високий рівень знань та практичних навичок адміністраторів таких мереж. Тому постає питання з'ясування доцільності застосування НМ в галузі ЕКМ на різних рівнях – від провайдерського до рівня невеликих корпоративних мереж, можливі рекомендації по впровадженню НМ в ЕКМ, які вже функціонують.

Висновки. Застосування НМ в сфері ЕКМ може значно поліпшити ефективність та надійність мережі, знизити вартість її обслуговування та підвищити якість послуг, які надаються користувачам. Дослідження може бути корисним для розробки більш ефективних систем ЕКМ у майбутньому, за умови вирішення ряду задач, пов'язаних із складністю і вартістю систем із ШІ на базі НМ.

ВВЕДЕННЯ ДО КОНЦЕПЦІЇ РОЗУМНОГО БУДИНКУ ТА ЙОГО ПОТЕНЦІАЛУ ДЛЯ ПОЛІПШЕННЯ КОМФОРТУ ТА ЕНЕРГОЕФЕКТИВНОСТІ

Ходаківський Дмитро Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Сучасні технології швидко проникають у всі сфери нашого життя, включаючи сферу житлового будівництва. Розумний будинок є одним з найзахоплюючіших та інноваційних напрямків в сфері житлових технологій. Він пропонує автоматизацію та інтеграцію різних систем та пристроїв у будинку, забезпечуючи більший рівень комфорту, безпеки та енергоефективності для мешканців.

Розумний будинок може управляти освітленням, опаленням, кондиціонуванням повітря, системою безпеки, аудіо-відео обладнанням та багатьма іншими системами. Ці системи здатні співпрацювати між собою, а також можуть бути керовані з використанням різних пристроїв, таких як смартфони, планшети або комп'ютери.

Основна перевага розумного будинку полягає в забезпеченні комфортного та зручного середовища для мешканців. За допомогою цієї технології, ви можете налаштувати освітлення та температуру у будь-якій кімнаті в будь-який момент часу, а також віддалено контролювати всі пристрої та системи в будинку. Наприклад, ви можете ввімкнути опалення перед вашим поверненням додому, щоб зустріти теплу та затишну атмосферу, або налаштувати автоматичне вимкнення освітлення в необітних кімнатах для енергозбереження.

Крім того, розумний будинок сприяє енергоефективності та зменшенню витрат на електроенергію. Системи автоматичного регулювання освітлення та температури дозволяють раціонально використовувати енергію, забезпечуючи оптимальні умови в будинку. Також, здатність до віддаленого керування дозволяє вимкнути пристрої, коли вони не

використовуються, або встановити графіки автоматичного ввімкнення та вимкнення систем згідно з вашим розкладом.

Висновок: Завдяки розумним системам керування освітленням, опаленням, безпекою та багатьма іншими, мешканці можуть налаштовувати умови у будинку залежно від своїх потреб. Це включає вмикання опалення перед поверненням додому, регулювання освітлення за допомогою мобільного додатку або автоматичне вимкнення пристроїв для енергозбереження.

Крім поліпшення комфорту, розумний будинок також сприяє енергоефективності. Системи автоматичного регулювання допомагають оптимізувати споживання енергії, зменшуючи витрати та сприяючи збереженню ресурсів. Віддалене керування дозволяє мешканцям ефективно керувати системами та пристроями у будинку з будь-якого місця та в будь-який час.

МІКРОСЕРВІСНІ СИСТЕМИ: СУЧАСНІ МЕТОДИ ТА ПІДХОДИ

Бондар Дмитро Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Мікросервісні системи - це архітектурний підхід до розробки програмного забезпечення, в якому програма розбивається на набір невеликих, незалежних сервісів, що працюють разом для виконання загальної функціональності системи. Кожен сервіс виконує конкретні завдання та має свою власну базу коду, базу даних та інтерфейси. Вони взаємодіють між собою за допомогою стандартизованих протоколів комунікації, таких як HTTP або AMQP.

Мікросервісна архітектура надає кілька переваг. Вона сприяє гнучкості та масштабованості, оскільки окремі сервіси можуть бути розгорнуті та масштабовані незалежно один від одного. Крім того, мікросервіси дозволяють легко впроваджувати зміни та оновлення, оскільки вони не мають жорсткої залежності між собою. Кожен сервіс може бути розроблений, тестований та впроваджений незалежно, що полегшує швидку розробку та внесення змін.

Ширше розглянемо питання сучасних методів та підходів у мікросервісних системах.

Декомпозиція монолітних застосунків на мікросервіси є процесом розбиття великого монолітного застосунку на набір незалежних сервісів, кожен з яких відповідає за конкретну функціональність. Цей підхід дозволяє покращити модульність, гнучкість та розширюваність системи, а також полегшує швидкість розробки та впровадження змін.

Процес декомпозиції починається з аналізу функціональності та залежностей в монолітному застосунку. Критично важливо ідентифікувати окремі логічні компоненти, які можуть бути використані як основа для створення окремих сервісів. Ці компоненти можуть бути функціональними блоками, що виконують специфічні завдання або мають свої власні вхідні та вихідні точки.

Після ідентифікації компонентів проводиться їх виокремлення в окремі сервіси. Кожен сервіс володіє своїм власним кодом, базою даних та інтерфейсами. Важливо визначити межі між сервісами та встановити стандартизовані способи комунікації між ними, такі як використання REST або мікросервісних шин.

Ключовим аспектом декомпозиції монолітних застосунків є забезпечення відокремленості функціональних модулів. Кожен сервіс може бути розгорнутий, масштабований та оновлюваний незалежно від інших сервісів, що полегшує розробку та підтримку системи. Крім того, декомпозиція дозволяє розробникам працювати над окремими сервісами паралельно, що покращує швидкість розробки та забезпечує більшу гнучкість у виборі технологій та інструментів для кожного сервісу.

Використання контейнеризації є одним з ключових методів у мікросервісних системах. Контейнери дозволяють упакувати сервіси та їх залежності разом у виконувану одиницю, яка включає в себе все необхідне для їх безперервної роботи. Основним інструментом контейнеризації є Docker, який надає стандартизований підхід до упаковки, розгортання та управління контейнерами.

Одна з переваг контейнеризації полягає в тому, що вона дозволяє створювати ізольовані середовища для кожного мікросервісу. Кожен контейнер містить свої власні бібліотеки, залежності та конфігурацію, що усуває проблему конфліктів та несумісностей між сервісами. Крім того, контейнери є переносимими, тому що вони можуть бути розгорнуті на будь-якій платформі, що підтримує Docker.

Загалом, використання контейнеризації у мікросервісних системах дозволяє забезпечити ізоляцію сервісів, прискорити розгортання та забезпечити ефективне керування та масштабування системи. Контейнери відкривають шлях до більш гнучких та складних архітектур, де кожен сервіс може функціонувати незалежно, а система в цілому може швидко реагувати на зміни та змінюватися залежно від потреб користувачів та бізнесу.

Керування та моніторинг мікросервісних систем є ключовими аспектами для забезпечення їх ефективності, доступності та надійності. З огляду на розподілений характер мікросервісної архітектури, де багато невеликих сервісів працюють разом, важливо мати механізми для керування цими сервісами та моніторингу їх стану.

Один з основних аспектів керування мікросервісними системами - це оркестрація та управління контейнерами, що містять сервіси. Оркестратори контейнерів, такі як Kubernetes, дозволяють автоматизувати розгортання, масштабування, реплікацію та керування життєвим циклом контейнерів. Вони надають зручні інструменти для налаштування, керування та моніторингу контейнерів, забезпечуючи стабільну та ефективну роботу мікросервісів.

Крім оркестрації контейнерів, важливо мати систему моніторингу, яка дозволяє відстежувати стан та продуктивність кожного сервісу у системі. Моніторинг допомагає виявляти проблеми, визначати навантаження та аналізувати пропускну здатність сервісів. Інструменти моніторингу, такі як Prometheus, Grafana або ELK Stack, дозволяють збирати, аналізувати та відображати дані про роботу мікросервісів, надаючи цінні інсайти для вирішення проблем та оптимізації роботи системи.

Додатково, для забезпечення доступності та надійності мікросервісних систем, можна використовувати систему управління помилками та відновленням. Це означає, що система повинна мати механізми для виявлення та обробки помилок, автоматичного відновлення сервісів та забезпечення безперервної роботи системи, навіть при виникненні проблем у окремих сервісах.

Керування та моніторинг мікросервісних систем є складними завданнями, але є необхідними для забезпечення високої продуктивності та стабільності системи. Правильно налаштовані інструменти керування та моніторингу дозволяють виявляти проблеми, швидко реагувати на них та забезпечувати ефективну роботу мікросервісних систем.

Отже, мікросервісні системи здатні забезпечити більшу гнучкість, масштабованість та швидкість розробки в порівнянні з монолітними архітектурами. Декомпозиція монолітних застосунків, використання контейнеризації та ефективне керування та моніторинг є ключовими методами та підходами при розробці мікросервісних систем. Розуміння цих методів дозволяє розробникам ефективно створювати та управляти мікросервісними системами.

Список використаних джерел

1. Docker Docs: How to build, share, and run applications | Docker Documentation https://docs.docker.com/

2. Про Microservices.io (Кріс Річардсон) https://microservices.io/patterns/observability/application-metrics.html

ПРОБЛЕМНІ АСПЕКТИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ METROETHERNET

Колос Валерія Миколаївна
Державний університет телекомунікацій
м. Київ

Нові технології розвиваються неймовірно стрімко, потреби користувачів зростають з кожним днем. Доступ в Інтернет, IP-телефонія, IP-TV пред'являють більш високі вимоги до пропускної здатності мережі та її надійності.

Для забезпечення високої якості і надійності передачі досить актуально використовувати оптичні мережі, побудовані на базі технології MetroEthernet. Гнучкість технології Ethernet, її відносна дешевизна, а також дуже велика поширеність і ймовірність підтримки мережевим обладнанням різних виробників робить MetroEthernet мережі практично ідеальним вибором для побудови пакетної агрегаційної магістралі міста.

Створення мережі MetroEthernet, повинно дозволяти значно розширяти спектр послуг, що надаються, і також запропонувати потенційним споживачам дешевий спосіб доступу до мережі оператора, зберігши при цьому характерні для виділених ліній рівень якості зв'язку, швидкості доступу та конфіденційності.

При побудові мережа повинна забезпечувати можливість надання повного спектру сучасних послуг передачі даних в місті (регіоні) з максимальною зоною охоплення.

Так як технологія MetroEthernet являє собою концепцію надання послуг мережі Ethernet в масштабах міста, вона має малу дистанцію підключення (відстань між операторським і абонентським обладнанням).У більшості великих міст при щільній забудові дана проблема навряд чи актуальна, однак, в сільських районах, слід застосування технології MetroEthernet істотно збільшує витрати на оптоволокно. Традиційним фізичним середовищем передачі даних по магістральних мережах є оптичне волокно. Способи його застосування класифікують за назвою точки сполучення зі споживачем і об'єднують назвою FTTx – оптоволокно до точки "x". Найчастіше застосовується: FTTB (FiberToTheBuilding) - оптика до адміністративної будівлі, FTTC (FiberToTheCurb) – до розподільної шафи, FTTH (FiberToTheHome) – до житлового будинку.

Потреби в більш високих швидкостях ведуть до непропорційного зростання витрат оператора при збільшенні абонентської бази, так як обладнання стандартів GigabitEthernet, 10 GigabitEthernet, а також прийдешніх 40 GigabitEthernet і 100 GigabitEthernet виявляється досить дорогим. Тоді коли буде розроблена технологія передачі даних протоколу Ethernet зі швидкістю 1 Тбіт/с , потрібно буде вирішувати безліч проблем, пов'язаних з фізичними явищами.

Також останнім часом основна увага приділяє питанням стандартизації. Це обумовлено тим, що раніше дуже багато виробників обладнання просували на ринок рішення, що забезпечують транспорт другого рівня за схемою "точка-точка" і "точка-багато точок". Ці рішення пропонувалися операторам для побудови міських універсальних мереж зв'язку.

Основна і дуже серйозна проблема, пов'язана з такими рішеннями, полягає в наступному: використовуючи досить прості і логічні засоби, не можна зістикувати ці рішення з міжміськими мережами. Подібне обладнання забезпечує роботу мережі в масштабах міста, але завдання з'єднання декількох вузлів в різних містах вимагає збільшення витрат на порядок. До того ж ефективність використання ресурсів мережі оператора знижується практично до нуля.

Тому варто б зосередитися на послугах міських універсальних мереж зв'язку з використанням VPN третього рівня. Цей підхід дозволить оператору краще зрозуміти вимоги клієнта, адже якщо розглядати модель взаємодії відкритих систем аж до сьомого рівня, то чим вище рівень, на якому оператор може аналізувати клієнтський трафік, тим ефективнішою є його обробка. Відповідно, оператор має більші можливості для розширення спектра послуг.

МАЙБУТНІ СФЕРИ ЗАСТОСУВАННЯ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Шаран Дмитро Олегович
Державний університет телекомінікацій
Навчально-науковий інститут телекомунікацій

Бездротові сенсорні мережі набули значної популярності завдяки своїй гнучкості у вирішенні проблем у різних сферах застосування та мають потенціал змінити наше життя різними способами. Вони використовуються в таких сферах життя як:

1. **Військова**. Бездротові сенсорні мережі, ймовірно, стануть невід'ємною частиною військового командування, контролю, зв'язку, обчислювальної техніки, розвідки, спостереження на полі бою, розвідки та цілевказівних систем.
2. **Моніторинг навколишнього середовища**: Бездротові сенсорні мережі можуть використовуватися для моніторингу різних параметрів навколишнього середовища, таких як температура, вологість, рівень шуму, якість повітря, забруднення води, радіація тощо. Це може застосовуватися в міських системах моніторингу, екологічних досліджень, контролю якості повітря та води, а також у промислових об'єктах.
3. **Транспортна**: інформація про дорожній рух у режимі реального часу збирається мережами БСМ, щоб пізніше подавати транспортні моделі та сповіщати водіїв про затори та проблеми з дорожнім рухом.
4. **Системи безпеки та спостереження**: Бездротові сенсорні мережі можна використовувати для створення системи безпеки та спостереження. Вони можуть бути встановлені у важливих місцях, будівлях, громадських місцях або на кордонах для виявлення незаконних дій, відстеження руху, контролю доступу та іншого.
5. **Додатки для охорони здоров'я**: деякі програми для охорони здоров'я для сенсорних мереж включають підтримку інтерфейсів для людей з обмеженими можливостями, інтегрований моніторинг пацієнтів, діагностику та введення ліків у лікарнях, телемоніторинг фізіологічних даних людини, а також відстеження та моніторинг лікарів або пацієнтів у лікарні.
6. **Моніторинг стану інфраструктури**: Бездротові сенсорні мережі можуть використовуватися для моніторингу стану інфраструктури, такої як мости, дороги, тунелі, будівлі тощо. Вони можуть виявляти деформації, вібрацію, напруження та інші параметри, що допомагають вчасно виявляти пошкодження або потенційні проблеми з безпекою.

Але час не стоїть на місці тому потрібно розглянути потенціально нові шляхи розвитку використання бездротових сенсорних мереж. Так було підібрано 5 максимальной ймовірних галузь де бездротові мережі зможуть себе проявити.

1. **Інтернет речей (Інтернет речей, IoT)**: З розвитком концепції IoT вимагається, що бездротові сенсорні мережі стануть невід'ємною складовою частиною пов'язаних пристроїв і систем. Вони можуть використовуватися для збору даних, взаємодії та управління великою кількістю пристроїв у побутовій техніці, містах, автомобілях, промислових системах та багатьох інших сферах.
2. **Розумні міста (Smartcity)**: Бездротові сенсорні мережі можуть бути використані для створення розумних міст, де вони можуть забезпечити моніторинг трафіку, контроль за якістю повітря, керування освітленням та іншими системами, управління водопостачанням, оптимізацію сміттєзбірників тощо. Це покращить рівень життя в містах в який входить: ефективність, зручність та якість життя.
3. **Здоров'я та медицина**: Бездротові сенсорні мережі вже використовуються у медицині але мають великий потенціал у покращенні медичних послуг. Вони можуть використовуватися для моніторингу стану захворювання, дистанційного контролю хвороб, виявлення надзвичайних ситуацій, автоматичного виклику допомоги та багато іншого. Такі мережі можуть сприяти покращенню діагностики, лікування та загального управління охороною здоров'я.

4. **Промисловість**: У концепції Четвертої промислової революції (Промисловості 4.0) бездротові сенсорні мережі відіграють важливу роль. Вони можуть використовуватися для моніторингу та контролю устаткування, прогнозування поломок, оптимізації виробничих процесів, забезпечення безпеки та підвищення продуктивності.

5. **Автономні транспортні засоби**: бездротові сенсорні мережі можуть бути використані для зв'язку та обміну даними між автономними транспортними засобами, дорожньою інфраструктурою та іншими учасниками дорожнього руху. Вони можуть підтримувати безпечну та ефективну координацію руху, уникати зіткнення та покращувати загальну безпеку та продуктивність транспорту.

Таким чином шляхів розвитку бездротових сенсорних мереж є неймовірна велика кількість і вона буде збільшуватися кожний рік або навіть кожен місяць якщо буде потреба такої цікавої та прогресивної технології.

Література:

4. Wireless sensor network (2023). https://en.wikipedia.org/wiki/Wireless_sensor_network
5. M.A. Matin and M.M. Islam (2012). Overview of Wireless Sensor Network.
6. Wireless Sensor Network Architecture and Its Applications https://www.elprocus.com/architecture-of-wireless-sensor-network-and-applications/
7. Applications of Wireless Sensor Networks https://encyclopedia.pub/entry/17294

РОЗВИТОК АЛГОРИТМІВ ШИФРУВАННЯ ІНФОРМАЦІЇ У МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ

Луценко Павло
Державний університет телекомунікацій

Приклади мобільних сенсорних мереж**:**

1. Система моніторингу забруднення повітря: Мобільні сенсорні пристрої (наприклад, смартфони або датчики, прикріплені до тіла) можуть бути використані для збору даних про рівень забруднення повітря, такі як рівень шкідливих речовин або концентрація пилу. Ці дані можуть бути використані для аналізу якості повітря та вжиття заходів для зменшення забруднення.

2. Система контролю руху транспорту: У мобільних сенсорних мережах можуть бути використані датчики, вбудовані у транспортні засоби (наприклад, автомобілі або велосипеди), для збору інформації про рух, швидкість, густину трафіку тощо. Ці дані можуть бути використані для оптимізації руху транспорту, управління сигналізацією на дорогах або прогнозування потенційних заторів.

3. Система відстеження та моніторингу здоров'я: У мобільних сенсорних мережах смартфони та носимі пристрої можуть бути використані для вимірювання фізіологічних показників, таких як пульс, кров'яний тиск, рівень активності тощо. Ці дані можуть бути використані для моніторингу здоров'я, виявлення потенційних проблем і розробки персоналізованих рекомендацій для покращення фізичного стану.

Розвиток алгоритмів шифрування спрямований на досягнення декількох цілей:

1. Забезпечення безпеки: Головною метою розвитку алгоритмів шифрування є забезпечення безпеки передачі інформації. Розробники створюють нові алгоритми та вдосконалюють існуючі, щоб ускладнити зламання шифру та забезпечити захист від несанкціонованого доступу до даних.

2. Ефективність: Окрім безпеки, ефективність також є важливим аспектом розвитку алгоритмів шифрування. Алгоритми повинні бути ефективними в плані швидкості шифрування та розшифрування, щоб не затримувати передачу даних і не споживати надто багато ресурсів пристрою.

3. Стійкість до криптоаналізу: Розвиваючи алгоритми шифрування, дослідники та експерти з криптографії ставлять мету створити алгоритми, які важко зламати. Вони проводять криптоаналіз для виявлення потенційних слабкостей і вразливостей і розробляють нові методи шифрування, щоб ускладнити атаки.

4. Відповідність вимогам та контексту: Алгоритми шифрування повинні відповідати вимогам і контексту, в якому вони використовуються. У випадку мобільних сенсорних мереж це означає, що алгоритми мають бути пристосовані до обмежених обчислювальних ресурсів мобільних пристроїв і ефективно працювати у бездротових середовищах.

5. Прозорість та відкритість: Бажаною властивістю розвиваючихся алгоритмів шифрування є їхня прозорість та відкритість. Це дозволяє експертам та громадськості перевіряти алгоритми на наявність потенційних проблем безпеки та впливати на їх розвиток.

Ці цілі спрямовують розвиток алгоритмів шифрування, щоб забезпечити безпеку, ефективність та відповідність вимогам в контексті мобільних сенсорних мереж.

Яка теоретична шкода може бути завдана, якщо алгоритм шифрування не достатньо надійний**:**

Якщо алгоритм шифрування не забезпечує достатньо високого рівня безпеки, можуть виникнути наступні теоретичні шкоди:

1. Виток конфіденційної інформації: Якщо алгоритм шифрування не ефективний і може бути легко зламаний, це може призвести до витоку конфіденційної інформації. Зламувачі можуть отримати доступ до зашифрованих даних і розшифрувати їх, що призведе до розголошення особистих, комерційних або конфіденційних даних.

2. Порушення цілісності даних: Якщо алгоритм шифрування не забезпечує цілісність даних, це може призвести до їхнього викривлення або модифікації без дозволу. Зламувач може змінити зашифровані дані, що може призвести до порушення цілісності, надійності та довіреності інформації.

3. Вразливість перед атаками: Якщо алгоритм шифрування має слабкості або вразливості, зламувачі можуть використовувати ці вразливості для проведення різних атак, таких як атаки з використанням обчислювальної потужності, аналізу шифру або соціального інженерингу. Це може призвести до незаконного доступу до системи, перехоплення даних або навіть зламу системи в цілому.

4. Втрата довіри та репутаційних збитків: Якщо алгоритм шифрування доводиться до відома громадськості або широко використовується в різних системах, і якщо він не забезпечує належний рівень безпеки, це може призвести до втрати довіри від користувачів та репутаційних збитків для організацій або індивідів, які використовують цей алгоритм.

Таким чином, несправні алгоритми шифрування можуть призвести до серйозних наслідків, таких як виток конфіденційної інформації, порушення цілісності даних, збільшення ризику атак і втрати довіри користувачів. Тому важливо продовжувати розвивати і вдосконалювати алгоритми шифрування для забезпечення надійного захисту інформації.

ЗМІСТ І МОЖЛИВОСТІ СУЧАСНИХ ПЛАТФОРМ NFV ТА ЇХ МОЖЛИВЕ ЗАСТОСУВАННЯ

Лижов Олексій Михайлович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Сучасні платформи віртуалізації мережевих функцій (NFV) надають розширений набір можливостей для ефективного розгортання, керування та управління віртуальними мережевими функціями (VNF). Ось деякі з цих можливостей:

Оркестрація ресурсів: Платформи NFV надають механізми для керування та оркестрації віртуальних ресурсів, таких як обчислювальні, мережеві та зберігання ресурси. Це дозволяє автоматично розгортати та масштабувати VNF, використовуючи доступні ресурси.

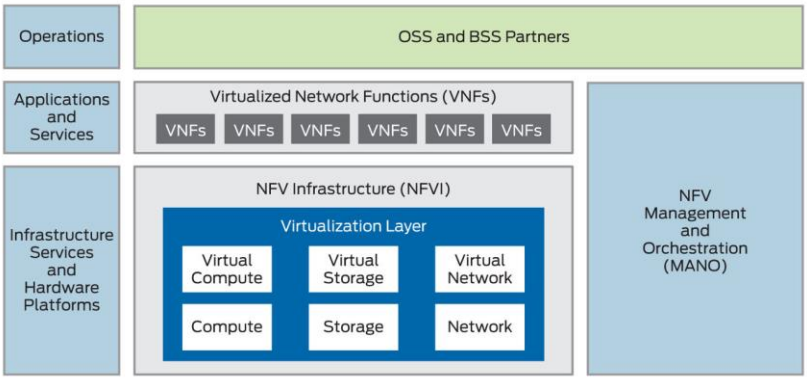
Управління життєвим циклом VNF: Платформи NFV забезпечують управління життєвим циклом VNF, включаючи їх створення, розгортання, налаштування, моніторинг, масштабування та видалення. Це дозволяє операторам зв'язку ефективно керувати та управляти віртуальними функціями в мережі.

Мережева служба та політика: Платформи NFV надають можливості для визначення та керування мережевими службами та політиками. Оператори зв'язку можуть встановлювати правила, політики безпеки та якість обслуговування для керування трафіком та забезпечення відповідного рівня послуг для користувачів.

Віртуальні мережеві інфраструктури: Платформи NFV надають віртуальні мережеві інфраструктури (Virtualized Network Infrastructure, VNI), які забезпечують віртуальні ресурси, такі як обчислювальні, мережеві та зберігання ресурси, необхідні для розгортання та функціонування VNF. Це може включати віртуальні мережеві комутатори, маршрутизатори, віртуальні простори імен та інші компоненти.

Багатовендорна підтримка: Сучасні платформи NFV надають підтримку для різних вендорів обладнання та програмного забезпечення. Це дозволяє операторам зв'язку використовувати рішення від різних постачальників та легко інтегрувати їх у свої мережі.

Моніторинг та аналітика: Платформи NFV надають можливості для моніторингу та аналізу стану VNF, мережевого трафіку, продуктивності та використання ресурсів. Це дозволяє операторам зв'язку відстежувати та оптимізувати роботу своїх мереж та послуг.



Платформи віртуалізації мережевих функцій (NFV) можуть застосовуватись у різних сферах індустрії зв'язку та мережевих послуг. Ось деякі з них:

Оператори зв'язку: NFV може бути використана операторами зв'язку для впровадження нових послуг та модернізації їхніх мереж. Вона дозволяє операторам зв'язку збільшити гнучкість мережі, швидко реагувати на зміни вимог ринку та швидко впроваджувати нові послуги без необхідності фізичної заміни апаратного забезпечення.

Дата-центри та хмарні сервіси: NFV може бути використана у дата-центрах та хмарних сервісах для віртуалізації мережевих функцій. Це дозволяє забезпечити гнучкість та ефективне використання ресурсів в мережевих сервісах, таких як віртуальні приватні мережі (VPN), файрволи, балансування навантаження тощо.

Постачальники послуг IT: Платформи NFV можуть бути використані постачальниками послуг IT для надання мережевих функцій як сервісу (Network Function as a Service, NFaaS). Це дозволяє підприємствам та організаціям отримати доступ до необхідних мережевих функцій без необхідності утримання власної інфраструктури.

Інтернет речей (IoT): NFV може бути використана для підтримки мережевої інфраструктури для IoT. Вона дозволяє забезпечити гнучкість та масштабованість мережі для підключення великої кількості пристроїв IoT та обробки великого обсягу даних, які генеруються цими пристроями.

Виробництво та індустрія 4.0: NFV може бути використана в контексті виробництва та індустрії 4.0 для впровадження мережевої інфраструктури, що забезпечує гнучкість та автоматизацію. Це дозволяє підприємствам швидко реагувати на зміни виробничих процесів та ефективно управляти мережевими ресурсами.

Застосування платформ NFV варіюються в залежності від конкретних вимог та потреб організацій. Вона може допомогти підвищити ефективність, знизити витрати та забезпечити більшу гнучкість у використанні мережевих ресурсів.

Отже, сучасні платформи NFV надають комплексні можливості для ефективного використання віртуалізації мережевих функцій у мережах операторів зв'язку. Вони дозволяють розгортати, керувати та управляти VNF у гнучкому та автоматизованому способі, що сприяє зниженню витрат та швидкому впровадженню нових послуг.

РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ ПРИЙНЯТТЯ РІШЕНЬ В УМОВАХ РИЗИКУ

Крюков В.Л.
Державний університет телекомунікацій, м. Київ

Досягнення інформаційних технологій революціонізували процеси прийняття рішень, пропонуючи потужні інструменти та методи зменшення ризиків. Цей розділ досліджує роль інформаційних технологій, таких як аналіз даних, імітаційні моделі та системи підтримки прийняття рішень, у покращенні процесу прийняття рішень в умовах ризику та невизначеності.

Аналіз стратегій прийняття рішень у невизначених та ризикованих ситуаціях. Порівняльне дослідження

Стратегії прийняття рішень відіграють ключову роль у подоланні невизначених та ризикованих ситуацій. У цьому сегменті розглядаються різні стратегії, такі як імовірнісний аналіз, планування сценаріїв та аналіз реальних варіантів. Мета есе-шляхом порівняння та протиставлення цих стратегій визначити найбільш ефективні підходи до прийняття рішень в умовах високого ризику[1, с.34].

Вплив когнітивних упереджень на прийняття рішень в умовах ризику. Когнітивні упередження суттєво впливають на процеси прийняття рішень, що часто призводить до неоптимального вибору в умовах ризику. У цьому розділі розглядаються поширені упередження, такі як прив'язка, упередженість підтвердження і неприйняття втрат, і їх вплив на прийняття рішень. Розуміння та усунення цих упереджень мають важливе значення для покращення результатів прийняття рішень в умовах ризику.

Вивчення застосування інструментів і методів прийняття рішень в управлінні ризиками. Ефективне управління ризиками вимагає застосування інструментів і методів прийняття рішень, адаптованих до конкретних завдань кожної ситуації. Ця частина досліджує практичне застосування таких інструментів, як дерева рішень, моделювання Монте-Карло та аналіз чутливості для управління ризиками та прийняття обґрунтованих рішень.

Вплив організаційної культури на прийняття рішень у ризикованих ситуаціях. Організаційна культура відіграє вирішальну роль у формуванні процесів прийняття рішень в умовах ризику. У цьому сегменті розглядається, як культурні фактори, включаючи схильність до ризику, моделі комунікації і норми прийняття рішень, впливають на якість і результати прийнятих рішень. Висновки, отримані в результаті цього аналізу, можуть допомогти організаціям у формуванні культури, що сприяє ефективному прийняттю рішень в умовах ризику.

Розробка інтегрованої структури для ефективного прийняття рішень в умовах ризику. Грунтуючись на попередніх розділах, в цій частині пропонується комплексна структура для ефективного прийняття рішень в ситуаціях високого ризику. Включивши елементи моделей прийняття рішень, стратегій, інструментів та організаційної культури, ця структура покликана забезпечити цілісний підхід до успішного подолання ризиків та невизначеності[2, с.7]..

Роль штучного інтелекту в прийнятті рішень в умовах ризику і невизначеності. Штучний інтелект (ШІ) має величезний потенціал для сприяння прийняттю рішень в умовах ризику та невизначеності. У цьому розділі розглядається застосування методів штучного інтелекту, включаючи Машинне навчання, обробку природної мови та експертні системи, для розширення можливостей прийняття рішень. Розглядаються переваги, проблеми та етичні міркування, пов'язані з впровадженням штучного інтелекту при прийнятті рішень.

Аналіз етичних наслідків прийняття рішень у сценаріях високого ризику. Прийняття рішень у ситуаціях високого ризику часто пов'язане з етичними дилемами та компромісами. Цей сегмент досліджує етичні наслідки, пов'язані з процесами прийняття рішень, враховуючи такі фактори, як інтереси зацікавлених сторін, потенційна шкода та моральні зобов'язання. Розробка етичних рамок для прийняття рішень може допомогти окремим особам та організаціям робити відповідальний вибір.

Розробка програм навчання прийняттю рішень для фахівців в галузях, схильних до ризику. Для підвищення компетентності в прийнятті рішень необхідні індивідуальні програми навчання, особливо для фахівців, що працюють в галузях, схильних до ризику. У цьому розділі розглядаються розробка та впровадження навчальних програм з прийняття рішень з акцентом на розвиток навичок, критичне мислення та аналіз ризиків. Ефективне навчання може дати людям можливість приймати обґрунтовані рішення в умовах підвищеного ризику[3, с.15].

На закінчення слід зазначити, що методи і засоби прийняття рішень в умовах ризику багатогранні і вимагають всебічного розуміння різних факторів. Цей нарис розглядав моделі прийняття рішень, Інформаційні технології, когнітивні упередження, стратегії прийняття рішень, організаційну культуру, штучний інтелект та етичні міркування. Узагальнюючи ці знання, організації та окремі особи можуть приймати обґрунтовані рішення та успішно справлятися з ризиками, що в кінцевому підсумку призводить до поліпшення результатів в умовах підвищеного ризику.

Література:

1. Балдін, К. в.управлінські рішення / К. В. Балдін, С. Н. Воробйов, в. Б. Уткін. - М.: Дашков і Ко, 2019. — 496 с.
2. Бусов, В.і. управлінські рішення : Підручник для бакалаврів / в. і. Бусов. - М.: Видавництво Юрайт, 2018. - 254 с.
3. Віханський О.С. Менеджмент: Підручник / Віханський О. С., Наумов А. і., — 6-е вид., перераб. і доп-м.: Магістр, НДЦ ИНФРА-М, 2019. 450 С.

НЕЙРОМОРФНІ ОБЧИСЛЮВАЛЬНІ СИСТЕМИ

Петрик Андрій Васильович
Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій

Проектування нейроморфних систем, здатних імітувати роботу біологічних нейронів та синапсів, моделювати когнітивні процеси людського мозку, розглядається як один із ключових напрямків у сфері штучного інтелекту. Дослідження, спрямовані на розвиток нових обчислювальних парадигм та апаратну реалізацію моделей нейронних мереж, що переходять на новий етап – досягнутий у світі технологічний рівень дозволяє створювати системи на кристалі, містять мільйони штучних нейронів та синапсів. Сьогодні проекти в галузі нейроморфних чіпів ведуться багатьма світовими гравцями – від технологічних гігантів до стартапів. Нейроморфні системи є важливим напрямком розвитку штучного інтелекту, оскільки вони дозволяють імітувати роботу біологічних нейронів та синапсів і моделювати когнітивні процеси людського мозку. Дослідження, спрямовані на розвиток нових обчислювальних парадигм та апаратної реалізації моделей нейронних мереж, дозволяють створювати системи на кристалі, які містять мільйони штучних нейронів та синапсів. Це відкриває нові можливості для створення інтелектуальних систем, здатних до виконання складних завдань у реальному часі.

Принцип побудови нейроморфних систем полягає у тому, що вони повинні імітувати роботу біологічного мозку, використовуючи властивості нейронів та синапсів. Для цього необхідно забезпечити взаємодію між нейронами та синапсами, що досягається за допомогою мережі електронних компонентів, що дозволяє передавати сигнали між нейронами та синапсами. Нейроморфні системи можуть бути побудовані на базі різних матеріалів, наприклад, на кремнієвих чіпах, що дозволяє отримати велику кількість нейронів та синапсів на одному чіпі. Одним із найважливіших викликів для розробників нейроморфних систем є реалізація ефективних методів навчання нейронних мереж. Традиційні методи машинного навчання, такі як зворотнє поширення помилок, можуть не бути ефективними для нейроморфних систем, оскільки вони потребують великої кількості обчислень. У статті розглянуто загальні принципи побудови нейроморфних систем та способи реалізації нейронних мереж, представлений огляд перспективних проектів у галузі нейроморфних обчислень.

Протягом кількох останніх десятиліть основною обчислювальною моделлю для переважної більшості комп'ютерних систем служила архітектура фон Неймана. У цій архітектурі пам'ять та центральний процесор спілкуються один з одним через шину даних, що обмежує продуктивність системи, особливо у додатках з інтенсивним використанням даних. Дедалі ширше використання алгоритмів машинного навчання, що потребують обробки величезних масивів даних, і також фізичні обмеження технології змушують шукати альтернативу процесорам із класичною архітектурою для створення систем зі штучним інтелектом.

На відміну від послідовних систем, до яких належать фонейманівські процесори, в людському мозку обробка інформації проводиться зовсім інакше. Кожен із майже 100 млрд нейронів обробляє інформацію незалежно, працюючи паралельно з іншими нейронами та отримуючи сигнали від них через синапси – зв'язок між нейронами з пам'яттю. На цьому принципі будують штучні аналоги біологічного мозку – нейроморфні системи (рис. 1). Апаратна реалізація нейроморфних систем дозволяє кардинально підвищити обчислювальну потужність за рахунок паралельної обробки даних на безлічі процесорах. Сьогодні з розвитком субмікронних та нанотехнологій створення таких систем стає все більш реальним завданням.

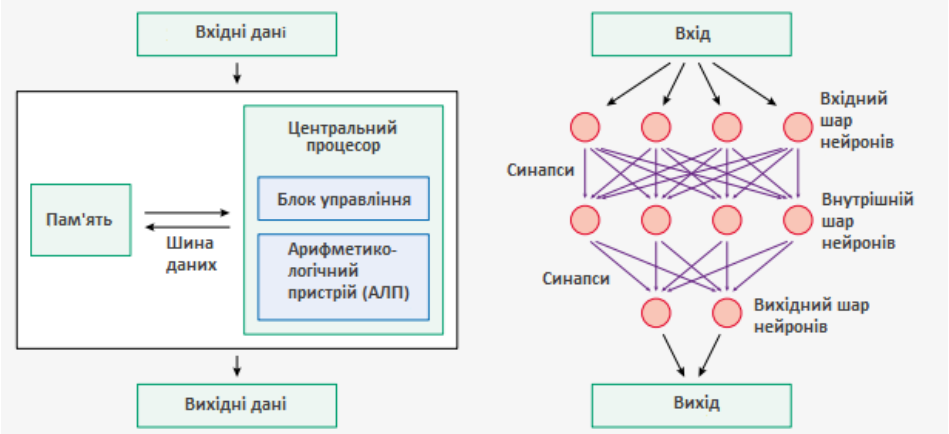


Рис. 1. Архітектура фон Неймана (зліва) та нейроморфна архітектура (справа)

Йдеться про системи, що містять як штучні нейрони кілька десятків тисяч і навіть мільйонів процесорних ядер. При цьому структура кожного процесора-нейрону простіша, ніж традиційного процесорного ядра, але за рахунок їх величезної кількості функціональність системи суттєво зростає.

Слід зважати на ще один важливий фактор – енергоспоживання. Сьогодні основною проблемою мобільних і периферійних пристроїв є жорстко обмежені бюджети споживаної потужності. Можливості традиційних обчислювальних архітектур з погляду зниження споживання незначні. Відповіддю може стати більш ефективна паралельна архітектура у поєднанні із можливістю навчання.

Дуже важливою є також можливість системи працювати автономно, без постійного обміну інформацією з віддаленим сервером або хмарою, оскільки це знижує безпеку та швидкодію системи. Тому бажано створити нейроморфну систему, що самонавчається, здатну обробляти дані локально, всередині пристрою.

Перехід на нейроморфну архітектуру на основі нової парадигми обчислень без розподілу процесів обробки та зберігання інформації обіцяє дати якісний ефект у вирішенні обчислювальних завдань та наблизити створення систем з так званим "сильним" штучним інтелектом.

Список використаних джерел:

1. Zhou, Peng, Dong-Uk Choi, Jason Kamran Eshraghian and Sung-Mo Steve Kang. “A Fully Memristive Spiking Neural Network with Unsupervised Learning.” 2022 IEEE International Symposium on Circuits and Systems (ISCAS) (2022): 634-638.

2. Yang, Chuan-Sen, Da-Shan Shang, Nan Liu, Elliot J. Fuller, Sapan Agrawal, A. Alec Talin, Yongqing Li, Baoshou Shen and Young Sun. “All-Solid-State Synaptic Transistor with Ultralow Conductance for Neuromorphic Computing.” Advanced Functional Materials 28 (2018): n. pag.

3. Chang, Chih-Cheng, Pin-Chun Chen, Teyuh Chou, I-Ting Wang, Boris Hudec, Che-Chia Chang, Chia-Ming Tsai, Tian-Sheuan Chang and Tuo-Hung Hou. “Mitigating Asymmetric Nonlinear Weight Update Effects in Hardware Neural Network Based on Analog Resistive Synapse.” IEEE Journal on Emerging and Selected Topics in Circuits and Systems 8 (2017): 116-124.

4. Peng, Hsuan-Tung, Mitchell A. Nahmias, Thomas Ferreira de Lima, Alexander N. Tait and Bhavin J. Shastri. “Neuromorphic Photonic Integrated Circuits.” IEEE Journal of Selected Topics in Quantum Electronics 24 (2018): 1-15.

АНАЛІЗ МОЖЛИВОСТЕЙ ТА ПЕРЕВАГ ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ

Добровольський Роман Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

У сучасному цифровому світі збільшується значимість безпеки даних у телекомунікаційних системах. Відсутність надійного механізму забезпечення конфіденційності та цілісності даних може призвести до серйозних наслідків, таких як витік інформації, підробка даних або несанкціонований доступ до комунікаційних мереж. У цьому контексті використання блокчейн-технологій стає актуальним, оскільки вони надають потенціал для створення розподіленої та недоступної для змін безпекової інфраструктури.

Блокчейн-технології базуються на концепції розподіленої бази даних, яка забезпечує надійне збереження та передачу інформації. Основою цієї технології є механізм консенсусу, який дозволяє підтверджувати правдивість транзакцій та забезпечувати безпеку даних. Наприклад, механізми Proof-of-Work і Proof-of-Stake дозволяють перевірити правильність транзакцій шляхом виконання складних обчислювальних завдань або за допомогою доказу власності.

Ще однією важливою характеристикою блокчейн-технологій є їхня здатність забезпечувати імутабельність даних. Коли інформація записана в блокчейн, вона не може бути змінена або видалена без погодження більшості учасників мережі. Це робить дані цілісними та надійними, оскільки будь-які спроби змінити записи стають очевидними для всіх учасників системи.

Смарт-контракти, які базуються на блокчейн-технологіях, відкривають нові можливості для автоматизації процесів перевірки безпеки даних. Вони дозволяють встановлювати умови доступу та зміни даних, що забезпечує додатковий рівень контролю та безпеки. Смарт-контракти можуть виявляти недобросовісний доступ до даних та недозволені зміни, що сприяє зменшенню ризику шахрайства та порушень безпеки.

Дослідження показують, що використання блокчейн-технологій в телекомунікаційних системах може мати численні переваги, такі як відстеження та аудит безпекових подій, забезпечення конфіденційності даних та зменшення ризику шахрайства. Однак, важливо враховувати потенційні обмеження та виклики, пов'язані з впровадженням цих технологій, такі як масштабованість та швидкодія.

Список використаних джерел:

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

2. Buterin, V. (2013). Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform.

3. Swan, M. (2015). Blockchain: Blueprint for a New Economy.

4. Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks.

ОСОБЛИВОСТІ ІНТЕРФЕЙСУ СИСТЕМИ ТЕСТУВАННЯ ЛЬОТНОГО ЕКІПАЖУ

Денисюк Роман Русланович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Сучасні авіаційні системи тестування льотного екіпажу вимагають належної уваги до деталей інтерфейсу [1]. Інтерфейс, який є простим, інтуїтивно зрозумілим і ефективним, може значно підвищити продуктивність, безпеку та зручність пілотів, зокрема під час тривалого та стресового навантаження [2].

Ця теза аналізує основні аспекти дизайну інтерфейсу системи тестування льотного екіпажу. Вона розглядає теоретичні та практичні аспекти дизайну інтерфейсу, включаючи відображення даних [3], мультимодальні взаємодії [4], адаптивність, розпізнавання ситуацій та ментальні моделі.

Серед важливих висновків - необхідність балансу між наданням достатньої інформації для прийняття рішень і уникненням перевантаження інформацією [2]. Крім того, простота та зручність використання повинні бути взаємопов'язані з гнучкістю, щоб дати пілотам можливість адаптуватися до різних сценаріїв [5].

Висновки

Загалом, кращий інтерфейс для системи тестування льотного екіпажу повинен враховувати ергономічні принципи, мультимодальні взаємодії, а також високий рівень адаптивності і розуміння користувачем.

Література:

1. Сміт, П. (2020). Авіація та людський фактор: Розуміння інтерфейсу для тестування льотного складу. Springer.
2. Джонсон, К., і Стентон, Н. (2021). Дослідження дизайну інтерфейсу авіаційних випробувальних систем. Журнал авіаційних технологій та інженерії.
3. Гарсія, А., і Томпсон, Д. (2022). Вплив дизайну інтерфейсу на системи тестування льотного складу: Якісний підхід. Журнал аерокосмічних інформаційних систем.
4. Лю, Ю., & Лі, Ф. (2023). Візуалізація даних в системах тестування льотного складу: Когнітивний підхід. Авіаційна психологія та прикладні людські фактори.
5. Еванс, Л. (2023). Мультимодальні взаємодії та адаптивні інтерфейси в системах тестування льотного складу. IEEE Transactions on Human-Machine Systems.

ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ RCS

Лаптінов Ярослав Борисович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Технологія RCS зазнала значного розвитку в останні роки і вважається перспективним напрямом у сфері мобільних комунікацій. Rich Communication Services (RCS) — це протокол для обміну повідомленнями між телефонами. Поступово RCS має повністю замінити SMS та MMS-повідомлення. RCS забезпечує повноцінний мультимедійний досвід прямо на телефоні. Впровадження RCS надає нові можливості для вдосконалення звичайних текстових повідомлень, забезпечуючи більш широкий спектр функцій і взаємодії між користувачами. В

даній тезі розглянемо перспективи впровадження технології RCS, аналізуючи її переваги, виклики та можливості.

Загалом, технологія відкриває широкі можливості для поліпшення способу комунікації між користувачами та розвитку бізнес-комунікацій. Багатофункціональність, покращена взаємодія з контентом, оптимізовані групові чати, підтримка читання та доставки повідомлень, а також інтеграція з послугами бізнесу є основними перевагами, які роблять RCS перспективною технологією для майбутнього комунікаційного середовища.

Завдяки RCS ми вже не обмежені звичайними текстовими повідомленнями. Тепер можемо додавати до них відео, фотографії, голосові повідомлення та навіть геолокацію. Це означає, що можемо висловлювати свої думки та почуття набагато більш точно, ділитися моментами та враженнями у більш багатогранному форматі.

Але на мою думку не менш важливим є відкриття цією технологією можливостей для бізнес-комунікацій. Тепер компанії можуть надсилати своїм клієнтам персоналізовані пропозиції, обмінюватися інформацією миттєво та покращувати взаємодію зі своїми клієнтами. Інтеграція бізнес-чатів з іншими сервісами дає можливість використовувати їх як інтернет магазини, економлячи час і ресурси компанії повязані з розробкою і підтримкою подібного функціоналу на їх вебсайті. Це відкриває нові можливості для розвитку бізнесу та підвищення задоволення клієнтів.

Технологія RCS забезпечує сумісність з існуючими мобільними мережами та стандартами, такими як GSM та LTE. Це дозволяє плавний перехід до нової технології без необхідності великих інвестицій у мережеву інфраструктуру. Крім того це дозволяє операторам мобільного зв’язку як мінімум частково замінити своїм сервісом OTT-мессенджери та окремо монетизувати RCS-повідомлення з величезною вигодою для себе у порівнянні з монетизацією об’ємів трафіку якими є повідомлення у Viber чи Telegram.

ВИСНОВКИ

Технологія RCS має великий потенціал для покращення зв'язку між користувачами та розширення можливостей бізнес-комунікацій. Впровадження RCS забезпечує більш багатофункціональне та інтерактивне спілкування, що сприяє поліпшенню користувацького досвіду та створенню нових можливостей для розвитку бізнесу. Попри виклики та перешкоди, технологія RCS має потенціал стати основним засобом комунікації у мобільному світі.

Література:

1. RCS - The future of messaging [Електронний ресурс] // GSM Association. – 2021. – Режим доступу до ресурсу: https://www.gsma.com/futurenetworks/rcs/.

2. The Future of Messaging: RCS. International Journal of Computer Science and Mobile Computing [Електронний ресурс] // Verma, S. – 2022. – Режим доступу до ресурсу: https://www.ijcsmc.com/docs/papers/May2022/V11I5202210.pdf.

ТЕХНОЛОГІЯ MPLS: ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ

Верхотуров Денис Олександрович
Державний університет телекомунікацій

MPLS (англ. Multiprotocol Label Switching - багатопротокольна комутація за мітками) - це концепція, відповідно до якої в комп'ютерних мережах здійснюється переадресація пакетів. Головна її особливість - у реченні альтернативи аналізу маршрутизаторами типу IPLP заголовків по всіх пакетів, який здійснюється з метою визначення напряму для пересилання до наступного компоненту інфраструктури. У разі якщо задіюється розглянута технологія, то аналіз заголовка здійснюється одноразово при вході в мережу MPLS, а потім ініціюється перевірка відповідності між параметрами пакету і властивостями потоку.

Особливості розробки MPLS

Розробили технологію MPLS фахівці, зацікавлені в реалізації універсального протоколу обміну даними, який би підходив для інфраструктури з комутацією каналів, так і для додатків, де здійснюється передача пакетів. У мережах MPLS можуть передаватися різні види трафіку IP (Internet Protocol), ATM (Asynchronous Transfer Mode), Ethernet, SONET і SDH (Synchronous Digital Hierarchy). Розробка концепції здійснювалася з урахуванням переваг і недоліків попередніх протоколів аналогічного призначення. При цьому в деяких аспекти MPLS передбачає реалізацію більш простих алгоритмів у порівнянні з підходами, що застосовуються в традиційних рішеннях. Як відзначають експерти, мережеве обладнання, що підтримує технологію MPLS, здатне витіснити з ринку традиційні рішення, що свідчить про те, що розробниками MPLS була проведена гарна робота по оптимізації і універсалізації даної концепції.

Ключові переваги MPLS: оперативність обробки даних

Найважливіша перевага MPLS полягає в затратах меншої кількості часу на обробку даних, ніж при зіставленні IP-адреси. Більше того, технологія MPLS зменшує час, який витрачається на пересилання пакета з використанням базових маршрутизаторів. Фактично може здійснюватися комутація з застосуванням декількох протоколів, при якій використовуються спеціальні мітки в рамках пакетів передаються мережевих даних. Завдяки цьому формуються відокремлені комутовані потоки.

Переваги MPLS: універсальність

Ще одна важлива властивість концепції - універсальність. Практично в будь мережі IP MPLS може бути впроваджена. Розглянута технологія добре підтримується на апаратному рівні. Принципово можливе застосування доступних за ціною рішень для впровадження MPLS - Mikrotik, наприклад. Універсальні принципи приведення інфраструктури в працездатний стан. Однак при конструюванні мережі MPLS налаштування обладнання повинна проводитися досвідченими фахівцями. Насамперед - компетентними в частині розуміння особливостей архітектури мережі, характеристик її апаратних компонентів.

Переваги MPLS: масштабованість

Інфраструктура MPLS характеризується масштабністю і ступенем автономності роботи щодо різноманітних протоколів, за допомогою яких здійснюється передача даних. Специфіка конкретних стандартів, що реалізуються на канальному рівні, не має значення. При впровадженні мережі MPLS немає необхідності забезпечення функціонування мереж на другому рівні, які оптимізовані під передачу тих або інших різновидів трафіку. З точки зору класифікації мереж за типом комутації MPLS правомірно віднести до інфраструктури, в якій здійснюється комутація пакетів.

Багатопротокольність технологій MPLS полягає в тому, що вона дозволяє використовувати протоколи маршрутизації не тільки стека TCP/IP (Transmission Control Protocol/Internet Protocol), а і любого іншого стека, наприклад IPX/SPX (Internet Work Packet Exchange/Sequence Packet Exchange). В цьому випадку замість протоколів маршрутизації RIP IP, OSPF та IS-IS застосовується протокол RIP IPX або ж NLSP (NetWare Link Services Protocol), а загальна архітектура LSR (MPLS) зостанеться такою ж під час розробки технології MPLS в середині 90-х років, коли на практиці функціонувало декілька стеків протоколів, така багатопротокольність вважалася важливою, проте сьогодні в умовах домінування стеку протоколів TCP/IP ця властивість не є важливою. Правда, сьогодні багатопротокольність MPLS можна розуміти по-іншому - як властивість передавати за допомогою з'єднання MPLS трафік різних протоколів канального рівня.

Встановлення та видалення MPLS тунелів

Існує два стандартних протокола управління тунелями в MPLS-мережі. LDP (англ. Label Distribution Protocol - протокол розподілу міток) і RSVP-TE, розширення RSVP (англ. Resource ReSerVation Protocol - протоколу резервування мережевих ресурсів) для оптимізації та

управління трафіком. Також існують розширення протоколу BGP, здатні керувати віртуальними каналами в MPLS-мережі.

Тема MPLS не вказує тип даних, що передаються до MPLS тунелі. У разі, якщо виникає необхідність передати двох різних типи трафіку між двома маршрутизаторами так, щоб вони по різному оброблялися маршрутизаторами ядра мережі MPLS, необхідно встановити два різних MPLS тунелю для кожного типу трафіку.

ОРГАНІЗАЦІЯ МЕРЕЖІ МОБІЛЬНОГО ЗВ'ЯЗКУ НА ОСНОВІ ТЕХНОЛОГІЙ ЧЕТВЕРТОГО ПОКОЛІННЯ

Чирва Богдан Миколайович
Державний університет телекомунікацій

Мережі мобільного зв'язку – це одні з найбільш важливих складових сучасного світу телекомунікацій. Щодня мільйони людей використовують їх для забезпечення спілкування, передачі даних, доступу до Інтернету і багато іншого. Одним з ключових етапів розвитку цих мереж було створення технологій четвертого покоління (4G), які забезпечують значно більшу швидкість передачі даних і забезпечують користувачам більш широкий спектр можливостей.

Однак, не зважаючи на успіх 4G, технології не стоять на місці, і на зміну їм приходять нові розробки – технології п'ятого покоління (5G). 5G має потенціал змінити підхід до побудови мобільних мереж і відкриває нові можливості для комунікацій, які раніше були неможливі.

Організація мережі мобільного зв'язку на основі технологій 4G і 5G має свої особливості, але існує деякий набір кроків, які необхідно здійснити для створення працездатної мережі. Одним з ключових аспектів є побудова інфраструктури мережі, яка включає в себе базові станції, маршрутизатори, комутатори і інші компоненти. Крім того, необхідно визначити параметри мережі, такі як швидкість передачі даних, частотні діапазони, пропускну здатність, інтерфейси тощо.Другим важливим аспектом є забезпечення безпеки мережі, оскільки мережі мобільного зв'язку мають великий потенціал для атак і злочинів в Інтернеті.

Для організації мережі мобільного зв'язку на основі технологій четвертого покоління (4G) використовуються різноманітні пристрої, такі як смартфони, планшети, модеми та інші, які можуть підключатися до бездротової мережі оператора мобільного зв'язку. 4G забезпечує значну швидкість передачі даних, що дозволяє користувачам отримувати доступ до Інтернету, переглядати відео, грати в ігри та використовувати різноманітні онлайн-сервіси з високою швидкістю та якістю зв'язку.

Однією з основних технологій, що застосовуються в мережах 4G, є Long-Term Evolution (LTE), яка забезпечує високу швидкість передачі даних та покращену якість зв'язку. LTE базується на технології OFDM (Orthogonal Frequency Division Multiplexing), яка дозволяє передавати сигнали на різних частотах, що забезпечує покращену ефективність використання радіочастотного діапазону.

У мережах 4G використовуються різні протоколи, такі як IP Multimedia Subsystem (IMS), що забезпечують підтримку різноманітних послуг, включаючи голосовий зв'язок, відеозв'язок, мультимедійні послуги. Крім того, мережі 4G підтримують технологію Voice over LTE (VoLTE), що дозволяє передавати голосовий трафік у форматі пакетів, забезпечуючи високу якість зв'язку.

У підсумку, технології четвертого покоління мобільного зв'язку відкривають нові можливості для створення більш швидких та надійних мереж, що забезпечують більші можливості для користувачів. Однак, також необхідно бути уважними до проблем безпеки, пов'язаних з використанням таких мереж, та постійно розвивати технології для забезпечення їхньої надійності та захищеності.

КОРПОРАТИВНІ МЕРЕЖІ SD-WAN

Тужик Андрій Юрійович
Державний університет телекомунікацій

SD-WAN (Software-Defined Wide Area Networking) є технологією, яка застосовується для побудови корпоративних мереж. Вона дозволяє підвищити ефективність та керованість мережевого трафіку, забезпечуючи підтримку різних видів підключень, включаючи приватні та громадські мережі, такі як Інтернет.

Основна ідея SD-WAN полягає в розділенні управління мережею від фізичної інфраструктури. За допомогою програмного забезпечення, яке використовується для керування мережею, можна гнучко налаштовувати політики маршрутизації, управляти пропускною здатністю та забезпечувати безпеку даних. SD-WAN також може здійснювати оптимізацію мережевого трафіку, наприклад, за допомогою компресії даних або кешування.

Одним з головних переваг SD-WAN є можливість підключення до різних типів мереж, включаючи традиційні приватні лінії, VPN-тунелі та громадський Інтернет. Це дає можливість організаціям використовувати більш доступні та вартісно ефективні засоби зв'язку, підвищуючи гнучкість та масштабованість їхньої мережі.

Корпоративні мережі SD-WAN також забезпечують підвищену безпеку. Вони можуть використовувати шифрування даних та віртуальні приватні мережі для захисту передачі інформації. Крім того, централізоване управління мережею дозволяє легко встановлювати політики безпеки та моніторити мережевий трафік, що допомагає виявляти та реагувати на можливі

Рішення SD-WAN надають кілька переваг для корпоративних мереж:

1. Покращення продуктивності: SD-WAN дозволяє оптимізувати шляхи передачі даних, вибираючи найефективніші маршрути. Це допомагає знизити затримки і втрату пакетів, покращує якість обслуговування та забезпечує кращу продуктивність додатків, включаючи хмарні та відеоконференції.
2. Гнучкість підключень: SD-WAN дозволяє підключати різні типи мереж, такі як приватні лінії, VPN-тунелі та громадський Інтернет. Це дає організації можливість використовувати доступні та вартісно ефективні засоби зв'язку, а також підключати віддалені робочі місця та філії з різних місць.
3. Централізоване управління: SD-WAN надає централізовану консоль управління, що дозволяє адміністраторам керувати та налаштовувати мережу з одного місця. Це спрощує управління політиками маршрутизації, безпекою та якістю обслуговування. Крім того, централізоване моніторинг та аналітика допомагають виявляти проблеми та забезпечувати високу доступність мережі.
4. Забезпечення безпеки: SD-WAN реалізує різні механізми безпеки, такі як шифрування даних, віртуальні приватні мережі та інтеграція з системами з обмеженням доступу. Це допомагає захистити передачу даних і забезпечити безпеку корпоративної мережі навіть через громадський Інтернет.
5. Скорочення витрат: SD-WAN може знизити витрати на мережу шляхом ефективнішого використання доступних ресурсів, включаючи більш доступні та вартісно ефективні засоби зв'язку. Він також спрощує управління мережею та знижує необхідність у фізичній інфраструктурі на місці.

В цілому, рішення SD-WAN допомагають покращити продуктивність, гнучкість, безпеку та ефективність корпоративних мереж, забезпечуючи кращий досвід користувача та знижуючи загальні витрати.

На ринку існує кілька провідних вендорів, які надають рішення SD-WAN для корпоративних мереж. Деякі з них включають:

1. Cisco SD-WAN (раніше відомий як Viptela): Cisco пропонує розширену платформу SD-WAN, яка включає роутери, контролери та централізоване управління. Вона надає гнучкість, безпеку та оптимізацію трафіку для корпоративних мереж.
2. VMware SD-WAN by VeloCloud: VMware пропонує SD-WAN-рішення, яке поєднує в собі віртуалізацію, широкий вибір підключень та автоматизоване управління. Вони також надають інтеграцію з іншими продуктами VMware.
3. Silver Peak SD-WAN: Silver Peak є одним з провідних вендорів SD-WAN, пропонуючи рішення, яке забезпечує безпеку, ефективність трафіку та простоту управління. Вони акцентуються на оптимізації приватних та громадських мереж.
4. Fortinet SD-WAN: Fortinet поєднує SD-WAN з безпекою, надаючи інтегровану платформу, яка забезпечує захист мережі, оптимізацію трафіку та гнучкість підключень.
5. Juniper Contrail SD-WAN: Juniper Networks пропонує Contrail SD-WAN, що надає високу масштабованість, безпеку та ефективність мережі. Вони також підтримують інтеграцію з хмарами та іншими продуктами Juniper.

Це лише кілька прикладів провідних вендорів SD-WAN на ринку, і існує багато інших варіантів. При виборі вендора SD-WAN важливо враховувати потреби вашої організації та вимоги до мережі.

ВПРОВАДЖЕННЯ СТРАТЕГІЙ МАСШТАБОВАНОСТІ ТА ОПТИМІЗАЦІЇ В ОБРОБЦІ ВЕЛИКИХ ОБСЯГІВ ДАНИХ

Андрійчук Владислав Вікторович
Державний університет телекомунікацій
Навчально-науковий Інститут телекомунікацій

Впровадження стратегій масштабованості та оптимізації є ключовим завданням в обробці великих обсягів даних. У даному рефераті проведено дослідження та аналіз підходів до масштабованості та оптимізації в обробці великих обсягів даних, а також розглянуті приклади їх впровадження в реальних сценаріях.

Масштабованість в обробці великих обсягів даних означає здатність системи ефективно працювати зі зростаючими обсягами даних. Це включає розширення ресурсів, таких як обчислювальна потужність та зберігання, для забезпечення продуктивності системи при збільшенні навантаження.

Оптимізація в обробці великих обсягів даних

Оптимізація в обробці великих обсягів даних включає використання різноманітних технік та алгоритмів для забезпечення швидкої та ефективної обробки даних. Це може включати покращення алгоритмів обробки, використання кешування, паралельної обробки та інших стратегій.

Стратегії масштабованості в обробці великих обсягів даних

Горизонтальне масштабування включає розподіл обробки даних між багатьма вузлами або серверами. Це дозволяє розподілити навантаження та забезпечити більшу пропускну здатність для обробки великих обсягів даних.

Вертикальне масштабування передбачає збільшення ресурсів на окремих вузлах або серверах, щоб підвищити їх продуктивність. Це може включати додавання більшої кількості процесорів, пам'яті або інших ресурсів для покращення обробки даних.

Використання розподіленої системи для масштабованості

Прикладом впровадження стратегії масштабованості є використання розподіленої системи, такої як Apache Hadoop або Apache Spark, для обробки великих обсягів даних. Ці

системи дозволяють розподіляти обробку даних між багатьма вузлами, що дозволяє ефективно працювати з великими обсягами інформації.

Використання кешування для оптимізації

Інший приклад оптимізації включає використання кешування даних для швидкого доступу до часто використовуваних даних. Наприклад, можна використовувати інструменти кешування, такі як Redis або Memcached, для збереження певних результатів обчислень або проміжних даних, що дозволяє уникнути повторного обчислення та прискорити обробку.

Застосування технологій масштабованості та оптимізації в обробці великих обсягів даних має широкі застосування в різних галузях. Одним із прикладів може бути сфера електронної комерції. Компанії, які мають велику кількість клієнтів та транзакцій, потребують потужних систем для обробки та аналізу даних. За допомогою горизонтального масштабування та розподіленої обробки даних, можна забезпечити швидку та ефективну обробку замовлень, рекомендацій товарів та аналітики продажів.

Ще одним прикладом є обробка даних у наукових дослідженнях. Багато галузей, таких як геноміка, астрофізика та кліматологія, генерують великі обсяги даних, які потребують потужних інфраструктур для обробки та аналізу. Застосування оптимізаційних технік, таких як паралельна обробка та оптимізовані алгоритми, дозволяє вченим ефективно працювати з великими обсягами даних та здійснювати складні обчислення для виявлення закономірностей та зроблення нових відкриттів.

Також, великі компанії в сфері соціальних мереж та медіа використовують стратегії масштабування та оптимізації для обробки масивних обсягів даних про користувачів, їх взаємодію та вміст. Це дозволяє аналізувати користувацькі вподобання, рекомендувати персоналізований контент та забезпечувати високу швидкість завантаження інформації для мільйонів користувачів одночасно.

Впровадження стратегій масштабованості та оптимізації є ключовим для успішної обробки великих обсягів даних. Горизонтальне та вертикальне масштабування дозволяють адаптуватись до збільшення обсягів даних шляхом розподілу навантаження або збільшення потужності окремого сервера. Оптимізація, у свою чергу, поліпшує продуктивність системи за допомогою паралельної обробки даних та використанням кешування.

Список використаних джерел:

1. Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. MIS Quarterly

2. Johnson, A., & Brown, C. (2020). Handling Big Data in Telecommunications Networks. International Journal of Communication Systems.

ПЕРЕВАГИ ТА НЕДОЛІКИ AJAX

Токар Богдан Сергійович
Державний університет телекомунікацій

Постановка задачі. Актуальним є питання в допомозі людям з частим запитанням: які переваги та недоліки Ajax? Говорячи про технології та їх використання, ми зазвичай обговорюємо плюси та мінуси всього. Звичайно, як і багато інших технологій, сам Ajax має багато різних переваг і недоліків. Давайте глибше розглянемо ці дві сторони технології Ajax.

Переваги AJAX.

Перша перевага. Першою і головною перевагою Ajax є його здатність покращувати продуктивність і зручність використання веб-додатків.

Щоб пояснити більш детально, методи Ajax дозволяють програмам рендерити без даних, що зменшує трафік сервера всередині запитів. Враховуючи це, веб-розробники можуть значно скоротити час відповіді обох сторін.

Завдяки цьому відвідувачам вашого веб-сайту ніколи не доведеться бачити біле вікно й чекати, доки сторінки Ajax оновляться.

Друга перевага. Увімкнення асинхронних викликів.

Ajax приносить користь веб-розробникам у тому, що його фреймворк можна використовувати для відкладеного завантаження. Lazy Loading, це метод оптимізації, який широко використовується для онлайн-контенту. По суті, Ajax дозволяє своїм користувачам здійснювати асинхронні виклики веб-серверу без перезавантаження всієї веб-сторінки. Як веб-відвідувачу, вам не потрібно чекати, поки вся сторінка повністю завантажиться, щоб отримати доступ до всього вмісту сторінки.

Концепція відкладеного завантаження допомагає завантажувати лише необхідний розділ і відкладає решту, поки вона не знадобиться користувачам. Таким чином, Ajax Lazy Loading не тільки покращує завантаження веб-сторінки, але й позитивно впливає на взаємодію з користувачем і коефіцієнт конверсії.

Третя перевага. Перевірка форми.

На відміну від традиційного надсилання форми, де перевірка на стороні клієнта відбувається після надсилання, метод AJAX забезпечує точну та негайну перевірку форми. AJAX забезпечує швидкість, що також є однією з його значних переваг.

Недоліки Ajax

Перегляд вихідного коду дозволений, і кожен може переглянути вихідний код, написаний для Ajax, що робить його менш безпечним порівняно з іншими технологіями та пошукові системи не можуть індексувати сторінки Ajax, які не можуть індексуватися Google, а також іншими пошуковими системами.

Найважливіше те, що Ajax значною мірою залежить від JavaScript, тому лише браузери, які підтримують JavaScript або XMLHttpRequest, можуть використовувати сторінки з технікою Ajax.

Висновки та перспективи.

Отже, в Ajax так як і в інших технологіях, є як переваги так і недоліки. Мною було розібрано малу частину переваг та більшу частину недоліків. Тому я можу сказати, що Ajax наданий момент є надійною технологією, як в використанні клієнтом, так і в розробці для користувачів, хоча вона й має недоліки, але з тим відсотком переваг які є, я можу сказати, що цією системою можна користуватися, і вона є надійною.

Список використаних джерел

1. AJAX SYSTEMS [Електронний ресурс]:[Електронний ресурс]: [Веб-сайт]. – Електронні дані. – Київ : AJAX SYSTEMS, 2023. – Режим доступу: https://ajax.systems/ua/products/ дата звернення 06.03.2023).

2. AJAX SYSTEMS SUPPORT [Електронний ресурс]:[Електронний ресурс]: [Веб-сайт]. – Електронні дані. : AJAX SYSTEMS SUPPORT, 2023. – Режим доступу: https://support.ajax.systems/en/ дата звернення 07.03.2023).

ВПЛИВ ТЕХНОЛОГІЇ 5G НА МАЙБУТНЄ КОМУНІКАЦІЙНИХ МЕРЕЖ

Христевич Олександр Сергійович
Державний університет телекомунікацій

Далі занурюючись в цифровий вік, технологія 5G виступає як критичний важелівий момент, впливаючи на значну трансформаційну дію на майбутнє комунікаційних мереж. Попередні технології сприяли вагомим досягненням, тоді як 5G вводить безпрецедентні

можливості, що переформовують спосіб передачі та отримання інформації, революціонізуючи різні галузі і змінюючи наш соціально-економічний ландшафт.

В основі трансформаційного потенціалу 5G лежить здатність значно покращити роботу мережі. Технологія володіє швидкістю блискавки, зменшеною затримкою, покращеною зв'язків і вищою надійністю. Ці атрибути сприяють передачі даних зі швидкістю до 100 разів швидше, ніж 4G, створюючи квантовий стрибок в якості та кількості даних, які можна обробити в мережах. Відповідно, це стимулюватиме розвиток та впровадження додатків і інновацій, які потребують великої кількості даних, розширюючи можливості дистанційного навчання, телемедицини, автономних автомобілів і багато іншого.

Більше того, архітектура технології 5G дозволяє впровадження зрізів мережі. Ця інноваційна функція дозволяє створювати кілька віртуальних мереж на одній інфраструктурі мережі 5G, кожна з яких адаптована до конкретних вимог. Зрізи мережі дозволяють ефективно розподіляти ресурси мережі залежно від потреб користувача, потреб застосувань і оперативних умов. Таким чином, оператори мережі можуть надавати спеціалізовані комунікаційні послуги, задовольняючи різні випадки використання, від застосувань з низькою затримкою в критичній інфраструктурі до споживчих розважальних послуг з високою пропускною здатністю.

З іншого боку, здатність 5G підтримувати масове підключення, разом з низькими енергетичними вимогами, прискорює розширення Інтернету речей (IoT). 5G буде служити кондуїтом для мільярдів підключених пристроїв, від повсякденних приладів до промислових машин, сприяючи створенню взаємозв'язаного екосистеми, яка сприяє ефективності, продуктивності і зручності. Такий високий ступінь підключеності відкриває шлях до розумних міст, будинків та промисловості, революціонізуючи спосіб, яким ми живемо, працюємо та взаємодіємо.

Впровадження 5G перевизначить заходи щодо безпеки мережі. Більш широка атакована поверхня, яка виникає внаслідок великого збільшення підключених пристроїв і складності мереж 5G, вимагає більш міцної, багатошарової та адаптивної стратегії безпеки. Щоб забезпечити цілісність мережі та довіру користувачів, рішення щодо кібербезпеки повинні розвиватися одночасно з цією технологією, вводячи інструменти штучного інтелекту та машинного навчання для автоматизації виявлення та реагування на загрози.

Тим часом, щільна мережева архітектура 5G, що базується на множині маленьких осередків, ставить питання щодо цифрового розриву. Хоча вона обіцяє надавати високошвидкісне з'єднання, її охоплення спочатку може обмежуватися щільно заселеними міськими територіями через значні інвестиції, необхідні для розвитку інфраструктури. Отже, необхідно мати стратегії, які розширять переваги 5G на сільські та віддалені громади, забезпечуючи рівний доступ до цієї перетворювальної технології.

Нарешті, впровадження технології 5G буде мати глибокі соціально-економічні наслідки. Сприяючи промисловості 4.0, створюючи нові бізнес-моделі та сприяючи економічному зростанню, воно обіцяє значне збільшення світового ВВП. Однак це також викликає питання щодо цифрової етики, приватності та витіснення робочих місць через автоматизацію, що вимагає злагоджених зусиль у сфері формування політики, освіти та підвищення кваліфікації.

Висновок: технологія 5G стоїть як основний стовп у формуванні майбутнього комунікаційних мереж. Її перетворювальний потенціал перевищує покращення роботи мережі, впливаючи на безліч аспектів наших суспільств та економік. Для того, щоб максимально використати її потенціал і подолати пов'язані з ним проблеми, необхідна багатодисциплінарна співпраця, що зводить до мінімуму розрив між технологією, політикою та суспільними потребами. У міру нашого переходу до епохи 5G на нас лежить відповідальність направити цю потужну технологію на інклюзивний, сталий прогрес.

ТЕХНОЛОГІЇ HOMEPNA ТА HOMECNA

Шмельов Михайло Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

HomePNA є технологією, яка використовує існуючу телефонну лінію для передачі даних в межах будинку. Вона дозволяє підключати різні пристрої до мережі, використовуючи інфраструктуру телефонної мережі. Це означає, що ви можете використовувати існуючі телефонні розетки у будинку для створення домашньої мережі без необхідності прокладання додаткових кабелів. HomePNA підтримує високу швидкість передачі даних і може бути використана для підключення різних пристроїв, таких як комп'ютери, телевізори, приставки до ігрових консолей і т.д.

HomePNA (HPNA), була розроблена Home Phoneline Networking Alliance. Сигнал HPNA працює у діапазоні від 5,5 до 9,5 МГц і не має впливу на роботу ADSL і VDSL-пристроїв або телефонів (див. рис.1). У рис.1 W відображає потужність сигналу, а F - частоту сигналу.

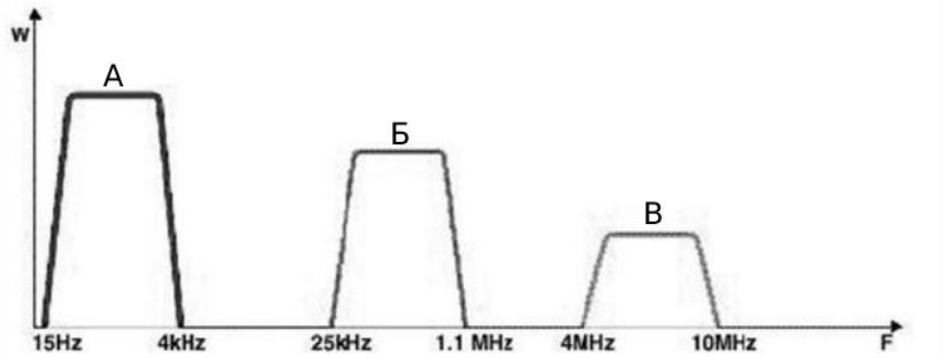


Рис.1 Частотний діапазон для телефонії (А), xDSL-обладнання (Б) та HomePNA (В)

Технологія HomePNA використовує метод доступу до середовища передачі, відомий як IEEE 802.3 CSMA/CD (Ethernet). Практично, HPNA є мегабітним Ethernet, який працює через телефонні кабелі. Це дозволяє використовувати широкий спектр програм, драйверів, застосунків і обладнання, сумісних з Ethernet.

Одна з привабливих особливостей технології HomePNA для використання в сегментах LAN є його "шинна" топологія, яка дозволяє просто організувати мережу шляхом прямого з'єднання декількох телефонних сегментів між собою (аналогічно до підключення кількох телефонів до однієї лінії). Таким чином, для розширення мережі не потрібно використовувати комутаційне обладнання (концентратори, комутатори та ін.). Крім того, можна організовувати каскадне з'єднання комп'ютерів паралельно до однієї телефонної розетки.

Технологія HomePNA має свій варіант під назвою HomeCNA (HCNA), при якому передача даних відбувається не через телефонну лінію, а по коаксіальному TV-кабелю.

Технології HomePNA 3.1 (HomeCNA 3.1) дозволяють передавати дані зі швидкістю до 320 Мбіт/с за допомогою наявного телевізійного кабелю.

Технологія HomePNA ТА HomeCNA дозволяє зручне підключення пристроїв у будинку, використовуючи наявну мідну інфраструктуру. Вона забезпечує високу швидкість передачі даних та можливість створювати розподілені мережеві точки для зручного доступу до мережі з різних місць у будинку.

СЕКЦІЯ 3

Інформаційна безпека телекомунікаційних систем і мереж

ТЕЛЕКОМУНІКАЦІЙНА БЕЗПЕКА: ЗАХИСТ ВІД КІБЕРЗАГРОЗ ТА ІНФОРМАЦІЙНИХ ВТОРГНЕНЬ

Іщенко Ілля
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

У сучасному цифровому світі, де технології телекомунікацій грають ключову роль, телекомунікаційна безпека стає невід'ємною складовою безпеки інформації та мережевих систем. Зростаюча кількість кіберзагроз та інформаційних вторгнень ставлять під загрозу конфіденційність, цілісність та доступність даних, а також надійність мережевих інфраструктур. Тому розробка та впровадження ефективних методів захисту від кіберзагроз та інформаційних вторгнень в телекомунікаційних системах стає надзвичайно актуальним завданням.

Системи телекомунікацій потребують комплексного захисту від кіберзагроз та інформаційних вторгнень, щоб забезпечити безпеку даних, стабільність мереж та довіру користувачів. Для досягнення цієї мети необхідно розробити та впровадити широкий спектр заходів, які включають технічні, організаційні та правові аспекти телекомунікаційної безпеки.

Перш за все, важливо забезпечити ефективний технічний захист, який включає захищені протоколи передачі даних, шифрування, брандмауери та системи виявлення вторгнень. Технічні заходи спрямовані на запобігання несанкціонованому доступу до інформації, забезпечення цілісності даних та захисту мережевої інфраструктури від різних видів атак.

Організаційні заходи є так само важливою складовою телекомунікаційної безпеки. Вони охоплюють розробку політик безпеки, проведення навчання та свідомості з питань безпеки серед персоналу, встановлення процедур контролю доступу та управління ризиками. Організаційні заходи сприяють створенню культури безпеки та включають усвідомлення загроз, вчасну реакцію на інциденти та постійне оновлення політик та процедур безпеки.

Крім технічних та організаційних заходів, правові аспекти також відіграють важливу роль у телекомунікаційній безпеці. Законодавча база має визначити права та обов'язки учасників телекомунікаційних процесів, а також надати механізми для притягнення до відповідальності осіб, які порушують безпеку мереж та інформації. Закони та положення повинні відповідати сучасним кіберзагрозам та враховувати міжнародні стандарти безпеки інформації.

Усі ці аспекти телекомунікаційної безпеки повинні працювати в комплексі, взаємодіючи між собою, щоб забезпечити найвищий рівень захисту від кіберзагроз та інформаційних вторгнень. Тільки комплексний підхід, враховуючи технічні, організаційні та правові аспекти, може забезпечити надійний захист телекомунікаційних систем та інформації.

Телекомунікаційна безпека, як важливий аспект цифрового світу, вимагає систематичного та комплексного підходу до захисту від кіберзагроз та інформаційних вторгнень. Розробка технічних заходів, організаційних політик та правової бази є вирішальними кроками для забезпечення безпеки даних, мереж та інфраструктур. Тільки шляхом поєднання цих аспектів можна забезпечити надійний та стійкий захист телекомунікаційних систем від кіберзагроз та інформаційних вторгнень.

БЕЗПЕКА В КЛІЄНТ-СЕРВЕРНИХ ВЕБ-ДОДАТКАХ

Кузьмук Андрій
Державний Університет Телекомунікацій
Навчально-науковий інститут Телекомунікацій

Безпека в клієнт-серверних веб-додатках є однією з найважливіших проблем, які потрібно вирішити в сучасному інтернет-середовищі. Зростання кількості загроз та атак на веб-додатки ставить під загрозу конфіденційність, цілісність та доступність важливих даних. Розглянемо різноманітні аспекти безпеки в клієнт-серверних веб-додатках з метою виявлення потенційних загроз та запропонування ефективних заходів для їх запобігання.

Аналіз загроз безпеці в клієнт-серверних веб-додатках: огляд основних видів атак, таких як кросс-сайтовий скриптинг (XSS), впровадження SQL-запитів (SQL injection), перехоплення сесій (session hijacking), міжсайтовий скриптинг (cross-site scripting, XSS) та міжсайтова підробка запитів (cross-site request forgery, CSRF), що можуть порушити безпеку веб-додатків та даних користувачів. Враховуючи ці загрози, досліджується ефективність методів захисту та запобігання їм.

Значення аутентифікації та авторизації в клієнт-серверних веб-додатках: розгляд процесу перевірки ідентичності користувача, забезпечення правильних рівнів доступу до функціоналу додатка та захисту конфіденційних даних. Вивчаються методи, такі як багаторівнева аутентифікація, двофакторна аутентифікація та використання ролей та дозволів для забезпечення безпеки.

Роль шифрування та підпису в забезпеченні безпеки комунікації в клієнт-серверних веб-додатках: дослідження методів шифрування та підпису даних для забезпечення конфіденційності, цілісності та автентичності передачі інформації між клієнтом та сервером. Розглядаються стандарти шифрування, такі як TLS (Transport Layer Security) і HTTPS (Hypertext Transfer Protocol Secure).

Аналіз сучасних інструментів та технологій для забезпечення безпеки в клієнт-серверних веб-додатках: огляд веб-фаєрволів, систем виявлення вторгнень (IDS), систем керування доступом (Access Control Systems) та інших рішень для забезпечення безпеки. Вивчається ефективність цих інструментів у запобіганні атак та захисті веб-додатків.

Роль навчання з використанням машинного навчання в підвищенні безпеки в клієнт-серверних веб-додатках: дослідження застосування методів машинного навчання для виявлення та запобігання атакам на веб-додатки. Вивчається ефективність алгоритмів машинного навчання, таких як виявлення вразливостей і класифікація атак, у забезпеченні безпеки.

Аналіз ризиків і загроз безпеці веб-додатків: вивчення різних типів атак, таких як кросс-сайтовий скриптинг (XSS), SQL-ін'єкція, крадіжка ідентифікаційних даних, і перехоплення сесій. Досліджуються можливі наслідки цих атак та рекомендації щодо їх запобігання.

Аналіз вразливостей веб-додатків та методів їх виявлення: дослідження потенційних слабких місць веб-додатків і розробка методів для виявлення цих вразливостей, таких як вразливості вводу даних, недостатній контроль доступу та недостатнє перевірка і валідація даних.

Розробка стратегій і рекомендацій для покращення безпеки веб-додатків: на основі проведеного аналізу безпеки веб-додатків висуваються пропозиції щодо покращення безпеки, такі як розробка сильних політик аутентифікації та авторизації, використання фаєрволів і систем виявлення вторгнень, регулярне оновлення та перевірка наявності вразливості.

СУЧАСНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Степаненко Юрій Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій м. Київ

Сучасні практики інформаційної безпеки включають широкий спектр технологій і методів, що використовуються для захисту конфіденційної та цінної інформації від несанкціонованого доступу, зміни, знищення або крадіжки. Деякі з найбільш поширених методів захисту інформації включають:

Криптографічні методи: шифрування та дешифрування інформації за допомогою різних алгоритмів, таких як AES, RSA, ECC тощо. Криптографічні методи забезпечують конфіденційність і цілісність даних.

Безпека мережі: використання безпечних мереж із увімкненим шифруванням трафіку, брандмауерам та іншими пристроями безпеки мережі. Це забезпечує безпеку трафіку між комп'ютерами та пристроями в мережі.

Методи автентифікації: використання паролів, біометричних методів, таких як відбитки пальців і розпізнавання голосу, щоб підтвердити особу користувача та гарантувати, що лише авторизовані користувачі мають доступ до систем і даних.

Фізичні методи захисту: використання біометричних методів, відеоспостереження та інших засобів захисту об'єктів, де зберігається цінна інформація, наприклад, використання ключ-карт і біометричний доступ до серверних кімнат.

Аудит безпеки: оцінка ризиків і виявлення слабких місць у системі безпеки для забезпечення захисту від внутрішніх і зовнішніх загроз. Включає аналіз логінів, використання ресурсів та інших показників, які можуть допомогти виявити підозрілу активність і запобігти потенційним атакам.

Безпечне програмне забезпечення: використання методів безпеки в процесі розробки програмного забезпечення для запобігання потенційній вразливості та витоку даних. Це може включати аудит коду, використання підпису програмного коду та інші методи безпеки програмного забезпечення.

Соціальна інженерія: навчання користувачів і підвищення їхньої обізнаності про загрози безпеці, які можуть призвести до витоку даних або інших проблем безпеки. Це може включати навчання, інформацію та регулярні попередження про загрози безпеці.

Ці методи можна використовувати як окремо, так і в комплексі для забезпечення комплексного захисту інформації від можливих загроз. Важливо зазначити, що це постійний процес, і заходи безпеки необхідно підтримувати та оновлювати, щоб забезпечити захист від нових загроз і вразливостей.

Захист інформації в мережах особливо важливий, оскільки мережі використовуються для передачі великих обсягів даних між різними комп'ютерами та системами, що збільшує ризик витоку даних або крадіжки конфіденційної інформації. Нижче наведено деякі додаткові методи безпеки, які можна використовувати для захисту ваших мереж.

Брандмауер: програма або пристрій, який контролює доступ до мережі та має можливість блокувати небажану або небезпечну активність. Брандмауер можна налаштувати так, щоб блокувати доступ до вірусів та інших шкідливих програм, зменшуючи ризик зараження системи.

Віртуальні приватні мережі (VPN): захищений канал даних між двома чи більше комп'ютерами, який забезпечує конфіденційність та інші заходи безпеки. VPN можна використовувати для захисту конфіденційної інформації, яка передається між кількома мережами або пристроями.

Інтегрована мережева безпека: це набір технологій і процедур, які захищають мережу від шкідливих програм та інших загроз безпеці. Це може включати використання програмного забезпечення безпеки, моніторинг мережі, тестування безпеки, криптографічні технології та інші методи.

Автентифікація та авторизація користувача: це процес перевірки облікових даних користувача для надання доступу до мережі та ресурсів. Це може включати використання паролів, біометричних даних, токенів тощо. Також важливо забезпечити регулярне оновлення механізмів безпеки та тестування вразливостей.

Крім того, існують інші методи захисту інформації, такі як захист від вірусів і шкідливих програм, захист від DDoS-атак і багато інших. Кожен із цих методів можна використовувати для захисту мережі, але їх застосування залежить від конкретних потреб і загроз безпеці.

Тому захист інформації в мережах є важливим завданням, оскільки збільшення обсягу даних, що передаються через мережу, створює більше можливостей для злочинців. Використання сучасних методів захисту інформації дозволяє знизити ризик несанкціонованого доступу до конфіденційних даних і забезпечити надійний захист від різних загроз безпеці.

Література

1. Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П. Основи кіберпростору, кібербезпеки та кіберзахисту. 2021р.
2. Эндрю Танєнбаум , Девід Уезеролл. Комп’ютерні мережі (5-е видання). 2012 р.

СПОСОБИ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ ЛІНІЙ ЗВ’ЯЗКУ У СТІЛЬНИКОВИХ МЕРЕЖАХ НОВОГО ПОКОЛІННЯ

Швець Валерія Валеріївна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Стільникові мережі нового покоління, такі як 5G, пропонують широкий спектр нових можливостей і переваг, однак, разом зі зростанням функціональності, постають нові виклики щодо безпеки комунікаційних ліній. Зловмисники постійно шукають способи зламати безпеку мереж і отримати несанкціонований доступ до конфіденційної інформації. Тому важливо вживати ефективні заходи для захисту ліній зв'язку і забезпечення конфіденційності та цілісності даних. [1]

Такими способами для підвищення рівня безпеки ліній зв'язку у стільникових мережах нового покоління можуть бути:

- Застосування шифрування – шифрування є основним засобом захисту даних в стільникових мережах. Використання сучасних алгоритмів шифрування дозволяє захистити передачу інформації від несанкціонованого доступу. Наприклад, використання протоколів шифрування, таких як Advanced Encryption Standard (AES), забезпечує конфіденційність даних і запобігає їх перехопленню зловмисниками.
- Двофакторна аутентифікація – двофакторна аутентифікація є ефективним методом підвищення безпеки ліній зв'язку. При використанні цього методу, крім звичайного пароля, користувач повинен пройти додаткову перевірку, наприклад, ввести одноразовий код, який надійшов на його мобільний пристрій. Це ускладнює заволодіння чужими обліковими записами і зменшує ризик несанкціонованого доступу до ліній зв'язку.
- Системи моніторингу та виявлення загроз – встановлення систем моніторингу і виявлення загроз є необхідним кроком для підвищення безпеки ліній зв'язку. Ці системи дозволяють вчасно виявляти підозрілу активність, вторгнення та інші загрози безпеці. Вони

забезпечують постійний контроль стану мережі і реагують на потенційні загрози, зменшуючи ризик несанкціонованого доступу і втрати даних.

- Фізичний захист – Окрім захисту через програмне забезпечення, необхідно також забезпечити фізичний захист ліній зв'язку. Це може включати захист від несанкціонованого доступу до технічних приміщень, контроль доступу до обладнання і забезпечення фізичної безпеки обладнання передачі даних.

Підвищення рівня безпеки ліній зв'язку у стільникових мережах нового покоління є важливою задачею. Застосування шифрування, двофакторної аутентифікації, систем моніторингу та виявлення загроз, а також фізичного захисту є ефективними способами забезпечення безпеки. Ці заходи допомагають запобігти несанкціонованому доступу до даних і зберегти їх конфіденційність та цілісність. Постійне вдосконалення і розробка нових методів безпеки є необхідними для забезпечення безпечного використання стільникових мереж нового покоління. [2]

З погляду безпеки, нові техніки, що використовуються для покращення продуктивності мережі 5G, також створюють вразливості безпеки. Наприклад, масивні MIMO-системи допомагають маскувати пасивне і активне прослуховування. Реалізація SDN за допомогою технології OpenFlow збільшує загрози від зловмисних додатків або активностей. Крім того, використання технології NFV викликає проблеми безпеки при міграції послуги або функції з одного ресурсу на інший.

Також виникають нові питання щодо конфіденційності через різноманіття бізнес-типів та сценаріїв застосування в мережах 5G. Відкритість платформи означає, що чутлива інформація користувача може легко і часто переходити зі закритого стану до відкритого. Відповідно, стан контакту змінюється з офлайн на онлайн, що значно збільшує ризик витоку даних. Тому питання приватності, з якими ми неодмінно зіткнемося в мережах 5G, стануть проблемою, з якою потрібно буде вирішувати в найближчі роки. На щастя, прогрес у сфері аналізу даних та технологій машинного навчання означає, що методи захисту приватності були добре навчені і стануть ще потужнішими у майбутньому.[3]

Список використаних джерел:

1. Bhadauria, R., R., & Jindal, A. (2020). Enhancing 5G Network Security Using Software-Defined Networking. Journal of Network and Systems Management.

2. Ming, Y., Zhang, H., & Li, X. (2018). Security Enhancement in 5G Mobile Networks with a Hierarchical Structure. IEEE Access.

3. Minghao Wang, Tianqing Zhu, Tao Zhang, Jun Zhang, Shui Yu, Wanlei Zhou (2020). Security and privacy in 6G networks: New areas and new challenges. Електронний ресурс [Режим доступу] – https://www.sciencedirect.com/science/article/pii/S2352864820302431#sec2

ЗАХИСТ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

Семененко К.О.
Київський національний університет будівництва і архітектури, Київ

Обробка інформації в інформаційно-телекомунікаційних системах потребує прийняття спеціальних заходів для забезпечення її безпеки. Загрози інформації в інформаційно-телекомунікаційних системах дуже різноманітні. Виток інформації технічними каналами та несанкціоновані дії з інформацією притаманні інформаційно-телекомунікаційним системам. Тому захист інформації в інформаційно-телекомунікаційних системах технічними засобами є безумовно, актуальною задачею.

Технічному захисту підлягає інформація з обмеженим доступом, яка обробляється, циркулює, відображається в автоматизованих системах і засобах обчислювальної техніки.

Носіями цієї інформації є електричні й електромагнітні поля і сигнали, що утворюються в результаті роботи засобів оброблення інформації з обмеженим доступом (основні технічні засоби) або впливу небезпечного сигналу на засоби оброблення відкритої інформації, на засоби і системи життєзабезпечення (допоміжні технічні засоби і системи).

Канали витоку інформації можуть виникати внаслідок випромінювання інформативних сигналів під час роботи ОТЗ і внаслідок наведення цих сигналів у лініях зв'язку, колах електроживлення і заземлення, інших комунікаціях, що мають вихід за межі контрольованої території. Інформативні сигнали можуть поширюватися на великі відстані і реєструватися засобами технічних розвідок за межами КТ.

Найбільш небезпечними, з погляду несанкціонованого зняття за рахунок побічних електромагнітних випромінювань і наведень (ПЕМВН), є монітори комп'ютерів зі стандартами розгорнень телевізійних систем. В усіх зазначених випадках навіть використання могутніх криптографічних методів захисту інформації не приводить до бажаних результатів, і тільки застосування спеціальних методів і апаратури захисту від ПЕМВН здатне усунути виникаючий канал витоку інформації.

Такими методами є:

1. Доробка пристроїв обчислювальної техніки з метою мінімізації електромагнітних випромінювань (застосування малоенергетичних мікросхем, пристроїв відображення на рідкісних кристалах, локальне екранування окремих пристроїв персональних комп'ютерів, гальванічна розв'язка за ланцюгами електроживлення і т. д.).

2. Електромагнітне екранування приміщень, у яких розташована обчислювальна техніка, а також інше електронне устаткування, використовуване для обробки як аналогової, так і дискретної інформації.

3. Активне радіотехнічне придушення побічних електромагнітних випромінювань і радіотехнічне маскування працюючої апаратури.

Доробка пристроїв обчислювальної техніки дозволяє істотно зменшити рівень побічних електромагнітних випромінювань, однак цілком їх не усуває. Необхідно також зазначити, що електромагнітне екранування вносить певний дискомфорт у роботу користувачів і обслуговуючого персоналу, а в деяких випадках зробити таке екранування неможливо.

Роботи з технічного захисту інформації (ТЗІ) в АС і ЗОТ передбачають: категоріювання об'єктів електронно-обчислювальної техніки; включення до технічних завдань на монтаж АС і ЗОТ розділу з ТЗІ; монтаж АС і ЗОТ відповідно до рекомендацій НД ТЗІ; обстеження (в тому числі технічний контроль) об'єктів електронно-обчислювальної техніки; установлення (при необхідності) атестованих засобів захисту; технічний контроль за ефективністю вжитих заходів.

Для захисту інформації від витоку технічними каналами застосовується:

- активний метод, а саме просторове зашумлення радіосигналом типу білий шум;
- пасивний метод із застосуванням фільтру низьких частот по мережі живлення основних та додаткових технічних засобів.

Перелік використаної літератури:

1.Андреев В.І. Стратегія управління інформаційною безпекою: підручник / В.І.Андреев, В.Д.Козюра, Л.М.Скачек, В.О.Хорошко. – К.: Вид. ДУІКТ, 2007. – 277 с.

2.Блавацька Н.М. Програмне забезпечення систем захисту інформації: підручник / Н.М.Блавацька, В.Д.Козюра, В.О.Хорошко. – К.: Вид. ДУІКТ, 2011. – 330 с.

3.Гайворонський М.В. Безпека інформаційно - комунікаційних систем / М.В.Гайворонський, О.М.Новиков. - К.: Видавнича група BHV, 2009. - 608 с.

4.Гребенніков В. Комплексні системи захисту інформації. В. Гребенніков — «Издательские решения», 2019.

СЕКЦІЯ 4

Соціально-економічні аспекти розвитку телекомунікацій

КЛЮЧОВІ ЕКОНОМІЧНІ КОНЦЕПЦІЇ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ В УКРАЇНІ

Качмала Вікторія Іванівна
канд.істор. наук, доцент
Державний університет телекомунікацій
Навчально-науковий інститут
менеджменту та підприємництва
kacmalaviktoria@gmail.com

Сучасні виклики, що постали перед українським суспільством, нові умови господарювання, вимагають стимулювання розвитку високотехнологічного виробництва з використанням технологій середньо-високого рівня. Ринок телекомунікацій в даний час стоїть на передовій технологічного та цифрового розвитку держави, на операторів покладаються величезні надії та надії щодо забезпечення країни повноцінним мобільним та інтернет-зв'язком. Окрім цього, дуже важливі наступні чинники: авторизація кредитних карток, передавання телеметричних даних, охоронна сигналізація, організація платежів населення, забезпечення міжстанційних зв'язків між базовими станціями систем персонального виклику, електронна та голосова пошта, і телевідеоконференцзв'язок, доступ до Інтернет, комп'ютерна телефонія тощо[1,с.19]. Питанням дослідження проблем та перспективам розвитку телекомунікаційного ринку присвятив свої роботи. Кулаков В. О [2], досліджували стан та перспективи розвитку ринку телекомунікаційного зв’язку в Україні Гранатуров В.М. та Л.А. Захарченко, В.М. [1], визначенням співвідношення показників розвитку галузі із загальними тенденціями економіки України займається Седікова І. О. [3].

Науковці стверджують, що ключові економічні концепції залежать від багатьох факторів: результатів інтелектуальної праці, технологічних розробок, удосконалення економічної діяльності. Вони формують результат практичного освоєння нового процесу, продукту або послуги та являють собою матеріалізований результат, отриманий від вкладення капіталу в нову техніку чи технологію, у нові форми організації виробництва праці, обслуговування, управління і т.п. Однією з важливих аспектів постає також і інноваційна діяльність, що передбачає цілий комплекс наукових, технологічних, організаційних, фінансових і комерційних заходів підприємств: перепідготовка персоналу для застосування нових технологій та обладнання; – маркетинг нових продуктів, що передбачає види діяльності, пов’язані з випуском нової продукції на ринок, включаючи попереднє дослідження ринку, адаптацію продукту до різних ринків, рекламну кампанію; – придбання «неречовинних» технологій у формі патентів, ліцензій, відкриття, «ноу-хау», торгових марок, конструкцій, моделей і послуг технологічного змісту; – придбання упредметненої технології – машин і обладнання, за своїм технологічним змістом пов’язаних з впровадженням на підприємстві продуктових чи процесних інновацій; – виробниче проектування, що включає підготовку планів і креслень для визначення виробничих процедур, технічних специфікацій.

Список використаних джерел:

1. В.М. Гранатуров, Л.А. Захарченко, В.М. Економіка телекомунікацій: навч. посіб. – О.: ОНАЗ, 2015. – 140 с.

2. Грицуленко С.І. Інтелектуальна власність в галузі зв'язку [Текст]: навч. посіб. [для студ. вищ. навч. закл.] / Грицуленко С.І., Потапова-Сінько Н.Ю., Гарбера К.М. – О.: ОНАЗ ім. О.С. Попова, 2011. – 394 с
3. Седікова І. О. Сучасний стан розвитку телекомунікаційного простору України / І. О. Седікова // Економічний вісник. Збірник наукових пр. МДУ. Мукачево, 2020, 214 с.

УДК 005.915:658.14/.17

РОЗВИТОК ТА ВПРОВАДЖЕННЯ СУЧАСНИХ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ УПРАВЛІННЯ ФІНАНСАМИ НА ПІДПРИЄМСТВАХ

Єрема В.О.
здобувач вищої освіти бакалаврського рівня 3-го курсу
КНЕУ імені Вадима Гетьмана
Науковий керівник – ст. викладач кафедри корпоративних фінансів і контролінгу
Круш В.В

На сьогодні, процес управління фінансами сучасних підприємств має бути розроблений з урахуванням інноваційних інформаційних систем, які стають дедалі популярними у фінансовому менеджменті та які базуються на засобах інтелектуальної обробки даних. Завдяки застосування інтернет-технологій вдосконалюються бізнес-процеси, наприклад: розрахунки, аналіз, управління та контроль, облік, звітність, а також з'являється можливість дистанційної обробки фінансових даних, відшкодування, аудиту, моніторингу і т. д. Нова модель фінансового менеджменту дає всі умови підприємствам створити централізоване управління, через мережі передачі даних й обміну даних, також створюється тісна взаємодія між внутрішніми відділами підприємства та іншими компаніями[1].

Наразі, усе частіше незалежні дослідники, консультанти й самі користувачі корпоративних систем наголошують на тому, що впровадження ERP-систем керівництво компаній залишаються поза використання даних систем. Дирекція підприємства після впровадження ERP-системи продовжує користуватися паперовими звітами. Нова система є обліковою програмою з наявними ознаками «обривистої» автоматизації, що охоплює тільки робітників та керуючих відділів, а топ-менеджмент досі працюють з «паперовою» інформацією.

Паралельно з розвитком ERP з'явилися OLAP-системи для аналізу та обробки інформації в реальному часі. Користувачі-аналітики віддають перевагу додаткам, які максимально відповідають їх уявленню про природу даних. Для більш наочного представлення даних використовують тривимірну модель, яка подібна до куба. Однак, додавання додаткових атрибутів статистики продажів може призвести до перевантаження нашої уяви.

Найбільша перевага OLAP-системи порівняно з ERP – автономність від внутрішньої служби автоматизації, набагато швидше задовольняє керівництво компанії аналітичними можливостями інформаційної системи. Менеджмент може бути безпосередньо залученим до розвитку інформаційних технологій власного підприємства. Участь керівництва в процесі побудови інформаційної системи є ключовим фактором успіху будь-якого проєту автоматизації.

З часом, реальною загрозою для ERP-систем стали OLAP-системи через те, що перевагами OLAP є те, що вона є інтерактивною системою, яка дозволяє у режимі реального часу (миттєво, без очікування на результат запиту) переглядати різні підсумки по багатовимірних даних, тому замовники почали частіше купувати аналітичні додатки як інтеграційний інструмент для своєї "клаптевої" автоматизації. Більшість виробників ERP-

систем сьогодні розробляє свої власні OLAP-додатки або тісно інтегрується з виробниками гарних OLAP, щоб запобігти цій тенденції.

Фінансовий менеджмент загалом має три класичні фази управління – планування, облік та контроль. Повноцінна автоматизація даних завдань завдяки тільки інструментів обліку чи тільки інструментів аналізу є неможлива. Для прикладу візьмемо функцію планування. Для реалізації цього завдання необхідні як мінімум дані, що випливають із кредиторській заборгованості [2]:

- Рахунку до оплати.
- Відкриті позиції (заборгованість у розрізі постачальників).
- Контракти на поставку.
- Замовлення на поставку.
- Платежі (поточні й планові).
- Бюджетні статті.

Фінансове планування включає безліч інших функцій управління, які складаються з багатьох етапів. Однією з них є бюджетування, ця складова як процес встановлення деталей і узгодження бізнес-цілей підприємства, також потребує механізму, який об'єднує зусилля багатьох користувачів в рамках єдиного інформаційного простору. Оскільки бюджетування має декілька етапів, таких як планування, облік і контроль, вони неминуче перетинаються між собою завдяки ітеративному характеру самого процесу бюджетування. Бюджетування загалом є частиною фази фінансового менеджменту - планування.

Велика кількість OLAP-виробників, усвідомивши необхідність у додатках такого роду, почали створювати версії, спеціалізовані для автоматизації завдань фінансового менеджменту з бюджетування, фінансового планування, аналізу й контролю[2].

Також, дуже зручними та швидкими є, BPM додатки - це програмні засоби, призначені для автоматизації та оптимізації бізнес-процесів в організації. Вони дозволяють створювати, моделювати, виконувати та контролювати бізнес-процеси в режимі реального часу, а також здійснювати аналіз ефективності цих процесів.

Аналітична функціональність BPM-додатків дає змогу швидко складати звіти, використовуючи елементи вимірів, що можуть бути розміщені у вікні аналітики та створювати «куб даних» прямо на екрані. Куб даних в інформаційній технології відноситься до методу організації, зберігання і аналізу даних. В основі концепції куба даних лежить ідея опису даних за кількома вимірами або аспектами. Кожен вимір представляє певну характеристику даних, і ці виміри утворюють вимірні простори, які утворюють багатовимірну структуру. Крім того, "контрольні агенти" BPM дозволяють виявляти відхилення фактичних показників від планових і повідомляти про них вчасно. Якщо менеджер вже знайомий з системою, вона може запропонувати деякі можливі варіанти вирішення проблем.

Отже, ERP-додатки мають такі обмеження у своєму функціоналі: : довгий строк упровадження; неповне охоплення підрозділів; обмеженість аналітичних можливостей; «клаптикова» охопленість пацівників додатком. Клаптикова охопленість в ERP додатках відноситься до рівня деталей, на якому дані збираються, зберігаються і аналізуються в системі. Це означає, що клаптикова охопленість визначає рівень глибини і докладності, з якою дані представлені в ERP-системі. Саме тому на сучасному етапі розвитку інформаційних технологій більш пріоритетним інструментом проведення аналізу даних фінансовим менеджментом підприємства є здійснення цього процесу з використанням OLAP-додатків. Проте, дані додатки теж мають свої обмеження щодо їх використання: спеціалізація на аналізі подій, що відбулися, без елементів прогнозування; відсутність можливості побудови «куба/звіту/форми». Щодо BPM-додатків, то вони автоматизують управлінські стратегії. Для того аби побудувати корпоративну систему управління необхідно впровадити додатки ERP, BPM, і OLAP. Для ефективного впровадження програмних додатків важливо дотримуватися послідовності фаз управління. Спочатку необхідно пройти процес планування, а потім перейти до фази обліку.

Тільки після цього можна розпочати побудову корпоративної системи управління, що автоматизує функції управлінського аналізу, оцінки бізнес-процесів сучасного вітчизняного підприємства задля прийняття найефективніших управлінських рішень щодо розвитку бізнесу для досягнення ним стратегічних цілей.

ВИКОРИСТАННІ ДЖЕРЕЛА:

1. Курков М.С. Концептуальна модель системи управління фінансами підприємств із застосуванням сучасних інформаційних технологій. 2019 URL: http://www.econ.vernadskyjournals.in.ua/journals/2019/30_69_5/30_69_5_1.pdf#page=148 (дата звернення: 12.05.2023)
2. Курков М.С., Гіваргізов І.Г. Розвиток та впровадження сучасних інтелектуальних систем управління фінансами на підприємствах. 2019 URL: http://www.econom.stateandregions.zp.ua/journal/2019/2_2019/2_2019.pdf#page=94 (дата звернення: 12.05.2023)
3. Жусь О.М., Ракицька С.О., Тожиєва Г.М. Стабілізація діяльності підприємств будівельної галузі через впровадження ERP-системи. 2023 URL: http://dees.iei.od.ua/index.php/journal/article/view/122 (дата звернення: 16.05.2023)

УДК 657.15:334.78]:004

.

ЗАСТОСУВАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ У КОРПОРАТИВНИХ ФІНАНСАХ

Леонова Б.І.
здобувач вищої освіти бакалаврського рівня 3-го курсу
Київський національний економічний університет імені Вадима Гетьмана
Науковий керівник – ст. викладач кафедри корпоративних фінансів і контролінгу
Круш В.В

У сучасному світі інформаційні технології займають все більш важливе місце у розвитку корпоративних фінансів. Інформаційні системи та технології допомагають підприємствам оптимізувати фінансові процеси, збільшувати ефективність управління ресурсами та знижувати витрати.

Інформаційні системи бухгалтерського обліку є важливою частиною корпоративних фінансів, оскільки вони допомагають автоматизувати бухгалтерські процеси, забезпечують точність та надійність фінансової звітності. Ці програмні продукти забезпечують планування, моніторинг, аналіз та управління фінансами компанії, що дозволяє приймати обґрунтовані управлінські рішення на основі достовірної інформації. У цьому контексті корпоративні фінанси стають більш ефективними та результативними завдяки застосуванню інформаційних систем бухгалтерського обліку.

Сучасні реалії бізнесу в Україні вимагають пошуку альтернативних програмних рішень і заміни монополій на автоматизацію бізнес-процесів, таких програмних продуктів, як «1С» і «BAS». З початку 2017 року в Україні під санкції потрапили компанії, які володіють правами на російські програми автоматизації бізнесу «1С» і «BAS». Заборона використання даних програмних продуктів не дозволяє використовувати їх у державних установах, ці програми можна використовувати лише у приватному секторі [1]. Це потребує заміни програмного забезпечення та навчання працівників роботі з новою технологією.

Прийняття ефективних управлінських рішень у корпоративних фінансах абсолютно залежить від належної організації бухгалтерського обліку, використання відповідної інформації

та програмного забезпечення. Якщо програмні продукти для автоматизації обліку, аналізу та оцінки бізнес-процесів корпоративного підприємства будуть чітко налаштовані і максимально правильно підібрані, то це забезпечить найвищу загальну ефективність управління бізнесом і допоможе в організації облікових процесів. Таким чином, за рахунок правильного застосування програмних продуктів для автоматизації бухгалтерського обліку можна оптимізувати ефективність використання наявних фінансових ресурсів корпоративного підприємства.

Найбільш розповсюдженими серед програмного забезпечення для обліку в Україні є такі продукти [2]:

1. «BOOKKEEPER SaaS» – актуальне, сучасне програмне рішення для українських бухгалтерів та фінансових аналітиків. для аутсорсингових бухгалтерів. У програмі можна працювати одночасно з клієнтами без втрати функціональності. Робітники компанії можуть самостійно складати основні документи, бухгалтерам залишається тільки перевірити правильність даних і скласти звітність. Програмний продукт розроблений для роботи з неприбутковими організаціями, ФОП та юридичними особами. Інтеграція з Приват-24, забезпечує прискорення документообігу між бухгалтерами та контрагентами, допомагає вести оперативний та податковий облік ФОП, відстежувати рух коштів і товарів. Податкові звіти готуються програмою автоматично, а банківські виписки можна завантажити у форматі DBF.

2. «MASTER:Бухгалтерія» – комплексний модуль для автоматизації бухгалтерського обліку на підприємствах малого та середнього бізнесу, а також бюджетних установах. Програма інтегрується з банком клієнта, спрощуючи роботу з рахунками. Можна обліковувати продажі, закупівлі, залишки запасів і фактичні виробничі витрати. Фінансові звіти формуються автоматично. Цей інтерфейс налаштовується користувачем індивідуально. Захист систем захищено від помилок, втрати важливої інформації та людського фактора.

Однією із сильних сторін «MASTER:Бухгалтерія» є поєднання всіх напрямків бухгалтерського обліку в одній програмі, з єдиним сховищем усіх даних у всіх модулях, гарантуючи при цьому цілісність інформації.

Програмний продукт "MASTER:Бухгалтерія" розроблений компанією IT-Enterprise, яка успішно функціонує на ринку з 1987 року та має велику клієнтську та партнерську базу в різних країнах світу, зокрема в Європі, Америці та Азії. В Україні компанія встановила плідну співпрацю з провідними організаціями, такими як МХП, Megogo, Roshen, Ferrexpo, Укрпошта, Укрнафта, Епіцентр [1].

3. Програмний продукт "M.E.DOC" допомагає взаємодіяти з документами різних форматів, видів та призначень, забезпечує можливість обміну документами з партнерами та подання звітності до контролюючих органів.

4. «SMARTFIN.UA» є програмою для обліку малих підприємств. Вона дозволяє збирати необмежену кількість ФОП в одному акаунті, щоб уникнути перемикання і втрати даних. Програма дає змогу вести бухгалтерський облік з мобільного телефону чи планшета, що дозволяє уникнути прив’язки до стаціонарного ПК. Бухгалтерський облік може здійснюватися як фахівцем, так і самостійно підприємцем.

Програмні продукти «SAP», «Microsoft», «Oracle» та «Odoo» від іноземних розробників є серед найбільш популярних замінників російських облікових програм «1С» та «BAS».

«SAP» є міцною платформою з безліччю функцій, створена німецькою компанією SAP, яка спеціалізується на виробництві корпоративного програмного забезпечення та наданні підтримки програм для підприємств будь-якого масштабу в усьому світі.

«Microsoft Dynamics» – інтегрована комплексна система управління підприємством, яка об’єднує такі функції, як управління фінансами, аналіз бізнес-процесів, управління виробництвом, логістика, електронна комерція та взаємодія з клієнтами [2].

«Oracle» – це потужна система для великих підприємств, а «Odoo» – це набір програмного забезпечення з відкритим кодом, який включає в себе рішення для всіх потреб

компанії, такі як CRM, бухгалтерський облік, управління складом, електронна комерція, точка продажу, проєктний менеджмент та інші.

Наведений перелік програмних продуктів бухгалтерського обліку не є вичерпним. На українському ринку існує величезна кількість бухгалтерського програмного забезпечення.

Багато малих підприємств використовують Microsoft Excel для бухгалтерського обліку. Використання даної програми полегшує процес роботи з вихідними документами та полегшує формування стандартної бухгалтерської звітності.

Однією з сильних сторін програми є можливість заповнювати звіти в таблиці Excel і надавати інформацію в необхідному форматі після завантаження зі спеціалізованої бухгалтерської програми. Однак суттєвим недоліком «Microsoft Excel» є його обмежені можливості для більш складного обліку, який може включати не більше 10-15 операцій і невелику кількість товарних позицій на місяць. [3, с. 151].

Отже, сьогодні ринок програмного забезпечення представлений великою кількістю автоматизованих інформаційних систем, здатних задовольнити потреби навіть найвимогливіших користувачів.

Використання інформаційних систем в управлінні бізнесом може мати значний вплив на фінанси підприємства. Це дає змогу зменшити складність прийняття рішень та підвищити ефективність обробки фінансових даних, що є запорукою прийняття об’єктивних та ефективних фінансових та управлінських рішень. Керівники підприємств можуть розглянути певні особливості програмного забезпечення бухгалтерського обліку, яке вони використовують, і зробити найкращий вибір для свого бізнесу, щоб досягти успіху в бухгалтерському обліку та бізнес-фінансах.

Список використаних джерел:

1. Грибовська Ю. М., Кононенко Ж. А. Застосування інформаційних систем в управлінні підприємством. [Електронний ресурс] / Ю. М. Грибовська, Ж. А. Кононенко // *Економіка та суспільство*. – 2023. – URL: https://www.economyandsociety.in.ua/index.php/journal/article/view/2171/2098.

2. Кривецький І. Альтернатива 1С в Україні: огляд українських та іноземних аналогів. URL: https://www.oneservice-consulting.com/alternatyva-1c-v-ukraini-ogljad-ukrainskyh-ta-inozemnyh-analogiv

3. Пономарьова Т. В., Матюшко М. М. Аналіз програмних продуктів, які використовуються для автоматизації бухгалтерського обліку суб’єктами підприємницької діяльності. *Соціальна економіка*. 2021. Вип. 62.С. 148–156.

УДК 336.225.611:004-047.64

АВТОМАТИЗАЦІЯ ФІНАНСОВИХ ПРОЦЕСІВ З ВИКОРИСТАННЯМ ІНФОРИАЦІЙНИХ СИСТЕМ

Корягіна Катерина Олександрівна
Студентка Київського національного економічного університету імені Вадима Гетьмана

Сучасна економіка немислима без фінансових процесів, які забезпечують раціональне використання ресурсів та забезпечують стабільність фінансової системи країни. Автоматизація фінансових процесів є необхідною умовою для ефективного управління фінансами в сучасних умовах. Використання інформаційних систем у фінансовому менеджменті дає можливість підвищити якість та швидкість прийняття рішень, зменшити ризики та покращити управління фінансовими ресурсами. Автоматизація фінансових процесів з використанням інформаційних систем дозволяє значно зменшити трудомісткість рутинних операцій, підвищити точність та

швидкість обробки даних, забезпечити збереження та надійність інформації, що обробляється. За допомогою фінансових інформаційних систем можна вести облік фінансових ресурсів, планувати та контролювати фінансову діяльність підприємств, проводити аналіз фінансових результатів та приймати рішення щодо їх оптимізації [1, с.24-32].

Україна не залишається осторонь процесів автоматизації фінансових процесів та використання інформаційних систем в цьому процесі. Сьогодні на ринку України існує велика кількість фінансових інформаційних систем таких, як: клієнт-банкінг, ERP-системи, Приват24, iPay, Portmone, які надають можливість автоматизувати рутинні процеси та забезпечувати повний контроль за фінансовими операціями. При цьому, використання інформаційних систем в фінансовому менеджменті дозволяє забезпечити більш точний та оперативний облік фінансових операцій, а також ефективніший контроль над ними.

Варто також зазначити, що автоматизація бізнес-процесів корпоративних підприємств має дуже багато переваг, серед яких можна виділити зниження витрат: автоматизація дозволяє знизити витрати на зарплату працівників, витрати на папір та інші матеріали, а також витрати на послуги зберігання даних. Також забезпечення точності та надійності, оскільки автоматизація дозволяє уникнути помилок, які можуть виникнути при ручному виконанні бізнес-процесів, а також зменшити ризик втрати даних та інформаційної безпеки.

Одним із вагомих чинників, який вплинув на активізацію використання новітніх фінансових інформаційних систем є прийняття Закону України «Про електронні документи та електронний документообіг», який визначає правові засади та принципи електронного документообігу в Україні. Згідно з цим законом, електронні документи мають таку ж юридичну силу, як і паперові документи. Державний агент з питань електронного урядування в Україні відповідає за розробку та впровадження систем електронного документообігу. За допомогою цієї системи, можна забезпечити повну автоматизацію процесів збереження, обміну та обробки фінансової інформації. Це дозволяє знизити трудомісткість та часові затрати на обробку документів, а також забезпечити їх безпеку та надійність [2].

Одним з прикладів використання фінансових інформаційних систем може слугувати система електронного декларування в Україні. Це онлайн-платформа, створена з метою забезпечення прозорості та боротьби з корупцією в державному секторі. За допомогою цієї системи публічні службовці можуть зручно та швидко подавати електронні декларації та редагувати їх в будь-який час. Також система автоматично перевіряє декларації на предмет відповідності законодавству та забезпечує доступ до них широкому загалу через веб-сайт NACP (Національне агентство з питань запобігання корупції).

Зокрема, система електронного декларування забезпечує:

- Зручне та безпечне подання декларацій
- Автоматичну перевірку декларацій на відповідність законодавству
- Публікацію декларацій на веб-сайті NACP
- Аналітичні звіти з даних, що містяться в деклараціях, для забезпечення моніторингу та контролю
- Автоматичну генерацію відповідних повідомлень та повідомлень про можливі порушення законодавства [3].

Однак, разом із перевагами, використання фінансових інформаційних систем також може створювати деякі ризики та проблеми. Наприклад, можливість зламу системи та несанкціонованого доступу до фінансової інформації, або недостатня якість програмного забезпечення, яке може призвести до помилок у фінансовому обліку [4, с.79-85].

Отже, використання фінансових інформаційних систем в Україні дозволяє підвищити ефективність та якість управління фінансовими ресурсами. Автоматизація фінансових процесів дозволяє знизити трудомісткість та збільшити точність та швидкість обробки фінансової інформації. Однак, важливо пам'ятати про можливі ризики та проблеми, які можуть виникнути при використанні інформаційних систем в фінансовому менеджменті. Необхідно приділяти

достатню увагу увагу питанням безпеки та захисту фінансової інформації від несанкціонованого доступу та зламів.

Україна вже має досвід успішного впровадження фінансових інформаційних систем, але необхідно продовжувати розвивати цю галузь, забезпечувати доступність нових технологій для фінансових установ та підвищувати кваліфікацію фахівців у галузі інформаційних технологій та фінансів.

Список використаних джерел

1. Глущенко, А.В. (2019). Автоматизація фінансових процесів підприємства: ефективність та переваги використання / А.В. Глущенко // Наукові праці інституту підприємництва та соціальних технологій КНТЕУ. - № 1. - С. 24-32.

2. Закон України «Про електронні документи та електронний документообіг» // Відомості Верховної Ради України. –2003. – № 851-IV, поточна редакція — Редакція від 01.08.2022.

URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

3. Національне агентство з питань запобігання корупції (2021). Електронна система декларування: система запобігання та протидії корупції [Електронний ресурс].

URL: https://nazk.gov.ua/uk/

4. Шарова, О.А. (2020). Використання фінансових інформаційних систем в управлінні фінансовими ресурсами / О.А. Шарова // Наукові записки Національного університету "Острозька академія". Серія "Економіка". - Т. 26. - С. 79-85.

ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ ТА АНАЛІТИКИ ДАНИХ ДЛЯ ВДОСКОНАЛЕННЯ БІЗНЕС-ПРОЦЕСІВ

Пашков С. І.

Державний університет телекомунікацій, м. Київ

Використання машинного навчання та аналітики даних для вдосконалення бізнес-процесів є важливим і перспективним напрямом в сучасному світі. За останні роки зростає обсяг даних, які генеруються бізнесом, і важливість їх аналізу та використання. В цьому контексті машинне навчання та аналітика даних надають компаніям можливість здійснювати обґрунтовані рішення на основі об'єктивних даних і покращувати ефективність бізнес-процесів.

Аналіз даних та застосування алгоритмів машинного навчання дозволяють виділяти недосяжні людському оку зв'язки та шаблони. Це дозволяє бізнесу отримувати нові уявлення про свої клієнтські потреби, ринкові тенденції та інші фактори, які впливають на бізнес-процеси. Аналіз даних з використанням машинного навчання допомагає зрозуміти специфіку клієнтських переваг і попередити майбутні тренди [2, с. 102-103].

Крім того, машинне навчання та аналітика даних сприяють автоматизації бізнес-процесів та швидкому прийняттю рішень. Розробка моделей машинного навчання дозволяє автоматизувати процеси та знижувати час, витрачений на прийняття рішень. Алгоритми машинного навчання можуть самостійно навчатись на основі даних та забезпечувати точні прогнози, що робить можливим швидке реагування на зміни в бізнес-середовищі [1, с. 5].

Використання машинного навчання та аналітики даних дозволяє прогнозувати та оптимізувати бізнес-процеси на основі аналізу великого обсягу даних. Машинне навчання та аналітика даних допомагають створити прогностичні моделі, які можуть передбачати поведінку клієнтів, попит на товари та інші фактори, що впливають на бізнес-процеси. Застосування таких моделей дозволяє ефективно планувати виробництво, запаси, маркетингові кампанії та інші бізнес-процеси [3, с. 73-75].

Застосування машинного навчання та аналітики даних в бізнесі є обґрунтованою стратегією для вдосконалення бізнес-процесів. Вони дозволяють виявляти складні зв'язки, автоматизувати процеси та прогнозувати майбутні результати, що призводить до підвищення ефективності та конкурентоспроможності підприємства.

Список використаних джерел

1. Олсон, К., Ерікасон, М. "Machine Learning: The High-Interest Credit Card of Technical Debt".
2. Пропоска, Ф., Фаулер, Т. Data Science for Business.
3. Сігель, Е. Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die.

ІНТЕЛЕКТУАЛЬНА АНАЛІТИКА ВЕЛИКИХ ДАНИХ ДЛЯ ПІДПРИЄМСТВ МАЙБУТНЬОГО

Грищенко Ярослав Олександрович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

Великі дані (big data) стали поширеним словом у бізнесі, а їхні можливі переваги отримують все більшу увагу з боку бізнесу в усьому світі. Переважна кількість даних, що збираються, зберігаються і передаються через нові технології, змінюють пріоритети для багатьох підприємств. Розробка нових аналітичних інструментів теж підлаштовується під вимоги бізнесу.

Почнемо з того, що термін big data стосується насамперед величезної кількості даних, які постійно збираються за допомогою пристроїв і технологій, таких як кредитні картки та картки лояльності клієнтів, Інтернету та соціальних медіа, а також через датчики WiFi і електронні мітки. Велика частина цієї інформації є обмежено структурованою – тобто це дані, які відповідають певній, заздалегідь встановленій моделі даних. Як правило, їх необхідно адаптувати до цілей використання, оскільки дані збираються за критерієм обмеженості сховища, а не вичерпності [1].

Технологія big data включає в себе зберігання інформації (наразі пов’язане з хмарними технологіями), її структурування (застосовують програмні рішення та платформи) та управління і аналіз (обробка та створення аналітичних звітів). Метою використання великих даних є [2]:

- покращення процесу прийняття рішень;
- управління ризиками;
- розвиток нових продуктів;
- підвищення маржі та ін.

Аналіз великих даних стає повсякденним завданням для компаній в усьому світі та для українських компаній зокрема. Понад 90% компаній підтвердили це, відповівши, що тією чи іншою мірою стикаються із завданням аналізу великих даних. Завдяки розвитку технологій і скороченню вартості систем зберігання сьогодні компанії можуть збирати та зберігати великі обсяги різнорідних даних. Важливий крок щодо вилучення знань і користі з таких даних – це завдання, яке належить зрештою вирішувати всім компаніям, які прагнуть зберегти свою конкурентоспроможність і місце на ринку [3].

Серед тих компаній, які сьогодні успішно просуваються в цьому напрямі, виділяються

великі організації приватного та державного сектору, які накопичили великі обсяги даних і, найголовніше, поставили перед собою завдання пошуку інформації та знань, корисних для їхньої діяльності. Залученість бізнесу і підтримка з його боку дуже важливі для успішних ініціатив по роботі з даними, як і правильний інструментарій, що дає змогу ефективно витягувати знання з великих обсягів даних. Необхідність вирішення цього завдання призвела до появи нових спеціальностей і посад співробітників, робота яких безпосередньо пов'язана з даними.

Очевидно, що вплив великих даних на бізнес є частиною більш глибокого процесу. Якщо взяти до уваги роботу Карлоти Перес, стосовно довгострокових технологічних хвиль, то в широкому контексті, big data є наступною хвилею після ери комунікацій та інформації [4]. За прогнозами застосування big data зросте в галузях виробництва, транспортування і логістики з тенденцією розвитку «Промисловості 4.0» (поява кіберфізичних систем). На сьогодні аналітику даних найбільше застосовують у сферах клієнтського обслуговування та внутрішньої операційної ефективності. Якщо брати до уваги тенденції зростання впливу економіки, основаної на даних (data driven economy) то очікується найбільше застосування великих даних для підтримки прийняття рішень, прогнозування, моделювання та візуалізації.

Висновки: Висновок полягає в тому, що використання інтелектуальної аналітики великих даних є важливим інструментом для підприємств майбутнього, які прагнуть до ефективнішого та інноваційного виробництва. Для цього необхідно забезпечити якісний збір та обробку даних, використовуючи сучасні технології, та використовувати методи машинного навчання для аналізу та оптимізації виробничих процесів. Також з’ясовано, що поява великої кількості даних в цифровому форматі, через технології їхнього зберігання та обчислення і до математичних інструментів аналізу цих даних призводить до трансформації в бізнес-процесах. Разом зі стрімким накопиченням інформації швидкими темпами розвиваються і технології аналізу даних. Таким чином компанії створюють додану цінність завдяки застосуванню big data.

Список використаних джерел:

1. Beyer M.A., Laney D.The Importance of “Big Data”: A Defiition [Electronic resource] / MarkA. Beyer, Douglas Laney // Gartner Inc. — Electronic data. — [Stamford: Gartner, 2012]. — Mode of access: World Wide Web: http://www.gartner.com/id=2057415/ (viewed on October 11, 2017). — Title from the screen.

2. Золотников Я., Бондарьов О. Друга нафта. В Україні з'явиться онлайн-курс з Big data — найбільш затребуваної в світі IT-професії [Електронний ресурс] / Ярослав Золотников, Олексій Бондарьов // Новое Время: електронний журнал. — Електронні дані. — [Київ: Новое Время, 2016]. — Режим доступу: http://nv.ua/ukr/science/druga-naftu-v-ukrajini-z-javitsja-onlajn-kurs-po-big-data-najbilsh-zatrebuvanoju-v-sviti-itprofesiji-89806.html

3. Perez C. Tecchnological revolutions and techno-ecoonomic paradigms [Electronic resource] / C. Perez. // Technology Governance. — Electronic data. — [Tallinn, Tallinn University of Technology, 2009]. — Mode of access: World Wide Web: http://technologygovernance.eu/files/main/2009070708552121.pdf

4. Cavanillas J. M. Curry E., Wahlster W. New Horizons for a Data-Driven Economy. A Roadmap for Usage and Exploitation of Big Data in Europe [Electronic resource] /José María Cavanillas, Edward Curry, Wolfgang Wahlster // Big Data Usage. — Electronic data. — [Springer, Cham, 2016]. Mode of access: World Wide Web: https://link.springer.com/chapter/10.1007/978-3-319-21569-3_8

АНАЛІЗ РОЗВИТКУ РИНКУ РОЗУМНОГО БУДИНКУ

Лісогор Гліб Денисович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

У 2021 році світовий ринок розумного дому оцінювався в 62,69 мільярда доларів США, і очікується, що з 2022 до 2030 року він зростатиме на 27,04% у середньому за рік рис.1. Продукти розумного дому представлені камерами безпеки, розумними світильниками, потоковими пристроями, посудомийні машини тощо. Очікується, що тенденція використання штучного інтелекту в побутовій техніці для розумних функцій збільшить попит на продукцію. Крім того, зростаюче проникнення Інтернету та смартфонів стимулює тенденцію до пристроїв розумного дому, підключених до Інтернету та смартфонів.

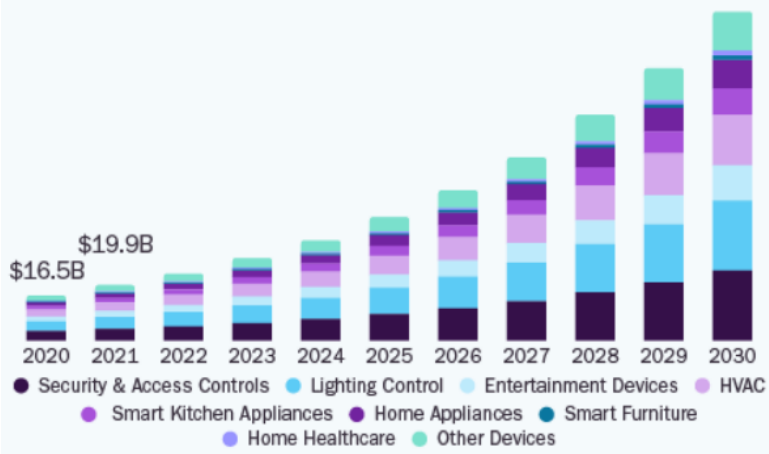


Рис.1. Прогноз світового ринку розумного дому

Цифрова допомога, інтегрована зі штучним інтелектом, пропонує користувачам зручне розгортання розумних пристроїв, що суттєво впливає на переваги покупця. Поширення цифрових помічників, зокрема Alexa, Google Assistant, Siri та Bixby, дає змогу керувати розумними пристроями за допомогою голосових команд. Нові функції цих цифрових помічників, такі як керування динаміками Bluetooth і перегляд каналів, стимулюють попит на пристрої для розумного дому на ринку. Крім того, покупці віддають перевагу персоналізованим пристроям за їх зручність і кращий досвід користувача.

Швидке впровадження сучасних технологій, таких як Інтернет речей (IoT), блокчейн, розумне розпізнавання голосу, штучний інтелект (ШІ) та інші, мало значний вплив на зростання ринку. Завдяки цій технології продукти розумного дому розпізнають голос користувачів і дають їм персоналізовані відповіді. Збільшення темпів впровадження Інтернету речей у регіонах, що розвиваються, і розвинених регіонах сприяло розвитку ринку розумних будинків. Здатність технологій забезпечити взаємозв’язок між пристроями допомогла створити подальший попит на ринку.

Пандемія COVID-19 призвела до зупинки промисловості та вплинула на виробництво. Пандемія порушила операційну ефективність і вплинула на ланцюжки створення вартості через необдумане закриття міжнародних і національних кордонів, що призвело до збитків і втрати прибутку. Існуючі розумні продукти, такі як телевізори та холодильники, залишалися популярними, оскільки вони сприяли попиту на розваги та зручність клієнтів, які були змушені

залишатися вдома. Ланцюжок створення вартості мав несприятливий вплив на постачання сировини, вплинувши на розвиток ринку розумних будинків.

Незважаючи на наявність розбіжностей у ланцюжках поставок, пандемія та її вплив виявили значні недоліки в секторах цифрових пристроїв та інтернет-інфраструктури, для усунення яких потрібен час. Розумну побутову техніку під час локдауну придбали багато людей. Через скорочення поставок і відставання виробництва не вистачало доступних напівпровідників для підтримки розумних продуктів. Це також вплинуло на компанії, які виробляють продукти, пов'язані з розумним будинком.

Список використаних джерел:

1. M. M. Noor, W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey", Computer Networks, Vo. 148, 2019, pp. 283–294.

2. Y. Ismail, "IoT and Smart Home Automation", book, IntechOpen Publisher, 2019.

АНАЛІЗ ЗАКОНОДАВСТВА ЄВРОПЕЙСЬКОГО СОЮЗУ В СФЕРІ ТЕЛЕКОМУНІКАЦІЙ

Тишик Вікторія Віталіївна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій

Євромайдан, він же Революція гідності, або Єврореволюція, дав розуміння того в яке майбутнє має бути спрямований вектор розвитку України. В 2014 р. було підписано Угоду про асоціацію між Україною та Європейським Союзом (ЄС): 21 березня було підписано політичну частину Угоди та Заключний акт Саміту, а 27 червня - економічну частина Угоди. 16 вересня 2014 р. Верховна рада та Європейський Парламент ратифікували дану Угоду. Але лише з 1 вересня 2017 р. ця Угода набула чинності в повному обсязі [1]. Навіть в умовах війни Україна продовжує інтеграцію в ЄС: 28 лютого 2022 р. Україна подала заявку на членство України в ЄС і для отримання членства в ЄС Україна має виконати вимоги щодо проведення реформ. Дослідження законодавства ЄС в сфері телекомунікаційних послуг є важливим етапом реформування і нормативно-правового наближення України до ЄС.

Законодавство ЄС [2] **в сфері телекомунікацій регулює засади функціонування телекомунікаційної галузі в країнах-членах ЄС.** В ЄС реалізується стратегія створення єдиного цифрового ринку, яка полягає в синергії між країнами ЄС у царині новітніх технологій, транскордонної торгівлі та надання послуг в межах Єдиного цифрового ринку.

Законодавством ЄС в сфері телекомунікацій закріплено намір створити на всій території ЄС **доступ до високошвидкісного цифрового зв'язку для всіх категорій і верств суспільства** та забезпечення стабільно стійкої системи зв'язку в будь-якій ситуації.

Політика ЄС направлена на сприяння розвитку безпечних, ефективних і стійких цифрових інфраструктур в ЄС, включаючи цифрову **мету по досягненню гігабітного зв'язку для всіх** до 2030 року. Дана Програма має забезпечити підключення для громадян і бізнесу, надання доступу до доступного високошвидкісного широкосмугового зв'язку, включаючи його найвіддаленіші регіони, сільські, периферійні, віддалені та ізольовані території та острови. Програма складається з визначення, проектування, розробки, перевірки та пов'язаних із цим заходів щодо розгортання для будівництва початкової космічної та наземної інфраструктури необхідної для надання послуг. Програма передбачає **поступове розгортання діяльності, спрямованої на завершення як космічної, так і наземної інфраструктури, необхідної для надання розширених урядових послуг, які наразі недоступні та виходять за межі найсучаснішого європейського супутникового зв'язку**. Програма має сприяти розвитку

користувацьких терміналів, здатних використовувати передові комунікаційні послуги. Експлуатаційна діяльність повинна розпочатися якомога швидше з наданням перших державних послуг вже в 2024 році, щоб якнайшвидше задовольнити потреби авторизованих державою користувачів. Програма має включати заходи, спрямовані на завершення як космічної, так і наземної інфраструктури, необхідної для розгортання повної оперативної спроможності до 2027 року. Потім Програма передбачає надання таких державних послуг як експлуатація, технічне обслуговування та постійне вдосконалення космічної та наземної інфраструктури після її розгортання, а також розвиток майбутніх поколінь державних послуг.

Надійний та захищений урядовий супутниковий зв'язок є одним з головних пріоритетів для ЄС. Його своєчасне та ефективне розгортання забезпечує незалежність ЄС від технологій третіх сторін, реалізацію стратегії зовнішньої політики та безпеки, є важливим для роботи поліції, прикордонників, пожежників, цивільних та військових кризових сил. Регламентом ЄС безпечні та надійні послуги супутникового зв'язку визначено найбільш підходящим варіантом за відсутності наземних систем зв'язку або в тих місцях де вони порушені чи ненадійні, також Регламентом зазначена потреба в доступному і економічно ефективному доступі до супутникового зв'язку, який необхідний у регіонах де немає наземної інфраструктури, зокрема, над океанами, у повітряному просторі, у віддалених районах та на територіях де наземна інфраструктура зазнає серйозних збоїв або де їй не можна довіряти в кризових ситуаціях. Супутниковий зв'язок є ресурсом, який обмежений пропускною здатністю супутника, частотою та географічним покриттям. Для того, щоб мати економічну ефективність від впровадження даної Програми розвитку в ЄС має бути оптимізована відповідність між попитом та пропозицією на державні послуги зв'язку і не має бути надлишку потужностей. **Супутниковий зв'язок має забезпечити і підвищити загальну стійкість комунікаційних мереж ЄС**, наприклад, пропонуючи альтернативу у випадку фізичних або кібератак на локальну наземну інфраструктуру, аварій або природних чи техногенних катастроф.

Законодавством ЄС передбачено забезпечення **надання та довгострокову доступність на території ЄС і в усьому світі безперебійного доступу до безпечних, автономних, високоякісних, надійних та економічно ефективних послуг супутникового урядового зв'язку для уповноважених урядом користувачів шляхом встановлення багатоорбітальної безпечної системи зв'язку**. Ситуаційна обізнаність, зовнішні дії і управління кризами мають вирішальне значення для економіки, навколишнього середовища, безпеки та оборони підвищують стійкість та автономію ЄС, зміцнюють технологічну та промислову базу супутникового зв'язку, уникаючи при цьому надмірної залежності від рішень поза межами ЄС, зокрема, для критичної інфраструктури та доступу до космосу.

Політика ЄС спрямована на забезпечення регуляторних і правових аспектів у сфері космічних комунікацій та супутникових систем для **забезпечення права користування орбітальними слотами та відповідними частотами**. Потреба в розподілі цих ресурсів виникає між супутниковими операторами та комунікаційними службами оскільки орбітальний простір та радіочастоти є обмеженими ресурсами. Право користування орбітальними слотами визначається отриманням дозволу або ліцензії на розміщення та експлуатацію супутникових апаратів на конкретних орбітальних позиціях. Орбітальні слоти визначаються міжнародними організаціями, такими як Міжнародний союз зв'язку (ITU), і надаються операторам у відповідності до установлених правил та процедур. Оператори, які отримують право користування орбітальними слотами, мають можливість розміщувати свої супутники на визначених орбітальних позиціях для забезпечення своїх послуг зв'язку. Одночасно з правом на орбітальні слоти пов'язане право на використання відповідних радіочастот. Частоти, які використовуються для комунікаційних послуг зв'язку через супутникові системи розподіляються та регулюються національними та міжнародними органами. Оператори, які отримують право на використання конкретних радіочастот можуть використовувати їх для

передачі та отримання сигналів між супутниками та земною станцією для надання своїх послуг зв'язку.

Космічна інфраструктура ЄС має сприяти стійкості ЄС, пропонувати послуги які замінять або доповнять наземну інфраструктуру для телекомунікацій. Це завдання має виконати **Програма урядового супутникового зв'язку ЄС GOVSATCOM**, яка спрямована на забезпечення безпечних і економічно ефективних можливостей зв'язку для критично важливих місій і операцій, включаючи суб'єктів національної безпеки та агенцій та установ ЄС. GOVSATCOM має на меті використання в ключовій інфраструктурі (включаючи космічні інфраструктури ЄС, такі як Galileo та EGNOS), кризове управління цивільних і військових місій, операцій безпеки та оборони, природних, антропогенних та гуманітарних катастроф, спостереження за незаконною торгівлею. Наявні та майбутні потужності компонента GOVSATCOM мають інтегруватись в систему безпечного зв'язку, покращити стійкість, безпеку та автономність комунікаційних служб ЄС. Наземна інфраструктура Програми повинна базуватися на концентраторах GOVSATCOM. Програма має на меті покращити безпечне з'єднання в географічних зонах стратегічного інтересу, таких як Африка та Арктика, а також Балтійське, Чорне море, Середземноморські регіони та Атлантика. Послуги, що надаються в рамках даної Програми повинні сприяти геополітичній стійкості, пропонуючи додаткове підключення відповідно до цілей політики в цих регіонах і спільного повідомлення Комісії та Верховного представника ЄС із закордонних справ і політики безпеки, глобального шлюзу, що забезпечує зв'язок між національними, регіональними мережами телекомунікацій та іншими країнами або континентами. **Без шкоди для послуг зв'язку, супутники, побудовані для цілей Програми, можуть бути оснащені підсистемами, включаючи корисні навантаження, які можуть дозволити збільшити пропускну здатність компонентів Космічної програми ЄС**, дозволяючи, таким чином, розвивати додаткові некомунікаційні послуги, які вирішуються на засіданні Програмного комітету у відповідній конфігурації згідно Регламенту ЄС. Якщо користь для компонентів Космічної програми Союзу буде належним чином встановлена, беручи до уваги потреби користувачів і бюджетні обмеження, ці підсистеми можуть бути розроблені так щоб пропонувати альтернативні послуги позиціонування, навігації та часу, доповнюючи Galileo, забезпечувати трансляцію повідомлень Європейської геостаціонарної навігаційної служби (EGNOS) з меншою затримкою, забезпечувати космічні датчики для космічного спостереження та підтримувати вдосконалення поточних можливостей Copernicus, зокрема для служб екстреної допомоги та цивільної безпеки. Крім того, ці підсистеми могли б надаватись державам-членам некомунікаційні послуги за умови, що це не впливає на безпеку та бюджет Програми.

Відповідно Декларації про Європейську квантову комунікаційну інфраструктуру (EuroQCI) ЄС планує **розгорнути сертифіковану захищену наскрізну квантову комунікаційну інфраструктуру**, що дозволить передавати та зберігати інформацію та дані, а також мати можливість зв'язувати критичні громадські комунікаційні ресурси на території ЄС. Програма сприятиме досягненню цілей Декларації шляхом розробки космічної та наземної інфраструктури EuroQCI, інтегрованої в урядову інфраструктуру Програми, а також шляхом розробки та розгортання наземної інфраструктури EuroQCI, якими володітимуть держави-члени. **Космічна, наземна та наземна інфраструктура EuroQCI** має бути розроблена в рамках Програми у два основні етапи: етап попередньої перевірки, який може включати розробку та перевірку кількох різних технологій і протоколів зв'язку, і етап повного розгортання. Однією з основних функцій EuroQCI буде забезпечення квантового розподілу криптографічних ключів (QKD). На сьогоднішній день технологія та продукти QKD недостатньо зрілі для використання їх для захисту секретної інформації ЄС (EUCI), ще потребують вирішення проблеми стандартизації протоколів QKD, аналізу побічних каналів і методології оцінки. Програма повинна підтримувати EuroQCI і дозволяти включення схвалених криптографічних продуктів в інфраструктурних проектах.

Загальносоюзні ініціативи, такі як стратегія забезпечення безпечного зв'язку, формуються завдяки широкій участі інноваційних малих і середніх підприємств, стартапів і великих підприємств з космічного сектору по всьому ЄС. В останні роки деякі суб'єкти космічного простору кинули виклик космічному сектору, зокрема **стартапи**, які розробляли інноваційні, орієнтовані на ринок космічні технології та програми, іноді з різними бізнес-моделями. Щоб забезпечити конкурентоспроможність космічної екосистеми ЄС, Програма має максимально використовувати інноваційні та революційні технології, а також нові бізнес-моделі та стартапи, які розробляють орієнтовані на ринок нові космічні технології та програми.

Політика ЄС в сфері телекомунікацій спрямована на заохочування інвестиції в приватний сектор шляхом проведення відповідних закупівель і агрегування контрактів на надання послуг, таким чином забезпечуючи довгострокову передбачуваність потреб державного сектору в послугах. Щоб забезпечити конкурентоспроможність європейської космічної галузі в майбутньому, програми ЄС мають сприяти розвитку передових навичок у сферах, пов'язаних з космосом і підтримувати освітню та навчальну діяльність для реалізації потенціалу громадян ЄС в цій сфері.

Захист навколишнього середовища, впровадження спільної та узгодженої методології оцінки та заходів прозорості щодо екологічного сліду електронних комунікаційних мереж і послуг в ЄС є важливим напрямком діяльності ЄС. Відповідно до цілей «Європейської зеленої угоди» ЄС має **мінімізувати вплив на навколишнє середовище наскільки це можливо**. Хоча космічні засоби самі по собі не викидають парникових газів під час використання, їх виробничі та пов'язані з ними наземні об'єкти мають вплив на навколишнє середовище. Тому має передбачатись вжиття заходів для зменшення цього впливу. З цією метою **при проведенні закупівель повинні бути враховані положення щодо мінімізації та компенсації викидів парникових газів, що утворюються в результаті розробки, виробництва та розгортання телекомунікаційної інфраструктури, а також заходи щодо запобігання світовому забрудненню**. Враховуючи зростаючу кількість космічних апаратів і космічного сміття на орбіті, програми розвитку в сфері телекомунікацій ЄС повинні відповідати критеріям космічної стійкості та бути прикладом передового досвіду в управлінні космічним рухом і в космічному нагляді та відстеженні. Політика ЄС в сфері комічних технологій націлена на зменшення кількості космічного сміття, запобігання зіткненням на орбіті та забезпечення належних заходів щодо завершення терміну експлуатації космічних кораблів.

Політика ЄС в сфері телекомунікацій має на меті підвищити **надійність комунікаційних служб ЄС, а також кіберстійкість ЄС шляхом розробки резервування, пасивного, проактивного та реактивного кіберзахисту та оперативної кібербезпеки та заходів захисту від кіберзагроз та інших заходів проти електромагнітних загроз і зміцнення потенціалу кібербезпеки в ЄС**. Політика ЄС направлена на підтримку виявлення та поінформованості про загрози та інциденти кібербезпеки, посилення готовності критично важливих організацій, а також зміцнення солідарності, узгоджене управління кризами та можливості своєчасного реагування в державах-членах. Закон про кіберсолідарність створює можливості ЄС для того, щоб зробити Європу більш стійкою та здатною реагувати на кіберзагрози, одночасно посилюючи існуючий механізм співпраці. Його реалізація спрямована на безпечне та захищене цифрове середовище для громадян і підприємств, а також захист критично важливих об'єктів і служб. Відповідно до Європейського союзу безпеки **ЄС зобов'язується забезпечити належний захист усіх європейських громадян і підприємств як онлайн, так і офлайн, а сприяти відкритому, безпечному та стабільному кіберпростору**. Зростання масштабів, частоти та впливу інцидентів кібербезпеки становить серйозну загрозу для функціонування мережевих та інформаційних систем і єдиного європейського ринку, військова агресія Росії проти України ще більше посилила цю загрозу. Закон про кіберсолідарність ЄС покликаний **зміцнити солідарність на рівні Союзу для кращого**

виявлення значних або великомасштабних інцидентів кібербезпеки, підготовки до них і реагування на них шляхом створення Європейського щита кібербезпеки та комплексного механізму надзвичайних кібернетичних ситуацій.

Академія кібернавичок ЄС покликана об'єднати приватні та державні ініціативи, спрямовані на підвищення навичок кібербезпеки на європейському та національному рівнях допомагаючи усунути дефіцит талантів у сфері кібербезпеки серед фахівців з кібербезпеки. Академія розміщена в Інтернеті на платформі Комісії Digital Skills and Jobs, а громадяни, зацікавлені в кар'єрі в галузі кібербезпеки, зможуть отримати навчання та сертифікати з усього ЄС в одному місці онлайн. Зацікавлені сторони зможуть запропонувати свою підтримку вдосконаленню навичок кібербезпеки в ЄС, ініціюючи конкретні дії, наприклад, пропонуючи навчання та сертифікації з кібербезпеки. Академія розвиватиметься, щоб включати спільний простір для наукових кіл, постачальників тренінгів і промисловості, допомагаючи їм координувати освітні програми, тренінги, фінансування та відстежувати еволюцію ринку праці в сфері кібербезпеки.

Комісія з кібербезпеки запропонувала ЄС поправку до Закону про кібербезпеку, щоб **уможливити в майбутньому прийняття європейських схем сертифікації для «керованих послуг безпеки»** спрямованих на допомогу компаніям та іншим організаціям в запоіганні, виявленні, реагуванні та відновленні після кіберінцидентів. Сертифікація є ключовою та може відігравати важливу роль у контексті резерву кібербезпеки ЄС та Директиви про заходи щодо високого загального рівня кібербезпеки в ЄС сприяючи також транскордонному наданню цих послуг.

Для швидкого й ефективного виявлення основних кіберзагроз розробляється створення Європейського кіберщита, який скрадатиметься з національних і транскордонних центрів безпеки у всьому ЄС. Ці організації виявлятимуть кіберзагрози та реагуватимуть на них використовуючи найсучасніші технології, такі як штучний інтелект і передову аналітику даних, щоб виявляти та своєчасно ділитися попередженнями про кіберзагрози та інциденти. Таким чином органи влади та відповідні структури зможуть більш ефективно та результативно реагувати на такі інциденти.

Штучний інтелект має бути інструментом, який підвищить добробут людей. Кожна людина повинна мати можливість користуватися перевагами алгоритмічних систем і систем штучного інтелекту, в тому числі шляхом прийняття власного усвідомленого вибору в цифровому середовищі, захищаючись від ризиків і шкоди своєму здоров'ю, безпеці та основним правам.

Законодавством ЄС передбачено встановлення обмежень для призупинення трансляції пропагандистських ЗМІ, які спотворюючи та маніпулюючи фактами ведуть діяльність спрямовану проти громадянського суспільства ЄС та сусідніх країн,.

До 2030 року в ЄС мають бути розширенні можливості людей і підприємств щодо цифрових технологій у глобальному контексті. Забезпеченням регулятивних функцій електронних комунікацій займається BEREC, метою діяльності якого є розвиток відкритих, безпечних, високоякісних, конкурентоспроможних та стійких цифрових систем.

Держави-члени ЄС та зацікавлені сторони повинні забезпечити **розгортання інтелектуальних лічильників, моніторинг додатків системи інтелектуального вимірювання та дотримання основних прав і свобод осіб**. Розгортання інтелектуальних мереж і систем інтелектуального вимірювання має дозволити постачальникам і операторам мереж перейти від широкого уявлення про енергетичну поведінку до детальної інформації про енергетичну поведінку окремих кінцевих споживачів. У світлі потенціалу розгортання інтелектуальних мереж особлива увага має приділятись безпеці та захисту персональних даних які обробляються розумними системами вимірювання. Системи інтелектуального обліку повинні включати авансові структури тарифів, реєстри часу використання та дистанційне керування тарифами. **Постачальники послуг повинні вживати відповідних заходів для**

забезпечення безпеки своїх послуг, у разі необхідності разом з провайдером мережі, та інформувати абонентів про будь-які особливі ризики порушення безпеки мережі.

Головна мета Єдиного цифрового ринку ЄС - усунення зайвих регуляторних бар'єрів і перехід від окремих національних ринків до єдиного, із загальноєвропейськими уніфікованими правилами у трьох телекомунікацій, довірчих послуг та електронної комерції.

Список використаних джерел:

3. Угода про асоціацію Електронний ресурс: https://www.kmu.gov.ua/diyalnist/yevropejska-integraciya/ugoda-pro-asociacyu

4. Офіційний сайт ЄС Електронний ресурс: https://eur-lex.europa.eu/homepage.html?locale=en

ЗМІСТ

СЕКЦІЯ 1
Телекомунікаційні системи та мережі

СЕКЦІЯ 2
Інформаційні системи та технології