МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

МАТЕРІАЛИ
XXVI МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ У XXI СТОЛІТТІ

Том 4

Харків 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЛЕКТРОНІКИ

МАТЕРІАЛИ 26-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ
«РАДІОЕЛЕТРОНІКА І МОЛОДЬ У XXI СТОЛІТТІ»

19 – 21 квітня 2022 р.

Том 4

КОНФЕРЕНЦІЯ

«ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОКОМУНІКАЦІЙ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ ТЕХНОЛОГІЙ»

Харків 2022

УДК 004:[621.317+621.391](06)

26-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. Матеріалів форуму. Т.4. – Харків: ХНУРЕ. 2022. – 53 с.

В збірник включені матеріали 26-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті».

Видання підготовлено факультетом інфокомунікацій
Харківського національного університету радіоелектроніки

61166 Україна, Харків, прос. Науки, 14
тел./факс.: (057) 7021397

E-mail: mref21@nure.ua

Програмний комітет конференції

Снігуров А.В. к.т.н., декан факультету ІК
Безрук В.М. д.т.н, зав. каф. ІМІ
Лемешко О.В. д.т.н., зав. каф. ІКІ
Захаров І.П. д.т.н., зав. каф. ІВТ

УДК 004:621.391

ПРОБЛЕМИ ІНФОКОМУНІКАЦІЙ

УДК 004:621.391]:658.7

СИСТЕМА УПРАВЛІННЯ ДАНИМИ В ЛОГІСТИЧНІЙ КОМПАНІЇ

Акіменко А.С.
Науковий керівник – к.т.н., доц. Токар Л.О.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна тел. +38(050)0841488, e-mail: andrii.akimenko@nure.ua

The main differences of the information logistic flow are shown. The main tasks of logistics in terms of the practical activities of the enterprise are considered. Arguments are given that characterize the need to choose such an integrated information processing system that meets the needs of timely supply of information of the required quality in order to achieve the effectiveness of management decisions. The management system of a transport logistics company is given.

Інформаційний потік, будучи невід’ємною складовою інтегрованого логістичного потоку, повинен активно відображати практичну діяльність в сферах фізичного розподілу, підприємства і матеріально-технічного постачання.

Логістика є істотним чинником реалізації заходів, вкладених у збільшення економічної ефективності виробництва. Для вирішення основного завдання логістики необхідне широке застосування електронної обробки даних, організація роботи на основі наукового функціонального аналізу та структуризації, а також застосування нових технологій.

Використання нових способів обробки та передачі в логістичних системах у зв'язку з бурхливим розвитком інформаційних технологій й визначає актуальність даної роботи. Інформаційні системи займають у цих технологіях центральне становище. Підприємство є відкритою системою, яка матеріальним та інформаційним потоками пов'язана з постачальниками, споживачами, експедиторами та транспортними організаціями. У цьому виникають проблеми подолання місць стику між інформаційними системами підприємства та інших організацій [1].

Одним з головних завдань сучасних інтегрованих інформаційних систем є забезпечення своєчасного постачання інформації потрібної якості менеджерам з метою досягнення ефективності управлінських рішень, що приймаються. Важливе місце у вирішенні цих проблем займають інтегровані інформаційні системи, які дозволяють вирішувати одночасно сукупність специфічних логістичних завдань на користь великих організацій.

При цьому основними проблемами побудови інформаційних систем є:

- неоднорідність інформаційних джерел;
- різноманітність бізнес-завдань;
- технічна (апаратна) неоднорідність;
- рівень кваліфікації користувачів та різноманітність вимог до інтерфейсних рішень.

Система управління має складатися з серверної і клієнтської частин [2].

Серверна частина повинна мати базу даних, що містить такі елементи:

- таблиця перевезень, що містить номер вантажу, за яким можна переглянути всю інформацію по перевезенню;
- таблиця рейсів, час і дата, де буде завантеження і розвантаження;
- таблиця робочого персоналу, а саме водіїв, які будуть виконувати рейси;
- таблиця обладнання (номер вантажівки і причіпа), на якому водій поїде в рейс;
- таблиця оплати за перевезення вантажу.

Приклад загальної структури системи управління даними в логістичній компанії наведено на рис. 1.

Рисунок 1 - Система управління даними в логістичній компанії.

Список використаних джерел:

1. Зайцев Е.І., Корольова Е.А. Логістика: Інформаційні системи і технології / Е.І. Зайцев, Е.А. Корольова. – М.: Альфа-Пресс. – 2008. – 607 с.

2. Гарсіа-Моліна Г. Системи баз даних. Повний курс / Г. Гарсіа-Моліна, Дж. Ульман, Дж. Уідом. – М: «Вільямс» . – 2003. – 1088 с.

УДК621.396.946

АНАЛІЗ ПОШИРЕННЯ РАДІОСИГНАЛІВ МІЛІМЕТРОВОГО ДІАПАЗОНУ ЧЕРЕЗ ДОЩІ У МЕРЕЖАХ ЗВ'ЯЗКУ 5 G

Водолажченко О.В.
Науковий керівник – д.т.н., проф. Коляденко Ю.Ю.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії
ім. В.В. Поповського, тел. (057) 702-13-20)
e-mail: oleksandr.vodolazhchenko@nure.ua факс (057) 702-13-20

The range of millimeter waves is not yet very actively used and has not yet been fully studied. Therefore, it is of interest to study the capabilities of 5G mobile communications in this wavelength range. The analysis of signal attenuation in free space from precipitation intensity at different values of optical visibility at the frequency of 30 GHz and at the frequency of 60 GHz is carried out. The analysis showed that the intensity of precipitation and optical visibility affect the attenuation of the signal, and is about 4 dB loss at 30 GHz and about 12 dB loss at 60 GHz.

Технологія нового покоління 5G / IMT-2020, як і будь-яка нова технологія, привносить свої специфічні особливості в усі аспекти, що стосуються практики її застосування [1]. Одним з таких особливо важливих аспектів є електромагнітна сумісність (EMC). На етапі підготовки до впровадження радіомереж технології 5G, названої NewRadio, необхідно завчасно подбати про вжиття заходів щодо ефективної оцінки умов EMC для цих мереж на основі ретельного аналізу особливостей технології 5G, а правильно і точно оцінивши ці умови - успішно забезпечити EMC радіозасобів нових мереж. Найменше освоєний міліметровий діапазон (ММД) хвиль, тому саме в цьому діапазоні можливий розвиток стандарту 5G зі швидкостями передачі даних від 1 до 10 Гбіт / с. Діапазон міліметрових хвиль використовується поки не дуже активно і вивчений ще не повністю. Тому становить інтерес дослідження можливостей мобільного зв'язку 5G в цьому діапазоні хвиль. Головними недоліками сигналів ММД є:

1) сильне ослаблення сигналу ММД при поширенні;

2) рівень сигналу істотно залежить від впливу гідрометеорів (краплі дощу, сніг, град, туман) і від присутності в атмосфері твердих неоднорідностей (листя дерев, зграї птахів, пил);

3) високий ступінь впливу на рівень сигналу перешкод, які закривають трасу;

4) наявність зон сильного ослаблення сигналу на деяких частотах через ослаблення сигналів ММД молекулами кисню і парами води.

Моделі поширення радіосигналів міліметрового діапазону у мережах зв'язку 5G детально подані у [2]. Модель поширення сигналів в радіоканалах ММД враховує:

- ослаблення радіохвиль у вільному просторі;
- втрати енергії радіохвиль при поширенні через дощі;
- ослаблення сигналу ММД при поширенні через листя дерев;
- ослаблення сигналів при проходженні через щільні перешкоди (будівлі, споруди, тощо).

У середовищі Matlab за допомогою математичного моделювання проведено аналіз ослаблення сигналу у вільному просторі від інтенсивності опадів при різних значеннях оптичної видимості на частоті 30 ГГц і на частоті 60 ГГц. В результаті експерименту отримані залежності ослаблення сигналу у вільному просторі від інтенсивності опадів при різних значеннях оптичної видимості (30, 50, 80 та 200 м) на частоті 30 ГГц (рис.1) і на частоті 60 ГГц (рис.2).

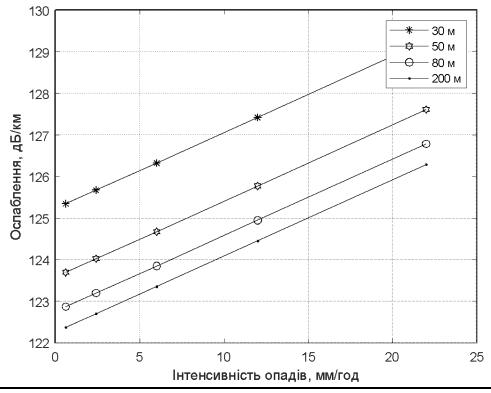


Рисунок 1 - Залежність ослаблення сигналу від інтенсивності опадів при різних значеннях оптичної видимості при частоті 30 ГГц

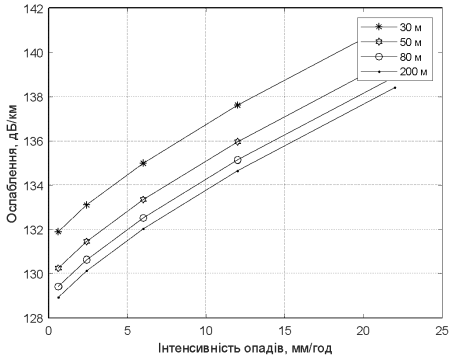


Рисунок 2 - Залежність ослаблення сигналу від інтенсивності опадів при різних значеннях оптичної видимості при частоті 60 ГГц

Проведений аналіз показав, що інтенсивність опадів і оптична видимість впливають на ослаблення сигналу, і становить біля 4 дБ втрат на частоті 30 ГГц і біля 12 дБ втрат на частоті 60 ГГц.

Список використаних джерел:

1. 3GPP TS 28.554. Management and orchestration; 5G end to end Key Performance Indicators (KPI). Ver. 2.0.0, release 15, Sep 2018.

2. Коляденко Ю.Ю. Модели распространения сигналов сетей связи 5 G/ Ю.Ю. Коляденко, Н.А.Чурсанов //Радіотехніка Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 205, с.161-168. DOI:10.30837/rt.2021.2.205.17

УДК 621.391

ВИЗНАЧЕННЯ ДОВЖИНИ ДІЛЯНКИ РЕГЕНЕРАЦІЇ КОГЕРЕНТНОЇ ВОСП

Герасьов С.С., Данилевський Д.В., Новак Є.О.
Науковий керівник – к.т.н., доц. Педяш В.В.
Державний університет інтелектуальних технологій і зв'язку,
каф. Систем електронних комунікацій,
м. Одеса, Україна
тел. +38(048) 705-03-53, e-mail: d.lowpole@gmail.com

Fiber optic transmission systems are used to provide broadband links in a telecommunication network. The most widely used in transport communication networks are optical transport hierarchy (OTH) transmission systems. This paper estimates the regeneration section length of OTH system with quadrature amplitude modulation (QAM). An simulation model in MatLab is proposed to investigate the performance of the OTH transmission system with KAM-M modulation. For an optical channel OTU3 (43 Gbit/s), it is found that the maximum regeneration site length of 1500 km is achieved with KAM-4 modulation.

Швидкий розвиток послуг з надання широкосмугового доступу до мережі Інтернет та сервісів доставки мультимедійного контенту потребує збільшення пропускної спроможності волоконно-оптичних систем передачі (ВОСП). Для побудови магістральних та міських фрагментів телекомунікаційної мережі використовують ВОСП оптичної транспортної ієрархії (ОТН). Вони дозволяють організувати цифрові тракти OTN зі швидкістю від 2,7 Гбіт/с (OTU1) до 111,8 Гбіт/с (OTU4). В оптичних каналах типу OTU3 і OTU4 застосовується когерентний прийом з метою підвищення стійкості до перешкод [1]. Оптичне волокно вносить лінійні та нелінійні спотворення сигнал, а оптичні підсилювачі формують шум посиленого спонтанного випромінювання. Ці негативні ефекти призводять до підвищення ймовірності помилки цифрового сигналу та зменшення довжини ділянки регенерації.

Метою даної роботи є визначення довжини ділянки регенерації сигналу OTU3 з модуляцією КАМ-*М*.

Для вирішення поставленого завдання у програмному середовищі MatLab було розроблено модель оптичного каналу ВОСП ОТН. Вона містить три основні блоки: передавач, волоконно-оптичний лінійний тракт (ВОЛТ) та приймач оптичного сигналу. Модель дозволяє визначати характеристики якості вихідного сигналу з урахуванням лінійних та нелінійних спотворень середовища передачі, а також сумарного шуму оптичних підсилювачів. За

допомогою моделі були отримані графіки залежності вірогідності помилки *BER* (рис. 1).

Блок лінійного тракту складається з $N_{\text{секц}}$ однакових підсилювальних секцій. До складу кожної секції входить волокно завдовжки 100 км, компенсатор хроматичної дисперсії та оптичний підсилювач на базі волокна, легованого ербієм Також міститься джерело шуму посиленого спонтанного випромінювання оптичних підсилювачів.

Когерентний оптичний приймач містить розділюючий пристрій і детектор квадратурного оптичного сигналу. Оптичне волокно моделювалось Фур'є методом розщеплення за фізичними факторами (SSFM) [2].

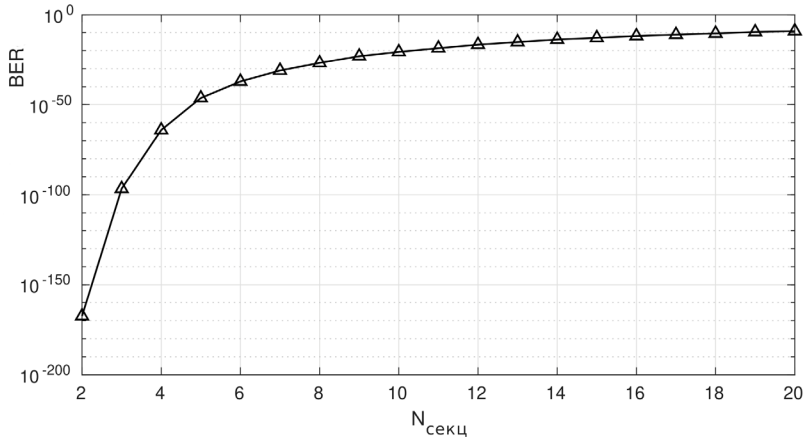


Рисунок 1 – Залежність ймовірності помилки від довжини ВОЛТ для КАМ-4

Дослідження показали, що зменшення ймовірності помилки біта *BER* слід оптимізувати потужність сигналу передавача. Для ВОСП OTU3 встановлено, що довжина ділянки регенерації 1500 км досягається при модуляції КАМ-4. Використання сигнальних сузір'їв великих порядків (M=16 і від) вимагає застосування коректорів нелінійних спотворень сигналу.

Список використаних джерел:

1. Kikuchi, K. (2016). Fundamentals of Coherent Optical Fiber Communications. Journal of Lightwave Technology, 34(1), 157-179. https://doi.org/10.1109/JLT.2015.2463719

2. Agrawal, G.P. (2013). Nonlinear Fiber Optics. Academic Press.

УДК 621.396.946

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СТАНДАРТІВ IEEE 802.11 ДЛЯ РЕАЛІЗАЦІЇ БСМ

Красніков А.О
Науковий керівник –к.т.н., доц. Токар Л.О.
Харківський національний університет радіоелектроніки, кафедра ІКІ ім В.В. Поповського,
м. Харків, Україна
тел. +38(096) 087-71-86, e-mail: andrii.krasnikov@nure.ua

The advantages of wireless sensor networks in comparison with conventional computer networks are shown. The features of the BSM are analyzed from the point of view of the ability of self-healing and self-organization. The possibility of using Wi-Fi technology for the implementation of BMS is considered. It is shown that for organizing hierarchical wireless «Ad-hoc» networks with mobile and static nodes, the IEEE 802.11s standard can be used as a promising one. The possibilities and advantages of this standard in comparison with earlier releases are substantiated.

Технологія безпроводових сенсорних мереж (БСМ) має ряд переваг перед звичайними обчислювальними мережами. Основними відмінностями БСМ вважаються: здатність до самовідновлення і самоорганізації; здатність передавати інформацію на значні відстані за малою потужністю передавачів (шляхом ретрансляції); низька вартість вузлів і їх малий розмір; низьке енергоспоживання і можливість електроживлення від автономних джерел; простота встановлення, відсутність необхідності в прокладці кабелів; можливість встановлення таких мереж на вже існуючий об'єкт без проведення додаткових робіт.

Для реалізації БСМ використовуються декілька безпроводових технологій. Серед них значне місце займає набір стандартів IEEE 802.11 (Wi-Fi). Відносно високі швидкості передачі (до 108 Мбіт/с) роблять перспективним можливе застосування їх в самоорганізуючих сенсорних мережах, в яких необхідно передавати великі обсяги інформації в реальному часі, що й обумовлює актуальність даної роботи.

Набір стандартів IEEE 802.11 працює на нижніх двох рівнях моделі ISO/OSI, фізичному рівні й канальному рівні. Стандарт IEEE 802.11 визначає два режими роботи мережі – режим «Ad-hoc» та режим «клієнт/сервер».

«Ad-hoc» – це проста мережа, в якій зв'язок між численними станціями встановлюється безпосередньо, без використання спеціальної точки доступу. Такий режим корисний в випадку, якщо інфраструктура безпроводової мережі не сформована, або з якихось причин не може бути сформована. У

режимі «клієнт/сервер» безпроводова мережа складається з однієї точки доступу, що підключена до проводової мережі, і деякого набору безпроводових кінцевих станцій. Така конфігурація носить назву базового набору служб (Basic Service Set, BSS). Два або більше BSS, що утворюють єдину підмережу, формують розширений набір служб (Extended Service Set, ESS). Так як більшості безпроводових станцій потрібно отримувати доступ до файлових серверів, Інтернет, доступним в проводовій локальній мережі, вони будуть працювати в режимі «клієнт/сервер».

Основне доповнення, внесене 802.11b в основний стандарт – це підтримка двох нових швидкостей передачі даних – 5,5 Мбіт/с та 11 Мбіт/с. Для досягнення цих швидкостей був обраний метод DSSS, так як метод частотних стрибків в силу обмежень FCC не може підтримувати більш високі швидкості. З цього випливає, що системи 802.11b будуть сумісні з DSSS системами 802.11, але не будуть працювати з системами FHSS 802.11.

Для організації ієрархічних безпроводових «Ad-hoc» мереж з мобільними й статичними вузлами перспективним можна вважати стандарт IEEE 802.11s [1]. У ньому запропоновано новий протокол MAC рівня для безпроводових mesh-мереж, що визначає, крім усього іншого, протоколи вибору шляху й пересилання повідомлень. На відміну від традиційних мереж Wi-Fi, в яких існує тільки два типи пристроїв: точка доступу та термінал, стандарт 802.11s припускає наявність так званих вузлів мережі й порталів мережі. Вузли можуть взаємодіяти один з одним та підтримувати різні служби. Вузли можуть бути суміщені з точками доступу, портали ж служать для з'єднання з зовнішніми мережами. На основі вже існуючих стандартів IEEE 802.11 можна будувати MANET-мережі, відмінною рисою яких можна назвати велику зону покриття.

Крім того, слід відмітити особливість стандарту IEEE 802.11s, яка полягає в тому, що в основі методу вибору шляху для передачі даних лежить механізм профілів. Цей механізм забезпечує сумісність пристроїв від різних виробників, які можуть підтримувати як стандартизовані механізми, так й власні.

Таким чином, за допомогою стандарту IEEE 802.11s є можливість створювати керовані мережі за рахунок протоколу, що займається оновленням таблиць маршрутизації в межах всієї мережі та працює на рівні L2 за моделлю OSI.

Список використаних джерел:

1. Guido R. Hiertz et al. IEEE 802.11s: the Wlan mesh standard / Guido R. Hiertz // IEEE Wireless Communications. – IEEE. – 2010. – PP. 104-111.

УДК 621.396.6

АНАЛИЗ ЭФФЕКТИВНОСТИ МЕТОДА ОПТИМАЛЬНОГО РАСПРЕДЕЛЕНИЯ ЧАСТОТНОГО РЕСУРСА ДЛЯ КОГНИТИВНОЙ РАДИОСЕТИ

Муляр Б.П.

Научный руководитель – д.т.н., проф. Коляденко Ю.Ю.

Харьковский национальный университет радиоэлектроники

(61166, Харьков, пр. Науки,14, каф. Инфокоммуникационной инженерии им. В.В. Поповского, тел. (057) 702-13-20)

e-mail: bohdan.muliar@nure.ua

A method for the optimal distribution of the frequency resource for a cognitive radio network is proposed. The method is based on the criterion of guaranteed communication quality, which in most cases will provide maximum quality uniformity in a grouping of equal priority subscriber stations.

С помощью имитационного моделирования проведен сравнительный анализ эффективности применения данного максиминного алгоритма и алгоритма при децентрализованном распределении частотного ресурса. В качестве критерия эффективности выбрано среднее значение вероятности правильного приема m_p и его среднеквадратическое отклонение σ_p. Эксперимент заключался в следующем. Формировалась матрица $P_{np}^{(mn)}$, состоящая из случайных величин, распределенных равномерно на интервале от 0,85 до 1. Из этой матрицы производилось присвоение частот по максиминному алгоритму и по алгоритму при децентрализованном распределении. За минимально допустимое значение вероятности правильного приема выбрано $P_{np}^{\min} = 0{,}99$. Для получения достоверных результатов анализа усреднение проводилось по 36 выборкам.

На рис. 1 представлены графики зависимостей среднего значения вероятности правильного приема m_p от $K = \frac{M}{N} \cdot 100\%$ - количества требуемых

Кривая 1 (рис.1) отражает зависимость m_p от K при распределении

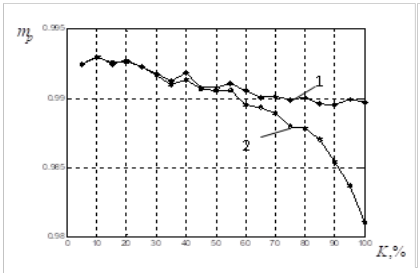


Рис.1. Зависимости среднего значения вероятности правильного приема от количества требуемых КС

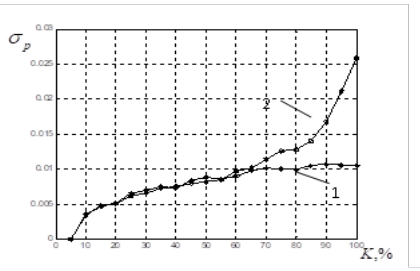


Рис.2. Зависимости среднеквадратического отклонения вероятности правильного приема от требуемых КС

частот по максиминному алгоритму, кривая 2 (рис.1) - зависимость m_p от K при децентрализованном распределении частот. Как видно из данных зависимостей, при распределении частот по максиминному алгоритму m_p остается практически неизменным и не выходит за пределы $P_{пр}^{\min} = 0{,}99$. При децентрализованном распределении частотного ресурса m_p резко снижается с ростом K и при достижении K=50% среднее значение вероятности правильного приема оказывается ниже допустимого.

На рис. 2 представлены графики зависимостей среднеквадратического отклонения вероятности правильного приема σ_p от K. Среднеквадратическое отклонение вероятности правильного приема σ_p при максиминном алгоритме (кривая 1, рис. 2) так же как и среднее остается неизменным в диапазоне изменения $K = 25...100\%$. При децентрализованном же распределении частотного ресурса (кривая 2, рис.5.32) наблюдается экспоненциальный рост σ_p, что свидетельствует о том, что одни АС обеспечены максимальным значением качества связи, а другие же получат ресурс, не обеспечивающий качество связи.

Список использованных источников:

1. *Tafazolli, R.* (ed) (2006): Technologies for the Wireless Future, volume 2, Wireless World Research Forum, (WWRF), John Wiley & Sons, Chichester, England.

2. *Burns P.* SDR For 3G. – Boston, Artech House, 2003 – 279 p.

3. *Haykin S.* Cognitiveradio: brain-empowereswirelesscommunications, IEEE JournalSelectedAreasinCommunication, vol. 23, no. 2, February 2005.

УДК 621.396

АНАЛІЗ ТЕХНОЛОГІЇ КОГНІТИВНОГО РАДІО В ТЕЛЕКОМУНІКАЦІЯХ

Ткаченко А.М.
Науковий керівник – д.т.н., проф. Коляденко Ю.Ю.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії, тел. (057) 702-13-20)
e-mail: alona.tkachenko@nure.ua

The concept of cognitive radio is presented in rich detail and closely related to the concept of software defined radio (English Software Defined Radio (SDR)). Since the first publication of the concept of cognitive radio, it has been discussed more than once, speaking about the optimal variation of the radio frequency spectrum. The essence of the concept of cognitive radio lies in the so-called “Spectrum white spots” in the spectrum of radio frequencies. The stench themselves can be used as “secondary” coristuvachs for the transmission of data.

Поняття когнітивного радіо представлено в багатьох дослідженнях і тісно пов'язане з поняттям програмно-обумовленого радіо (англ. Software defined radio (SDR)).

Радіопристрій з програмованими параметрами (SDR): Радіопередавач і / або радіоприймач, який використовує технологію, що дозволяє за допомогою програмного забезпечення встановлювати або змінювати робочі радіочастотні параметри, включаючи, зокрема, діапазон частот, тип модуляції або вихідну потужність, за винятком зміни робочих параметрів, використовуваних в ході звичайної попередньо визначеної роботи з попередніми установками радиоустройства, згідно з тією чи іншою специфікації або стандарту системи.

Система когнітивного радіо (CRS): Радіосистема, що використовує технологію, що дозволяє цій системі отримувати знання про своєму середовищі експлуатації та географічному середовищі, про усталені правила і про свій внутрішній стан; динамічно і автономно коригувати свої експлуатаційні параметри і протоколи, згідно отриманим знанням, для досягнення заздалегідь поставлених цілей; і вчитися на основі отриманих результатів. Саме когнітивна система виконує функції збору інформації, враховує задані правила і динамічно коригує необхідні параметри.

Після першої публікації концепції когнітивного радіо про нього не раз згадували, говорячи про оптимальне використання спектра радіочастот.

Суть концепції когнітивного радіо полягає в використанні так званих «Білих плям» (англ. Spectrum white spots) в спектрі радіочастот. Саме вони можуть бути використані «вторинними» користувачами для передачі даних.

В певні моменти часу, в вибраному діапазоні, наявність білих плям може відрізнятися. Бувають також ситуації їх повної відсутності. Саме тому когнітивне радіо не зможе гарантувати вторинному користувачу доступ до спектру. Отже, CRS не може бути окремою службою електрозв'язку з гарантованим наданням послуг.

CRS повинна виконувати розширені завдання в порівнянні з звичайним приймачем і передавачем. Через це, виникає деяка складність реалізації алгоритмів роботи всіх функцій пристрою і безпосередньо самого пристрою.

У багатьох лабораторіях когнітивне радіо існує на основі прототипу. Наприклад, пристрій під назвою «CogRadio». Він був створений компанією Radio Technology Systems в Ocean Grove, Нью Джерсі. Він може швидко змінювати радіоканал, а також безперервно передавати відеопотік.

«Сьогодні це найкращий з експериментальних прототипів когнітивного радіо. Це дуже важливо, адже всі зацікавлені в тестуванні і розгортанні такої технології», – розповідає директор Winlab, в Rutgers University.

Пристрій може працювати в діапазоні від 100 МГц до 7500 МГц, включаючи частоти для ТВ, Wi-Fi, GSM і ін. За словами авторів, пристрій здатний детектувати незайняті частоти і перемикатися між ними за 50 мкс (в деяких випадках – за 1 мкс). Когнітивне радіо може маршрутизувати стільникові дзвінки на Wi-Fi і використовуватися для резервування трафіку з оптоволокна, через наявний спектр телебачення в 400 МГц діапазоні.

Висновки

В його основі лежить система радіозв'язку з програмованими параметрами (SoftwareDefined Radio (SDR)). Воно в змозі відслідковувати особливості апаратури для того, щоб програмуватися по смузі частот або за режимом використання. Використання технології когнітивного радіо передбачає підвищення функціональності окремих кінцевих радіопристроїв і їх конвергенцію – для прийому відео- і аудіосигналів радіомовної служби, сигналів рухомої служби буде вимагатися тільки один пристрій.

Список використаних джерел:

1. Стенін А.В. Розробка і дослідження моделей когнітивного радіо [Текст] / Новосибірськ/ 2018. – 77 с.

2. Звіт МСЭ-Р SM.2152 «Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS)», 2009. – С. 1

3. В. І. Комашінскій Когнітивні системи і телекомунікаційні мережі/В. І. Комашінскій, Н. А. Соколов // Вісник зв'язку. 2011. No 10. С. 4-8.

УДК 621.396

КРИТЕРІЙ ЕНЕРГЕТИЧНОЇ ЕКВІВАЛЕНТНОСТІ ДЛЯ ОЦІНКИ ЕМС ПРИ РЕФАРМІНГУ РАДІОЧАСТОТНОГО СПЕКТРУ

Чурсанов М.О.
Науковий керівник – д.т.н., проф. Коляденко Ю.Ю.
Харківський національний університет радіоелектроніки, каф. Інфокомунікаційної інженерії ім. В.В. Поповського, м. Харків, Україна
тел. +38(057) 702-13-20), e-mail: mykyta.chursanov@nure.ua

The criterion of energy equivalence for estimation of EMC at reforming of a radio frequency spectrum is offered. The essence of reforming is the possibility of additional use of previously allocated radio frequency bands by newer cellular technology. As a result of such a procedure, several technologies can be combined in one frequency range.

Критерій базується на еквівалентності енергетичних характеристик в мережі, що замінюється і новій мережі різних стандартів, досить тільки врахувати відмінні риси різних стандартів РЕЗ [10]. Практична значимість такого підходу полягає в тому, що умови ЕМС для більш "динамічних" радіоінтерфейсів можуть бути визначені на базі вже апробованих умов для діючих мереж зі значно меншими витратами. Використовуючи запропонований критерій, можна на етапі планування фрагмента мережі з новою технологією, визначити його склад за кількістю передавачів і допустимій потужності їх випромінювання. Це дозволяє виключити можливу надмірність частотно-територіального плану, що формується для фрагмента мережі, що в кінцевому підсумку може вплинути на вартість експертизи ЕМС. І, нарешті, запропонований критерій є універсальним і може бути використано по відношенню до інших потенційно несумісних РЕЗ, для цього слід лише обрати відповідну ширину смуги пропускання його приймача.

Енергетична еквівалентність в зазначених умовах полягає в балансі енергетики, що випромінється каналами старої мережі і нової мережі в смузі пропускання потенційно несумісного РЕЗ. Еквівалентність енергетики завад від старої мережі і нової в загальному має вигляд:

$$P_{T\Sigma нова}(\Delta f_{РЭЗ}) \le P_{T\Sigma стара}(\Delta f_{РЭЗ}), \quad (1)$$

де $P_{T\Sigma стара}(\Delta f_{РЭЗ})$, $P_{T\Sigma нова}(\Delta f_{РЭЗ})$ - сумарні потужності передавачів базових станцій (БС) старої і нової мережі в смузі пропускання $\Delta f_{РЭЗ}$ потенційно несумісного РЕЗ відповідно. Ступінь можливого збільшення потужності потенційнї завади від нової мережі щодо діючої завади від старої в смузі частот $\Delta f_{РЭЗ} = a \cdot m_f \Delta f_{стара}$ описується співвідношенням [10]:

$$\eta = \frac{P_{T\Sigma н}(\Delta f_{РЭЗ})}{P_{T\Sigma c}(\Delta f_{РЭЗ})} = \frac{S_{\Sigma(\Delta f_{РЭЗ})н} \cdot \Delta f_н}{S_{ср(\Delta f_{РЭЗ})c} \cdot \Delta f_c} =$$
$$= \frac{P_{Tн}}{P_{Tc}}(1-\beta_н)\alpha \frac{n_{Tн} N_н}{\sum_{i=1}^{L_f}(1-\beta_c) n_c(f_i)}, \quad (2)$$

де $S_{\Sigma(\Delta f_{РЭЗ})н}$ – сумарна спектральна густина потужності випромінювання передавачів БС нової мережі в смузі частот $\Delta f_{РЭЗ}$; $S_{ср(\Delta f_{РЭЗ})c}$ – сумарна спектральна густина потужності випромінювання передавачів БС старої мережі в смузі частот $\Delta f_{РЭЗ}$; Δf_c, $\Delta f_н$ – смуги частот старої і нової мережі відповідно; m_f - параметр, що характеризує кількість можливих частотних каналів старої мережі в смузі нової; $n_{Tc}(f_i)$ – число передавачів старої мережі, що випромінюють на одній завадовій частоті f_i; $n_{Tн}$ – кількість передавачів на площадці нової мережі; $N_н$ – кількість площадок, на яких планується установка передавачів нової мережі; β_c – показник, що враховує чинні обмеження потужності БС старої мережі; $\beta_н$ – ступінь можливого обмеження потужності передавачів нової мережі; L_f – кількість частот, які не повторюються старої мережі в смузі приймача РЕЗ; α – параметр, який показує, наскільки смуга РЕЗ більше (менше) смуги нової мережі:

$$\alpha = \begin{cases} \frac{\Delta f_{РЭЗ}}{\Delta f_н}, & \Delta f_н > \Delta f_{РЭС}, \\ 1, & \Delta f_н \le \Delta f_{РЭС}. \end{cases} \quad (3)$$

Список використаних джерел:

1. Скрынников В.Г. Новый критерий для оценки условий ЭМС при рефарминге радиочастотного спектра / В.Г. Скрынников/ Ежемесячный научный журнал Международного союза ученых "Наука. Технологии. Производство". – № 3 (7). – 2015. С. 45-58. Коляденко Ю.Ю. Аналіз електромагнітної сумісності угрупувань радіоелектронних засобів в мережах мобільного зв'язку при рефармінгу радіочастотного спектру [Електронний ресурс] / Ю.Ю. Коляденко, Н.А. Чурсанов // Проблеми телекомунікацій. – 2019. – № 2 (25). – С. 56 - 66. – Режим доступу до журн.: http://pt.nure.ua/wp-content/uploads/2020/02/192_kolyadenko_chursanov.pdf.

УДК 681.7:004.7

ПЕРЕВАГИ ВИКОРИСТАННЯ PON-ТЕХНОЛОГІЇ У ЯКОСТІ ТРАНСПОРТНОГО СЕГМЕНТУ МЕРЕЖІ

Шаповалов І.Р.
Науковий керівник –к.т.н., доц. Токар Л.О.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Науки, 14, кафедра ІКІ ім В.В. Поповського,
м. Харків, Україна

тел. +38(063)6606768, e-mail: ivan.shapovalov@nure.ua

The advantages of fiber-optic communication lines are considered. It is shown that the use of PON-technologies as a transport network for the organization of broadband transmission is an actual solution in the organization of lines using fiber-optic components. The variant of building a network for urban extended infrastructures - "optical ring", which is an economical solution among transport topologies, is analyzed. Practical schemes for connecting users to the network are considered.

Незаперечні переваги волоконно-оптичних ліній зв'язку (ВОЛЗ) засновано на вимогах до сучасних систем інфокомунікацій. Серед безлічі переваг ВОЛЗ слід виділити основні - це висока швидкість передачі інформації, надійність, захищеність.

Ефективне застосування ВОЛЗ відзначається як для побудови ліній зв'язку між елементами мереж, так і для організації мультисервісних мереж з інтенсивними потоками даних [1]. Одним з варіантів побудови таких мереж є застосування PON-технологій, що визначає актуальність даної публікації.

PON (Passive Optical Network) є архітектурою оптичного доступу для організації широкосмугової передачі між оптичним терміналом OLT (Optical Line Terminal) і різними віддаленими оптичними мережевими пристроями ONU (Optical Network Units) в межах пасивної оптичної мережі. PON може об'єднувати трафік від 32 ONU та передавати його центральному модулю CO (Central Office), використовуючи архітектуру типу "дерева", "шини" або "кільця". Для організації оптичних мереж між відправником та одержувачем за схемою "крапка-мультикрапка" можуть використовуватися тільки оптичні змішувачі та розгалужувачі без будь-яких активних елементів, що будуються за вимогами стандарту IEEE 802.3ah [2].

PON працює на першому рівні транспортної технології (L1). Раніше у більшості оптоволоконних системах використовувалися стандарти SONET/SDH. Ці, зазвичай, кільцеві структури припускають регенерацію

сигналу у кожному вузлі. Вони оптимізовані для передачі даних на великі відстані у міських та регіональних мережах.

PON пропонує економне рішення – "оптичне збірне кільце" для міських протяжних інфраструктур SONET/SDH. PON забезпечує низькі початкові витрати, оскільки оптичний сигнал передається до входу користувача (subscriber). Щоб зменшити витрати, можна додати мультиплексування по довжині хвилі (WDM). Адже вузли PON є вузлами опорної мережі. На рис. 1 показана організація "оптичного кільця" на основі технології PON.

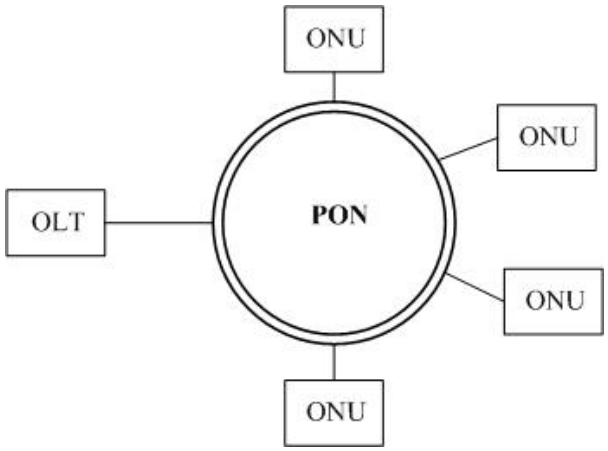


Рисунок 1 - "Оптичне кільце" на основі технології PON

Архітектура PON використовує TMD-мультиплексування між ONU та OLT. Відомі кілька можливих практичних схем підключення користувачів до мережі: мережі "крапка-крапка", мережі, що комутуються та мережі з пасивними оптичними розгалужувачами.

Таким чином, враховуючи динамічне зростання потреб у передачі інформації, зростання вимог щодо якості передачі, вимог захищеності та управління з'єднань, одним із основних напрямків побудови транспортних мереж слід виділити транспортні мережі, що базуються на волоконно-оптичних технологіях.

Список використаних джерел:

1. Филимонов А. Ю. Построение мультисервисных сетей Ethernet / А. Ю. Филимонов. – М.: Издательство: "BHV". – 2008. – 592 с.

2. IEEE 802.3ah-2004. IEEE Standard for Information technology [Електронний ресурс]. – 2004. – Режим доступу до ресурсу: https://standards.ieee.org/ieee/802.3ah/3179/.

УДК 004.056:355.451

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

УДК 004.056.53:614.2

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В МЕДИЧНИХ ЗАКЛАДАХ

Бугай К.Ю.
Науковий керівник - к.т.н., с.н.с. Пшеничних С.В.
Харківській національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії ім. В.В. Поповського, тел. (057) 702-00-00
e-mail: kateryna.buhai@nure.ua

The main aspects of the problem of ensuring security in medical institutions of Ukraine are considered. The main threats that pose a danger to medical institutions and affect the safety of medical care are analyzed.

В доповіді розглядаються питання забезпечення інформаційної безпеки в медичному закладі, а також можливі загрози безпеки приміщення, призначеного для надання медичних послуг підчас яких обговорюється інформація, яка становить лікарську таємницю або конфіденційну інформацію. Актуальністю даної роботи є необхідність захисту конфіденційних даних, інформації та відомостей, розголошення або спотворення яких може спричинити за собою негативні наслідки для пацієнтів та медичного закладу.

Щодо захисту медичної інформації, то вона належить до конфіденційної і є об'єктом захисту на законодавчому рівні у відповідності до Закону «Про захист персональних даних» від 01.06.2010р., № 2297-VI.

Сьогодні йде інтенсивна інформатизація системи охорони здоров'я.

В інформаційній системі медичного закладу об'єктами захисту є:

– інформація в базах даних (БД) систем керування базами даних (СКБД);

– ресурси файлового сервера лікувально-профілактичного закладу;

– резервні копії БД СКБД і архівні копії ресурсів файлового сервера;

– керуюча інформація операційної системи, СКБД, автоматизоване робоче місце (АРМ) адміністратора медичної інформаційної системи (МІС) та адміністратора інформаційної безпеки (ІБ);

– технологічний процес збору, обробки, зберігання та передачі інформації в МІС;

– апаратно-програмний комплекс, що забезпечує роботу МІС.

На практиці МІС мають власну систему безпеки. Основне завдання системи безпеки – забезпечення цілісності інформації і виключення несанкціонованого доступу до ресурсів системи, її програм і даних.

До МІС висуваються підвищені вимоги щодо достовірності та обмеженості доступу до інформації, технічних заходів захисту даних і програм медичної інформаційної системи, юридичної відповідальності.

З юридичної точки зору медичні відомості є інформацією, яка складає професійну таємницю, отже доступ до них обмежений, а охорона забезпечується законодавчо. Будь-який користувач лікувально-профілактичного закладу, отримавши доступ до МІС несе моральну, адміністративну і кримінальну відповідальність за конфіденційність інформації, яку він вносить, використовує або передає іншим користувачам.

У відповідності до цього в МІС реалізовано ряд заходів безпеки, які проводяться системно на всіх етапах її діяльності: від проектування і розробки до впровадження і експлуатації, перекривають всі відомі загрози безпеки, орієнтовані на тактичне випередження загроз, при цьому повинні відповідати нормам законодавства і відомчим актам системи охорони здоров'я.

Технічні засоби виконують такі функції захисту: створення перешкод на можливих шляхах проникнення і доступу потенційних порушників до МІС, ідентифікацію та аутентифікацію користувачів, розмежування прав доступу до ресурсів, реєстрацію подій, криптографічний захист інформації.

Програмно-технічні заходи системи безпеки МІС надають засоби розподілу прав доступу, гарантуючи можливість отримання доступу користувача тільки до тієї інформації і програмам, які необхідні для виконання функціональних обов'язків.

Інформаційна безпека забезпечується спеціальними програмними засобами – підсистемою інформаційної безпеки, що виконує такі основні функції:

– організація санкціонованого доступу до даних;

– моніторинг небезпечних подій;

– управління властивостями користувача МІС;

– ведення журналів безпеки.

Вказані засоби забезпечення безпеки дозволяють МІС здійснювати необхідний комплекс заходів захисту інформації та програм, що є необхідною умовою придатності МІС до її експлуатації.

Список використаних джерел:

1. Основи законодавства України про охорону здоров'я: ВЕРХОВНА РАДА УКРАЇНИ від 03.02.1993р. №2978-XII.

2. Безпека пацієнта/пров. з англ. за ред. О.Л. Ніконова. М: ГОЕТАР-Медіа, 2010. 184 с.

3. Захист медичної інформації – важлива задача сьогодення | Блоги БДМУ. БДМУ | Головна сторінка. URL: https://www.bsmu.edu.ua/blog/2531-zahyst-medychnoi-informacii/. (дата звернення: 30.01.2022).

УДК 004.057.4:355.451]:004.75

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРОТОКОЛІВ ДОСТУПУ ДО ХМАРНИХ РЕСУРСІВ

Євсюкова О.О.
Науковий керівник – Сацюк В.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14,
кафедра Інфокомунікаційної інженерії ім. В.В. Поповського,
тел. (057) 702-13-20), e-mail: olena.ievsiukova@nure.ua

The cloud computing model is the organization of users' access via the Internet to a certain general fund of computing resources. The resources themselves can be different - remote services, storage devices, servers, software (software) and others. The main principle remains the same: the resource that the user accesses are not on his computer and on his local network. The problem of information security is becoming increasingly important for the further development of distributed network applications and the concentration of computing resources.

Як відомо, хмарні ресурси функціонують на протоколах VDI (Virtual Desktop Infrastructure). Протоколи VDI — це інфраструктура віртуальних робочих столів. До появи персональних комп'ютерів співробітник організації робив за столом з паперами, звітами, скріпками, папками. З поширенням ПК (Персональний Комп’ютер) дані поступово перенесли в електрону форму.

Важливим протоколом доступу до хмарного сховища є RDP (Remote Desktop Protocol) – протокол доступу до віддаленого ПК. Це закритий протокол прикладного рівня, який знаходиться на сьомому рівні моделі OSI. RDP клієнти були написані майже для всіх існуючих операційних систем (Windows, Macintosh, Linux) та за замовчуванням присутні у всіх системах сімейства Windows. Також за замовчуванням серверна частина сховища використовує для підключення порт TCP 3389.

Ще одним протоколом є PCoIP (Personal Computer over Internet Protocol). Це так званий пропрієтарний протокол, що використовується в рішеннях, пов'язаних з віддаленими робочими станціями та робочими столами. Даний протокол спочатку був розроблений компанією «Teradici», але згодом був перейнятий компанією «VMware», яка в свою чергу інтегрує його у свої продукти для реалізації доступу до віртуальних машин або віддаленим робочим столам VDI інфраструктури.

На рисунку 1 приведена схема взаємодії клієнтських частин протоколів PCoIP та RDP з серверними частинами системи, встановленими в операційних системах кінцевих віртуальних машин.

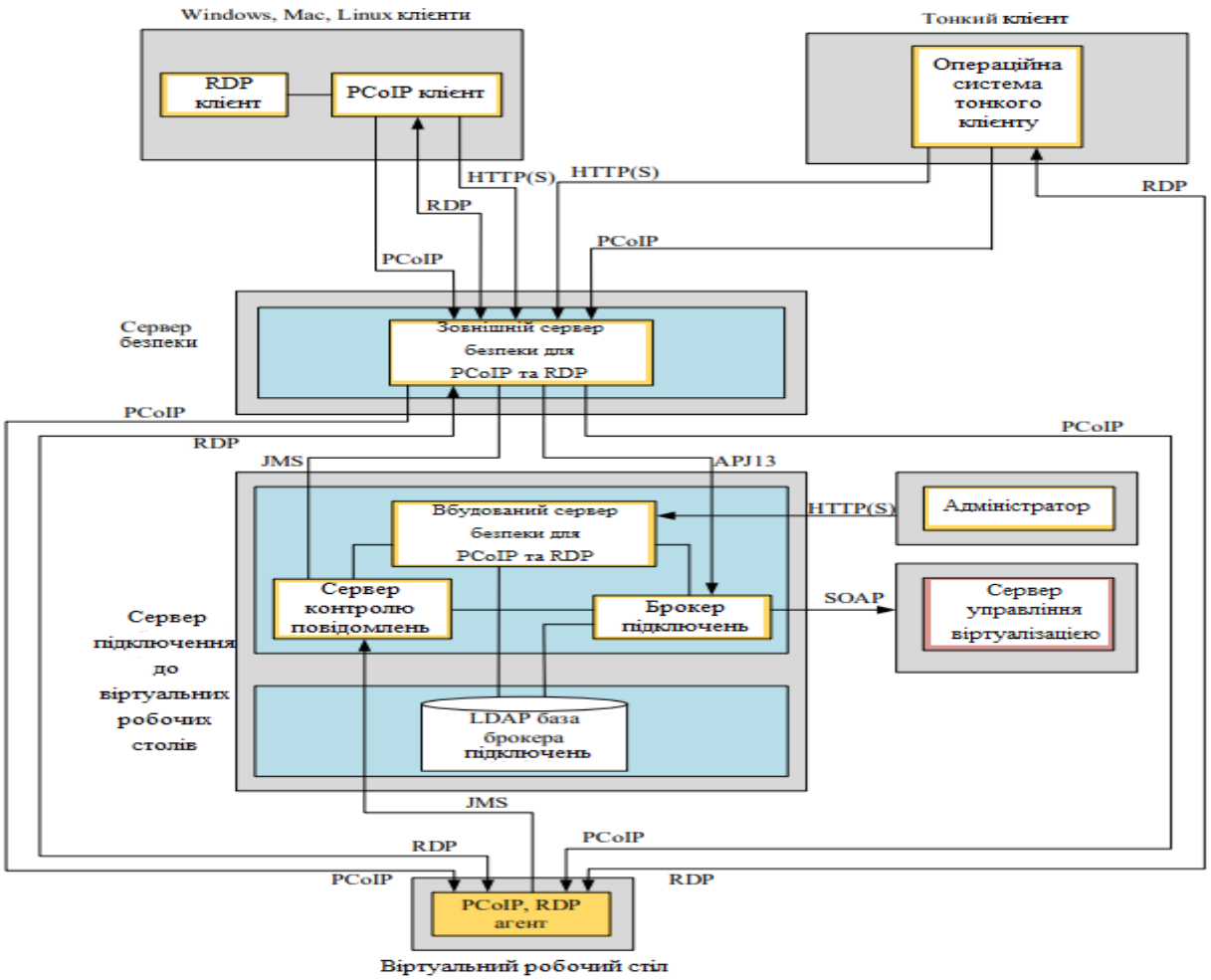


Рисунок 1 – Схема взаємодії PCoIP и RDP протоколів

Протокол PCoIP має можливість стискати та шифрувати весь потік даних, що обробляється в центр обробки даних і у стандартної IP-мережі, також передає інформацію очікуванням PCoIP пристроям. При цьому відбувається передача лише про змінені пікселі.

Висновки

Розглянуті в докладі протоколи мають досить широкий діапазон можливостей, серед яких відтворення відео та різних графічних ефектів, шифрування даних, контроль якості картинки та багато іншого, але вони значно відрізняються за своєю суттю.

Список використаних джерел

1. Аулов І.Ф., Горбенко І. Д. «Хмарні обчислення та аналіз пиатнь інформаційної безпеки в хмарі» / Прикладна радіоелектроніка: наук.-техн. Журнал – 2013. – Том 12. – №2. – 194-201 с.

2. The NIST Definition of Cloud Computing, NIST Special Publications 800-145, 2018. – 28 p.

УДК 004.357:621.391.26

ПРЕДВАРИТЕЛЬНАЯ ОБРАБОТКА ГОЛОСОВОГО СИГНАЛА В СИСТЕМАХ АУТЕНТИФИКАЦИИ

Камени Нгалани Г.Б., Пастушенко Н.С.
Научный руководитель – ктн, профессор Пастушенко Н.С.
Харьковский национальный университет радиоэлектроники каф. ИКИ,
г. Харьков, Украина
тел.050 942 27 78, e-mail: Mykola.pastushenko@nure.ua

The scientific problem of increasing the efficiency of voice authentication systems is considered. As the direction of research, the procedures for preprocessing the voice signal are chosen, which in modern systems are reduced to normalizing the signal in amplitude and duration. Based on the phase information of the voice signal, it is proposed to implement procedures for eliminating distortions in the recording materials of the user's acoustic wave and the signal-to-noise ratio.

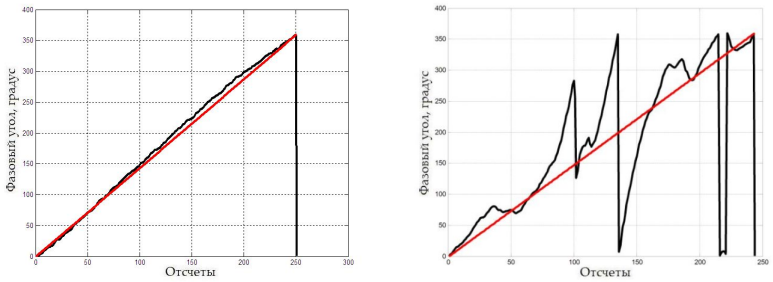
В настоящее время особую актуальность приобретают вопросы кибербезопасности, поскольку широкое распространение приобрели случаи хищения, шифрования и уничтожения информации. Одним из барьеров безопасности есть системы аутентификации, которые в этом тысячелетии используют биометрические признаки пользователя. К сожалению, дактилоскопия, на которую возлагали большие надежды, не оправдала ожиданий. Поэтому в последнее десятилетие особое внимание уделяется системам голосовой аутентификации (СГА), которые относятся к динамическим (поведенческим) системам.

Как и другие биометрические системы голосовые имеют недостаточные количественные характеристики. Одним из направлений существенного повышения качества голосовых систем это использование фазовых данных речевого сигнала, которые до последнего времени игнорировались. В работах [1, 2] показана эффективность использования фазовых данных для оценки большинства характеристик шаблонов в СГА. Однако, фазовые данные голосового сигнала можно использовать и на этапе предварительной обработки голосового сигнала.

При приеме и регистрации сигналов в различных системах радиолокации и радиосвязи стремятся к наилучшему восстановлению полезной исходной информации с помощью процедур предварительной обработки. Как известно, предварительная обработка голосового сигнала, осуществляемая в СГА, сводится к нормализации сигнала по амплитуде и

длительности. В работе предлагается использовать фазовую информацию голосового сигнала на этапе предварительной обработки.

Указанное утверждение базируется на том, что фазовая информация голосового сигнала имеет известную форму пилообразного сигнала. (на рисунках ниже показана красным цветом), который по амплитуде изменяется в интервале от 0 до 360 градусов. При этом длительность сигнала неизвестна. Пример фазового сигнала (черный цвет) показан на рис. 1а. В некоторых случаях фазовый угол имеет ошибочные значения, что показано на рис 1б. Причинами этого могут быть: влияние помех и шумов, низкое отношение сигнал-помеха, ошибки квантования и дискретизации, ошибки при оценке фазового угла и др.



а б

Рисунок 1 – Ожидаемая и расчетная зависимости фазового угла при отсутствии (а) и наличии (б) ошибок

Выявление причин появления ошибок в оценке фазового угла и их устранение и будет составлять существо процедур предварительной обработки голосового сигнала. В результате получим не только более качественные оценки фазового угла, но и устраним ошибки в исходном регистрируемом голосовом сигнале. Такой подход позволит более качественно сформировать признаки шаблона пользователя.

Список использованных источников

1. Pastushenko, M. &Pastushenko, V. &Pastushenko, O. Specifics of Receiving and Processing Phase Information in Voice Authentication Systems. *International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T).* (pp. 621-624). 2019, Kyiv, Ukraine.

2. Pastushenko, M. & Krasnozheniuk, Y. & Lemeshko, O. Analysis of voice signal phase data informativity of authentication system. *Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020).* (pp 1040-1053). April 27-May 1, 2020, Zaporizhzhia, Ukraine.

УДК 004.056:355.451

СУЧАСНІ ТЕНДЕНЦІЇ КІБЕРАТАК ТА КРАЩІ ПРАКТИКИ ДЛЯ ЗАХИСТУ ВІД НИХ

Качан В.Є., Нгуєн Х.Н.
Науковий керівник – к.т.н., доц. Куля Ю.Е.
Харківський національний університет радіоелектроніки
(61166, м. Харків, пр. Науки, 14, кафедра ІКІ імені В.В. Поповського, тел. +38(050) 702-55-92) email: vadym.kachan@nure.ua, khai.nhuien@nure.ua

This work is devoted to assessing current trends in attacks and best practices to protect against these attacks. The main trends that are not controlled by the security team are considered. Microsoft Security Intelligence Report and SANS (SysAdmin, Audit, Network and Security) Attack Threat Report are used. Common security controls have been identified as the best ways to improve protection.

Засоби масової інформації освітлюють багато порушень, збоїв та статистичних даних про кількість атак, здійснених у кіберпросторі. Однак треба ретельно шукати інформацію, щоб знайти надійні поради щодо виявлення та запобігання загрозам. Індустрія потребує експертного аналізу того, як менеджери з безпеки повинні розставляти пріоритети, щоб підвищити ефективність та результативність боротьби з відомими загрозами, а також мінімізувати ризики від нових атак.

Можна виділити три масштабних тенденції [1], кожна з яких не контролюється командою безпеки.

1. Винахідники постійно і не передбачувано придумують нові технології, протоколи та додатки. Зазвичай вони роблять це з акцентом на швидкість, простоту використання та прибутковість. На безпеку не робиться великий акцент.

2. Лідери бізнесу швидко впроваджують нові технології, а за ними і інші. Для інтеграції безпеки потрібен час, який компанії-першопрохідники не можуть собі дозволити, бо в такому випадку втратять свої переваги.

3. Хакери та злочинці швидко використовують вразливі місця.

Щорічний звіт Microsoft Digital Defense Report [2] є надійним джерелом тенденцій атак на комп’ютери та сервери Windows. У останній версії виявлено фішинг та BEC (Business Email Compromise, зловмисник за допомогою фішингу намагається обдурити компанію) як найпоширеніший початковий вектор атаки та виділила дві додаткові тенденції:

1. Зловмисники все частіше націлені на C-suite (найважливіша та найвпливовіша група осіб у компанії) та директорів, використовуючи

глибоке дослідження своїх цілей та використовуючи індивідуальні фішингові атаки.

2. Зловмисники у фішингових атаках все частіше видають себе за представників популярних брендів (торгових марок компаній) для підвищення випадків обману. Топ найпопулярніших брендів, за які себе видають зловмисники, а також топ 10 галузей для BEC-атак зображено на рисунку 1.

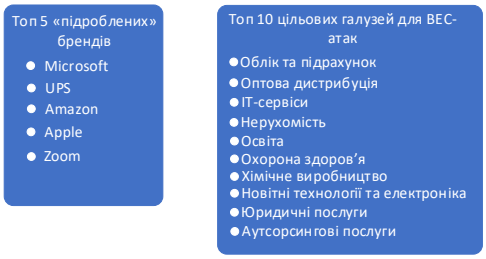


Рисунок 1 - Топ «підроблених» брендів та галузей для BEC-атак

Серед кращих методів покращення захисту виділяють загальні засоби контролю безпеки, які можуть зменшити ймовірність шкоди.

1. Уникнення багаторазових паролів. Фішингова атака, яка захоплює облікові дані та паролі привілейованих користувачів, уможливлює понад 70% усіх шкідливих атак. Дослідження Microsoft показали, що просте додавання SMS (Short Message Service) повідомлень як другого фактора аутентифікації зупинить 99,9% усіх фішингових атак. 2FA (2 Factor - двофакторна аутентифікація) не незламною, але вона піднімає планку проти зловмисників і змушує їх використовувати методи, які набагато легше виявити, ніж коли вони контролюють внутрішньо підключені ПК (Персональні комп'ютери).

2. Основна гігієна безпеки - керування конфігурацією, своєчасне виправлення, мінімізація привілеїв, сегментація мережі та контроль програм можуть запобігти ефективності більшості шкідливих виконуваних файлів, навіть якщо зловмиснику або програмі їх вдасться встановити.

3. Активний пошук загроз (threat hinting). Активний пошук аномалій і підозрілої поведінки для швидкого пошуку нових загроз зменшить збитки для бізнесу.

Список використаних джерел:

1. Pescatore J. SANS 2021 Top New Attacks and Threat Report [Електронний ресурс] / John Pescatore. – 2021. – Режим доступу до ресурсу: https://fs.hubspotusercontent00.net/hubfs/8645105/white-paper/sans-attack-threat-report-2021.pdf.

2. Microsoft Digital Defense Report [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.microsoft.com/en-us/security/business/security-intelligence-report.

УДК 004.056:355.451

СУЧАСНІ КІБЕР-РИЗИКИ ІНТЕРНЕТУ РЕЧЕЙ ТА МЕТОДИ ЗАХИСТУ ВІД НИХ

Качан В.Є., Нгуєн Х.Н.
Науковий керівник – к.т.н., доц. Куля Ю.Е.
Харківський національний університет радіоелектроніки
(61166, м. Харків, пр. Науки, 14, кафедра ІКІ імені В.В. Поповського,
тел. +38(050) 702-55-92), e-mail: vadym.kachan@nure.ua , khai.nhuien@nure.ua

This work is devoted to assessing current cyber risks of the IoT (Internet of Things) and best practices for protection against them. The use of IoT devices in botnets is considered.

Існують мільйони «розумних» підключених до Інтернету пристроїв, які складають IoT, починаючи від мобільних телефонів і закінчуючи комп'ютерами, домашніми термостатами, камерами відеоспостереження та кавоварками. Інтернет речей має як переваги, так і низку недоліків безпеки. Наприклад, пристрої Інтернету речей часто не мають вбудованих потужних функцій безпеки, які запобігають доступу хакерів до них. Окрім проблем особистої конфіденційності та безпеки, які виникають через ці прогалини в безпеці, більша небезпека полягає в тому, що ці пристрої можуть бути використані хакерами для створення ботнету, який є мережею з пристроями зараженими шкідливим програмним забезпеченням без відома користувача.

У світі пристроїв Інтернету речей існує ряд кібер-ризиків [1]. Деякі з основних кіберзагроз IoT в нинішній час включають наступні ризики:

1. відсутність регулярних оновлень і слабкі механізми оновлення;
2. слабкий захист паролем;
3. незахищені інтерфейси. Вразливості в інтерфейсах дозволяються хакерам зламувати пристрої IoT, а далі і проникати у локальну мережу користувачів;
4. шкідливе програмне забезпечення. Після зараження пристроїв IoT шкідливим програмним забезпеченням вони можуть бути використані в DDoS (Distributed Denial of Service) атаках [2], використання таких пристроїв є сучасним трендом у формуванні ботнетів. Такими атаками є, наприклад SYN (Syncronized) flood або UDP (User Datagram Protocol) flood;
5. незашифровані дані. Відсутність шифрування може дозволити суб'єктам загрози перехоплювати пакети з мережі пристроїв за допомогою атак «людина посередині» або інших методів втручання в мережу та отримання доступ до конфіденційних даних. Незашифровані дані та мережі є актуальною проблемою, яка є причиною катастрофічних зломів компаній. Серед кращих практик захисту від атак на IoT можна виділити декілька [3].

1. Зміна налаштувань маршрутизатора за замовчуванням. Більшість людей забувають перейменувати маршрутизатор і залишають назву за замовчуванням. Це може зашкодити безпеці приватного Wi-Fi (Wireless Fidelity). Рекомендується змінити ім'я, яке не містить у собі особисту інформацію. Wi-Fi є першим рубежем, що потребує захисту від хакерів, оскільки багато пристроїв IoT підключено до нього.

2. Від'єднання пристроїв IoT, коли вони не потрібні. Більшість сучасних пристроїв можуть підключатися до Інтернету, наприклад, холодильники та телевізори. Але це не означає, що потрібно підключати їх до Інтернету. Рекомендується уважно ознайомитися з функціями пристроїв і точно дізнатися, який пристрій потребує підключення до Інтернету.

3. Вибір надійного паролю. Для надійного захисту слід використовувати принцип "три з чотирьох", тобто використовувати хоча б три параметри з чотирьох в паролі - великі і малі літери, цифри, спеціальні символи.

4. Уникнення використання Universal Plug and Play. Хоча Universal Plug and Play (UPnP) має своє застосування, він може зробити принтери, маршрутизатори, камери та пристрої IoT вразливими до кібератак. UPnP дозволяє полегшити підключення пристроїв та допомогти їм автоматично виявляти один одного. Тим не менш, це приносить більше користі хакерам, ніж користувачам, оскільки вони можуть виявляти всі пристрої Інтернету речей за межами локальної мережі. Тому краще повністю вимкнути UPnP.

5. Постійне оновлення вбудованого та встановленого ПЗ (програмного забезпечення). Оновлення ПЗ пристрою IoT гарантує, що пристрій має найактуальнішу систему безпеки. Крім того, це допомагає системі усунути недоліків безпеки старих версій ПЗ. Незважаючи на ризики, малоймовірно, що IoT перестане розповсюджуватись у домах, офісах і т.д. Через це, нікуди не дінуться і хакери. Тому, найголовнішим є пам'ятати про безпеку своїх пристроїв. Розуміння їхніх вразливостей і використання правильних інструментів захисту необхідні для протистояння загрозам у мінливому світі IoT.

Список використаних джерел:

1. Cyber Threats Haunting IoT Devices in 2021 [Електронний ресурс] – Режим доступу до ресурсу: https://securityboulevard.com/2021/09/cyber-threats-haunting-iot-devices-in-2021/. 2. Reo J. DDoS Hackers Using IoT Devices to Launch Attacks [Електронний ресурс] / Joy Reo – Режим доступу до ресурса: https://www.corero.com/blog/ddos-hackers-using-iot-devices-to-launch-attacks/.

3. Swamini K. How to secure IoT devices and protect them from cyber attacks [Електронний ресурс] / Kulkarni Swamini – Режим доступу до ресурсу: https://bit.ly/3B4R8Ah.

УДК 621.391

CALL CENTRY НА ОСНОВІ CTI CRM-СИСТЕМИ

Радченко Р.В.
Науковий керівник – Сабурова С.О.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Науки, 14,
кафедра Інфокомунікаційної інженерії ім. В.В. Поповського,
тел. (057) 702-13-20 e-mail ruslana.radchenko@nure.ua, (095) 640-65-28

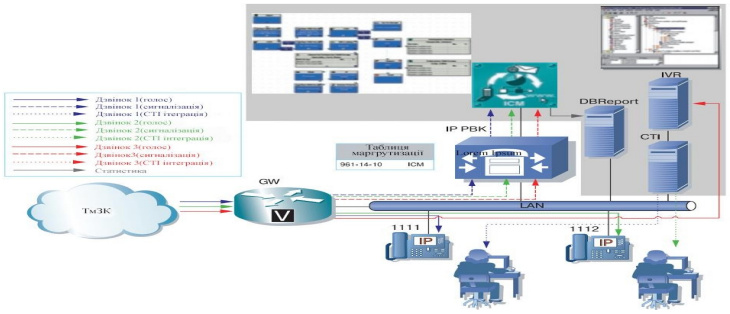
The most important mission and task of all organizations, business structures and enterprises is to obtain maximum income. The possibility of instant and effective access to timely information, its analysis, review and distribution give the employee the opportunity to use it appropriately. CTI CRM systems are seamless integration or merging of computers and telephone systems. CTI is also defined as a technology platform that integrates voice and data services at the functional level to add tangible benefits to business applications. To achieve a high level of customer satisfaction, many call centers today use CTI technology in PSTN.

Найважливішою місією і завданням всіх організацій, бізнес-структур і підприємств, є отримання максимального доходу. Можливість миттєвого та ефективного доступу до своєчасної інформації, її аналіз, огляд і розподіл дають співробітнику можливість доцільно її використовувати.

Зростання абонентської бази позитивно позначається на розвитку бізнесу, а саме: забезпечує підвищення прибутку і зміцнює позиції компанії на ринку. Основний обсяг прибутку CALL CENTRY корпоративних мереж надходять за рахунок клієнтів, що звернулися. Таким чином можна зробити висновок, що клієнт - це ключова ланка в діяльності будь якої організації та бізнес-структури. Для операційних діяльності CALL CENTRY виділяють 4 основні групи показників, за якими проводиться аналіз, це доступність, якість контактів з клієнтами, продуктивність, результативність.

Ефективне управління CALL CENTRY неможливо без відстеження певних KPI (показників ефективності). Це правило застосовується до будь-якої галузі бізнесу. Перший крок в постановці цілей і вимірі результатів діяльності - це визначення загальних ключових показників ефективності (KPI) для компанії (або системи показників). Такі вимірювання повинні бути введені для всіх видів діяльності, безпосередньо пов'язаних з обслуговуванням клієнтів (наприклад, відповіді на дзвінки або правила написання електронних листів). Для підвищення ефективності параметрів KPI у CALL CENTRY компаній успішно проводиться модернізація на базі впровадження CTI CRM-системи. CTI CRM-система - це безшовна інтеграція або злиття комп’ютерів та телефонних систем [1]. CTI також визначається як

технологічна платформа, яка об'єднує послуги голосу та даних на функціональному рівні, щоб додати відчутні переваги для бізнес-додатків. Щоб досягти високого рівня задоволення клієнтів, сьогодні багато телефонних центрів застосовують технологію CTI CRM-системи у ТМЗК. В



CALL CENTRY, коли

Рисунок 1 – Схема роботи CALL CENTRY с використанням CRM-системи

використовується обладнання CRM-системи (Cisco IPCC) для прийому телефонних дзвінків розглянемо три одночасних дзвінка. На схемі (рис.1) елементи, які стосуються Cisco IPCC (виділені фоном): ICM, IVR, CTI, DBReport. IP PBX, в свою чергу, запитує у ICM: «Що робити з дзвінком?». ICM запускає сценарій маршрутизації дзвінка, який відповідно згідно алгоритму, вибирає вільного оператора, і виконує дві дії: повідомляє IP PBX номер IP-телефону оператора і паралельно повідомляє CTI ім'я оператора, на якого буде переключене виклик. IP PBX, отримавши від ICM номер IP-телефону, перемикає на нього виклик (аналогічно тому, як це робиться в першому варіанті). А CTI, отримавши інформацію від ICM про ім'я оператора, запускає на екрані монітора оператора механізм CTI-інтеграції та забезпечує спливання вікна CRM-системи (рис. 1).

Висновки:

1. На сьогоднішній день методи і платформи для побудови IT-інфраструктури CALL CENTRY є досить зрілими (в багатьох випадках). Основні технології та системи CALL CENTRY операторів фіксованого зв’язку, що займають великі частки корпоративного IT-ринку, пройшли перевірку роками і динамічно розвиваються. 2. CALL CENTRY в умовах модернізації на базі використання платформи CRM-системи дасть можливість забезпечити якісний менеджмент послуг.

Список використаних джерел:

1 Багатоканальний електрозв’язок та телекомунікаційні технології [Електронний ресурс]: підручник у 2-х томах. /О. В. Лемешко, В. А. Лошаков, В. В. Поповський, С. О. Сабурова та ін.// за редакцією В. В. Поповського-.Х.: ТОВ «Компанія СМІТ», 2018. // Режим доступу до ресурсу: http://www.smit-book.com/books.html – 1012 с.

УДК 621.391:004.056.5

АНАЛІЗ ЕФЕКТИВНОСТІ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ

Семеренська В.В.
Науковий керівник – к.т.н., с.н.с. Пшеничних С.В.
Харківській національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії ім. В.В. Поповського, тел. (057) 702-00-00
e-mail: viktoriia.semerenska@nure.ua

Designing of integrated complex security systems is based on realization of ideas of system concept of complex object security with parallel solution of tasks of control automation of such life support systems of the object as power supply, ventilation, heating, water supply, elevator equipment, air conditioning, etc. Designing integrated comprehensive security systems is one of the determining factors that can reduce losses from unlawful acts, emergencies, natural disasters, as well as the cost of eliminating the consequences of these events.

Підвищення ефективності систем сигналізації на об'єктах в умовах різкого загострення криміногенної обстановки неможливе без розробки і впровадження наукомістких інтегрованих систем безпеки (ІСБ), здатних скоротити збитки від протиправних дій, надзвичайних ситуацій, стихійних лих, а також витрати на усунення наслідків зазначених подій.

У зв'язку з цим певний інтерес представляють дослідження в області створення ІСБ на основі інтегрування інноваційної технології лазерного сканування (ЛЗ) і системи відеоспостереження (СВН) з метою забезпечення більш високого рівня безпеки і показників виявлення несанкціонованого вторгнення в контрольовану зону особливо важливих об'єктів.

Інтеграція ЛЗ і СВН підвищує ефективність систем відеоспостереження і зменшує відсоток хибних спрацьовувань, оскільки дозволяє здійснювати комплексний аналіз ситуації на об'єкті:

−при появі тривожного сигналу керована камера відеоспостереження, яка закріплена за відповідною зоною, позиціонується в програмоване положення;

−на моніторі оператора пульта спостереження з'являється повідомлення про спрацювання системи, супроводжується звуковим сигналом, а на карті (плані об'єкта) відображається місцезнаходження порушення і транслюється відеопотік з відповідної камери;

−оператор обробляє тривожне повідомлення і при необхідності може перехопити управління камерою для супроводу суб'єкта порушення;

−всі дії оператора, що пов'язані з появою і відпрацюванням тривожного повідомлення, а також відеоархів, зберігаються в системі з прив'язкою до дати і часу.

Таким чином система відеоспостереження виконує не тільки функцію відеофіксації подій, а й додаткового рубежу охорони.

Переваги інтеграції різних датчиків в систему відеоспостереження очевидні і все частіше подібні рішення стають стандартною комплектацією системи безпеки об'єкта.

Для оцінки ефективності інтегрованої системи безпеки існують методи, на основі яких можна порівнювати конкуруючі варіанти ІСБ, оцінювати та обґрунтовувати забезпечення заданих замовником характеристик.

Ефективність системи безпеки характеризує ймовірність виконання системою своєї основної цільової функції щодо забезпечення захисту об'єкта від загроз, джерелами яких є навмисні протиправні (несанкціоновані) дії фізичних осіб (порушників).

Система вважається ефективною, якщо виконуються наступні вимоги:

−в заданих умовах експлуатації повністю і у встановлені терміни система виконує завдання, що стоять перед нею (технічна ефективність);

−витрати на створення та експлуатацію системи не перевищують позитивного ефекту від її використання (економічна ефективність).

Імовірнісні методи включають такі параметри як ймовірність реалізації загроз; виявлення загроз, хибних тривог; припинення несанкціонованих дій та ін. Зазначені параметри можуть бути отримані на основі статистичних даних та експертних оцінок.

Комбіновані методи, що враховують як економічні, так і ймовірнісні характеристики, дозволяють визначити максимальний відносний збиток, який вдалося запобігти від реалізації всіх загроз з урахуванням випадкового характеру їх появи.

Зазначені критерії можуть бути застосовані як до системи безпеки в цілому, так і до окремих підсистем. Однак, остаточний і більш повний висновок можна зробити тільки на основі аналізу ефективності функціонування всіх підсистем не окремо, а у взаємодії.

Список використаних джерел:

1. Рижова В. А. (2013). Проектування та дослідження комплексних систем безпеки. НІУ ІТМО

2. Членов А. Н., Рябцев Н. А., & Буцинська Т. А. (2019). Оптимізація проектування охоронної сигналізації з урахуванням показника ймовірності ефективного виявлення. Технології техносферної безпеки.

УДК 004.056

АНАЛІЗ ОСНОВНИХ РИЗИКІВ ПРИ ВПРОВАДЖЕННІ GDPR

Товкун Ю.І.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського, м. Харків, Україна
тел. +38(066) 129-66-30, email: yuliia.tovkun@nure.ua

The modern vision of personal data protection involves an ongoing assessment of the risks that may arise for both the campaign and for other entities that are in one way or another associated with the company in the processing of personal data.

Risk assessments are essential to effective cybersecurity, helping organizations address issues that, if left unaddressed, can lead to chaos.

Organizations may mistakenly believe that the only risks they face come from cybercriminals trying to infiltrate their systems.

However, the GDPR makes it clear that data is also vulnerable to accidental or unlawful destruction, loss or disclosure.

Актуальність теми пов’язана з важливістю впровадження вимог GDPR в українських компаніях, що виходять на європейський ринок. Не дивлячись на те, що GDPR є внутрішнім актом Європейського Союзу (ЄС), у певних випадках він має екстериторіальну дію. Так, на значну частину українських компаній поширюється обов’язок GDPR compliance, що обумовлює наступне: якщо компанія виявить ризики, які мають високий рівень небезпеки у контексті обробки персональних даних (ПД), то ігнорування процедури мінімізації таких ризиків може призвести до застосування до компанії штрафних санкцій. GDPR охоплює набагато більше, ніж просто дотримання вимог регламенту. Він також може впливати на інші ризики, з якими компанії стикаються на регулярній основі [1].

У роботі розглянуто деякі з ризиків відповідності GDPR, яким слід приділити пріоритетну увагу в контексті впровадження GDPR.

1. Комплаєнс-ризики.

Розмір штрафів відповідно до GDPR є одним із головних приводів для занепокоєння більшості компаній. Штрафи накладаються за порушення відповідності – до 20 мільйонів євро або сума, що становить 4% від річного глобального обороту компанії, про яку йдеться [2].

2. Юридичні ризики.

Той факт, що GDPR поширюється на всі компанії, які опрацьовують дані громадян ЄС, викликає занепокоєння у компаній, які не розташовані в ЄС. Це також порушує питання про потенційні конфлікти з місцевим

законодавством, а також про так звані сірі зони для GDPR – правила боротьби з відмиванням грошей та подібних до них.

3. Ризики кібербезпеки.

В ідеалі всі компанії повинні спочатку мати відповідний рівень безпеки даних. На жаль, це не так, і компаніям слід приділяти пильну увагу своїм заходам щодо забезпечення безпеки та конфіденційності даних, оновлюючи та розширюючи їх за потреби.

4. Репутаційні ризики.

Ще одна частина ризиків, пов'язаних з дотриманням GDPR, стосується кількох нових прав, доступних кожному громадянинові ЄС. До них відносяться право дізнатися, які дані про громадян зберігає фірма, право стерти ці дані, тощо [2].

5. Ризики, пов'язані з новими продуктами.

Вимога проведення оцінки впливу на захист даних (DPIA) та інших оцінок змушує деякі компанії сильно змінити свої поточні графіки та операційні механізми, щоб реалізувати принцип безпеки "за умовчанням", пов'язаний з GDPR, для всіх оброблюваних даних [1].

Під час кожної оцінки ризиків необхідно враховувати кілька важливих моментів [3]. Першим з багатьох кроків є розуміння як типу, так і характеру ПД, які компанія обробляє на регулярній основі. Після визначення того, які особисті дані є у компанії і як вони обробляються, вирішуються питання щодо захисту інформації та мінімізації ризиків.

Крім того, дотримання GDPR також вимагає, щоб було підтверджено відповідальність перед різними органами захисту даних як у формі документального підтвердження зусиль із забезпечення безпеки, так і у формі демонстрацій [1].

Отже, компанія завжди повинна бути готова до ідентифікації нових ризиків та бути спроможною вирішувати питання щодо їх мінімізації. Саме така готовність, у поєднанні з іншими заходами, що реалізуються, допоможе компанії мати статус GDPR compliance на постійній основі.

Список використаних джерел:

1. GDPR [Електронний ресурс] – Режим доступу до ресурсу: https://gdpr-info.eu/.

2. Risk assessment and GDPR [Електронний ресурс] – Режим доступу до ресурсу: https://www.cpprotect.com/blog/gdpr-compliance-risks/# GDPR_compliance_risks.

3. Добринін І.С., Мальцева Н.О. Вдосконалення методики факторного аналізу інформаційних ризиків //Системи обробки інформації. – 2017. – №3. – С. 146-150.

УДК 004.056

АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОТОКОЛУ ZIGBEE ДЛЯ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

Фукс М.А.
Науковий керівник – к.т.н, доцент Куля Ю.Е.
Харківський національний університет радіоелектроніки
каф. ІКІ ім. В.В. Поповського, м. Харків, Україна
e-mail: maksymillian.fuks@nure.ua

The Internet of Things (IoT) is becoming extremely popular not only among big companies or businesses but also among people in their homes since more and more devices are designed to collect, process, and exchange vital data via the network. A wireless technology “Zigbee” was supposed to provide a low-power and cost-effective wireless IoT network. In terms of security, the technology also gives opportunities to create a highly secure network, yet it is optional since it depends on a manufacturer, which is responsible for finding a balance between security and the price of a system.

Zigbee Alliance – некомерційна організація, що займається стандартами IoT, у 2003 році створює новітню технологію на основі радіо стандарту IEEE 802.15.4 – ZigBee. Відкритий стандарт безпроводової мережі ZigBee концентрується на впроваджені сумісності Machine-to-Machine (M2M) продуктів різноманітних виробників. Більш того, впровадження зазначеного стандарту значно підвищує відмовостійкість системи, збільшує строк життя кінцевих пристроїв від однієї батареї, передбачає велику кількість підключень, а також низьку вартість. До типової структури ZigBee мережі можна віднести наступні компоненти [1]:

- координатор – грає роль центра довіри для контролю безпеки;
- роутер – відповідає за зв’язування координатора з кінцевими пристроями (забезпечення маршрутизації мережевого трафіку);
- кінцевий пристрій – звичайні пристрої, які можуть спілкуватися лише через батьківські вузли.

Довірчі відносини складають основу безпеки розглянутої мережі. Відповідно до специфікації, технологія ZigBee заснована на 128-бітному симетричному алгоритмі блочного шифрування AES, а тому обидві сторони мають знати загальний ключ для комунікації [2]. Необхідно розуміти, що стандарт IEEE 802.15.4 визначає перші два рівня – Physical Layer та Medium Access Control Layer, а ZigBee вже надбудовує додаткові рівні: Network та Application Layers. На останніх трьох рівнях забезпечується безпека передачі фреймів. Моделі безпеки, що відрізняються можливостями прийняття нового пристрою до мережі та методами захисту даних, доволі сильно впливають на роботу усієї мережі, наприклад, розподілена модель містить лише роутери та кінцеві пристрої, тому й вважається простішою, але й менш захищеною.

Кожен з роутерів може генерувати network keys, а для підключення до такої мережі кінцеві пристрої мають містити правильний pre-configured global link key, за допомогою якого, останні розшифровують повідомлення з network key від батьківських роутерів. Network key необхідний кожному з пристроїв для підтримання комунікації у мережі. Централізована система, у свою чергу, набагато безпечніша, але й складніша. Вона передбачає застосування ZigBee Trust Center (TC), що й грає роль координатора мережі. Він встановлює унікальний Global link key для використання ним та кожним з вузлів, Unique link key для кожного зі з'єднань TC-вузол, що згодом змінюється на згенерований TC link key, а також Application link key для комунікації між парою пристроїв. Насправді, ключі, які пов'язані з TC є сконфігуруваними завчасно, наприклад, у вигляді QR коду, а link keys між пристроями генеруються та шифруються з network key для передачі від TC. Він також визначає network key. Новий пристрій повинен мати pre-configured global link key для приєднання. Такий ключ може бути визначений через стандарт, як «ZigBeeAlliance09», для можливості приєднання сторонніх пристроїв, або створений виробником для обмеження такої можливості. При відсутності такого ключа координатор має можливість відправити network key у відкритому вигляді, що, звичайно, відкриє дірку у безпеці. Такий варіант поширення network key є стандартним, що є недопустимим до використання. З іншого боку, навіть знаючи link key, зловмисник може злегкістю отримати network key через захват пакетів у мережі за допомогою спеціального сніферу. Саме тому вибір та впровадження pre-configured global link key має колосальне значення, що не регулюється специфікацією ZigBee та повністю покладається на уважність виробника. Безперечно, задання власного pre-configured global link key значно підвищить безпеку усієї мережі, але така дія ускладнить впровадження нового пристрою до мережі для звичайного користувача. Отож, у залежності від цілей виробника, він може гнучко налаштовувати рівень безпеки розгортаємої мережі ZigBee. На жаль, більшість з них вкрай недооцінюють важливість запровадження достатніх рівнів безпеки, побоюючись значний ріст ціни на продукцію. Згідно зі звітом компанії Cisco вже у 2023 році кількість M2M з'єднань досягне 14.7 мільярдів, що на 15% більше у порівнянні з 2018 роком [3]. Саме тому з ростом популярності IoT пристроїв питання безпеки конфіденційної інформації повинне розглядатися більш гостро.

Список використаної літератури:

1. Security Analysis of Zigbee / Xueqi Fan., 2017. – 18 с. ZigBee Specification, 2004. – (ZigBee Alliance). Cisco Annual Internet Report (2018–2023). // White paper Cisco public. – 2020. – С. 35.

УДК 004.032.2:621.391

ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

УДК 61:621.397.13

ДОСЛІДЖЕННЯ ПРОБЛЕМАТИКИ ЗАБЕЗПЕЧЕННЯ QOS У ТЕЛЕХІРУРГІЇ ТА АНАЛІЗ ПІДХОДІВ ДО ОРГАНІЗАЦІЇ ТЕЛЕМЕДИЧНИХ СИСТЕМ НОВОГО ПОКОЛІННЯ

Воробей К.В.
Науковий керівник – доц. Омельченко А.В.
Харківський національний університет радіоелектроніки,
61166, Харків, пр. Науки, 14, каф. IMI,
тел. +38(093) 090-03-09, e-mail: kyrylo.vorobei@nure.ua.

The object of research – analysis of ways to improve quality of telesurgery services. One of the most important issues to be tackled in telesurgery is to find favorable links for routing as well as providing high Quality of Service (QoS).

The purpose of this work is analysis approaches to improve QoS level in telesurgery. In the practical part, an efficient solution over the Software Defined Networks (SDN) in order to achieve optimal and reliable routes for telesurgery application was considered.

Розвиток інтернету спричинив багато змін у науці та промисловості, де медицина не є винятком. Інтернет вплинув як на розвиток, так і на вдосконалення медичних послуг. Однією з таких послуг є телемедицина – міст між медициною та інженерією, в якій інженерні засоби можуть використовуватися медичною спільнотою для підвищення рівня здоров'я суспільства. Телемедицина використовує сучасні мультимедійні інструменти та технології, а також комунікаційні системи для надання медичних послуг дистанційно. Одним з найважливіших застосувань телемедицини є телехірургія.

Телехірургія, також відома як дистанційна хірургія, є типом хірургії, який поєднує робототехніку з сучасними технологіями. При виконанні хірургічної операції хірург не обов'язково повинен бути в тому ж фізичному місці, що й пацієнт. Основним фактором, який дозволяє хірургу контролювати операцію, є надійність телекомунікаційного каналу, який використовується для зв’язку між хірургом і хірургічним кабінетом. Це жорстка система реального часу, так що низька якість отриманого відео або тривала затримка на прийом команд роботами можуть спричинити незворотні наслідки та поставити під загрозу життя пацієнта. Однією з найважливіших проблем телехірургії є пошук сприятливих зв’язків для маршрутизації, а також забезпечення високої якості обслуговування (QoS). Загалом, кількість наскрізної затримки не повинна перевищувати більше 100 мс. Крім затримки, якість отримання відео також є важливим фактором для

забезпечення якості обслуговування (QoS). Якість отриманого відео має зворотне відношення до втрати пакетів; таким чином, чим більше втрат пакетів, тим менше якість отриманого відео. На цій основі зменшення наскрізної затримки та втрати пакетів є важливими проблемами, які постачальник мережі телеопераций повинен гарантувати для успішного виконання операції. Забезпечення QoS у телехірургії, в традиційних мережах, завжди стикалося з безліччю обмежень, які робили телеопераційю неможливою. Ці мережі, як правило, складаються з багатьох комутаторів, маршрутизаторів, брандмауерів і різноманітних центральних інструментів різних типів та подій, які можуть відбутися одночасно.

Програмно-визначені мережі (SDN), у свою чергу, являють собою сприятливі підходи до конфігурації та керування мережею. У цьому поколінні мереж рівень управління глобально керує мережею через систему адміністрування мережі, яка відповідає за визначення шляхів даних. Він відокремлений від площини даних і розміщений на центральному сервері під назвою контролер. Площина даних відповідає за передачу даних. Таке відокремлення логіки керування і розміщення її в центральному контролері, який є мозком мережі, дає можливість застосовувати політику керування, динамічно програмувати комутатори, конфігурувати та переналаштовувати мережу, легше розвивати основні мережі. Зв'язок між площиною управління та площиною даних можливий з використанням API, таких як OpenFlow. На рис.1 показана архітектура запропонованої моделі для застосування в телехірургії.

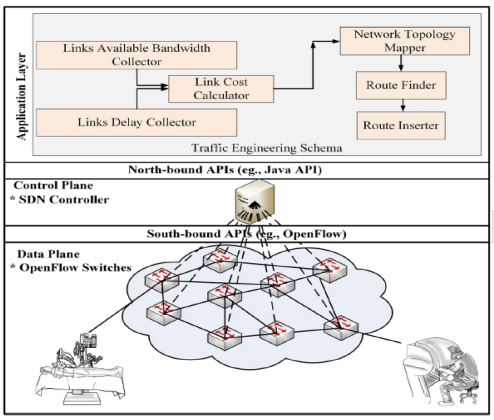


Рисунок 1 – Запропонована архітектура

Список використаних джерел:

1. Applying software-defined networking to support telemedicine health consultation during and post Covid-19 era. URL: https://link.springer.com/article/10.1007/s12553-020-00502-w (дата звернення: 25.02.2022).

УДК 656.13:004.8

ВИЗНАЧЕННЯ ОПТИМАЛЬНОГО ШЛЯХУ ТРАНСПОРТНИХ ПОТОКІВ ТА ПРОГНОЗУВАННЯ ДОРОЖНІХ ЗАТОРІВ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

Гнилицький Я. В.
Науковий керівник – ст. викл. каф. ІМІ Малінін О.П.
Харківський національний університет радіоелектроніки,
61166, Харків, пр. Науки, 14, каф. ІМІ,
тел. +38(095) 157-91-41, e-mail: yan.hnylytskyi@nure.ua.

Traffic congestion reduces the efficiency of road networks. The decline in efficiency leads to direct and indirect costs to society such as reduced working hours or environmental pollution. The purpose of the report is to develop a system that allows you to prevent traffic jams through artificial intelligence. The possibility of using it on city roads by using cameras installed next to traffic lights.

Сучасний світ вступив у нову еру обчислювальної техніки, яка привнесла багато визначних технологій, включаючи штучний інтелект (AI). Штучний інтелект дозволяє машинам або пристроям сприймати навколишнє середовище, а потім приймати розважливі рішення з подальшим виконанням ефективних дій, щоб максимізувати шанси на успішне виконання бажаного завдання або мети. Тим не менш, з швидким розвитком суспільства чисельність населення також різко зростає у всьому світі, особливо у міських районах порівняно із сільськими районами. Різке зростання населення призводить до збільшення попиту на транспорт і, отже, кількість транспортних засобів невпинно зростає. В результаті управління дорожнім рухом стає однією з основних проблем інфраструктури великих міст у всьому світі. Затори на дорогах знижують рівень працездатності дорожніх мереж. Зниження рівня призводить до прямих і непрямих витрат суспільства. Безпосереднім наслідком пробок на дорогах є втрачені робочі години. Згубні наслідки заторів різко зростають, коли цінність часу як товару різко зростає під час надзвичайних ситуацій. Знаходження в пробці впливає на поведінку людей. Високий рівень заторів може призвести до агресивної поведінки водіїв. Ця агресія може виявлятися в агресивному керуванні, що збільшує ймовірність нещасних випадків. Високий рівень заторів також призводить до збільшення викидів парникових газів, що згубно впливає на навколишнє середовище.

Метою доповіді є розробка системи, яка дозволяє запобігати заторам на дорогах за рахунок штучного інтелекту. Інфраструктура, необхідна для збору даних про трафік, удосконалювалася протягом десятиліть. Це поліпшення у поєднанні з підвищеною доступністю обчислювальних ресурсів дозволило

використати можливості прогнозування глибоких нейронних мереж. Система може забезпечити зменшення заторів та може сприяти вільному потоку трафіку, а також допомогти в керуванні світлофором, але справжня перевага технології у тому, що вона звільнює людей від стомлюючої та трудомісткої повсякденної роботи та надає можливість виконувати більш важливу працю. До уваги беруться п'ять параметрів, включаючи обсяг трафіку, щільність трафіку, зайнятість, індекс завантаженості трафіку та час у дорозі під час моніторингу та прогнозування заторів на дорогах. Прогнозуючі моделі трафіку є ключовою частиною визначення маршруту руху. Якщо прогнозується, що трафік в одному напрямку може стати інтенсивним – автоматично знаходиться альтернатива з меншим трафіком. Також враховується низка інших факторів, таких як якість доріг. Дорога асфальтована чи не асфальтована, покрита гравієм чи брудом? Такі елементи можуть утруднити рух дорогою, у зв'язку з цим ця дорога зарекомендована як частина маршруту користувача з меншою ймовірністю. Також відіграють ключову роль розмір і прямолінійність дороги - їхати шосе часто більш ефективно, ніж меншою дорогою з декількома зупинками. А звіти про інциденти дозволять швидко показати, чи закрита дорога чи провулок, чи є поблизу будівництво, несправний автомобіль чи об'єкт на дорозі і чи є несподівані зміни через зсуви, снігові бурі чи інші стихійні лиха.

Залежно від характеру даних, що збираються, застосовуються різні підходи AI для оцінки параметрів перевантаження. Прогнозування заторів на дорогах складається із збору даних та розробки моделі прогнозування. Кожен крок методології важливий і може вплинути на результати, якщо не буде виконаний правильно. Після збору даних обробка даних грає важливу роль для підготовки наборів даних для навчання та тестування. Область дослідження відрізняється для різних досліджень. Після розробки моделі вона перевіряється з іншими базовими моделями та підтверджує справжні результати.

Список використаних джерел:

1. Moranduzzo T., Melgani F. Automatic Car Counting Method for Unmanned Aerial Vehicle Images. IEEE, 2013. 1635 c. URL: https://doi.org/10.1109/TGRS.2013.2253108.

2. Zhuang P., Shang Y., Hua B. Statistical methods to estimate vehicle count using traffic cameras. Multidimensional Systems and Signal Processing. 2008. Т. 20, № 2. С. 121–133. URL: https://doi.org/10.1007/s11045-008-0068-x.

3. Janson B. N. Dynamic traffic assignment for urban road networks. Transportation Research Part B: Methodological. 1991. Т. 25, № 2-3. С. 143–161. URL: https://doi.org/10.1016/0191-2615(91)90020-j.

УДК 621.396.6

ДОСЛІДЖЕННЯ ХАРАКТЕРИСТИК РАДІОМЕРЕЖІ ІЗ ВИКОРИСТАННЯМ ПОВІТРЯНОГО РЕТРАНСЛЯТОРА

Шейко П.Ю.
Науковий керівник – доцент Іваненко С.А.
Харківський національний університет радіоелектроніки, каф. ІК
м. Харків, Україна
тел.+380958261364, e-mail: pavlo.sheiko@nure.ua

The air repeater contains a transport platform, an automatic system control of unmanned aerial vehicle, radio station, antenna device. Transport the platform is made in the form of an unmanned aerial vehicle. Air repeater further comprising a signal analysis device, a control and monitoring device, a deviceautomatic signal power control. A radio repeater is a combination of a radio receiver and a radio transmitter that receive and retransmit a signal so that two-way radio signals can travel longer distances. The repeater, located at high altitude, can pass two mobile stations, otherwise - out of sight of each other's range, for communication. Repeaters are available in professional, commercial and government mobile radio systems, as well as in amateur radio.

В сучасному світі дуже часто ставиться питання зв'язку на складній місцевості, наприклад в горах, і при цьому не витрачати багато часу і грошей запускаючи супутник, тому все частіше використовують повітряні ретранслятори, які можуть бути розташовані хоч на повітряній кулі, хоч на БПЛА або літаку у кожного з цих типів розміщення, є плюси та мінуси. Далі ми розглянемо кілька прикладів їх використання

Для початку згадаємо що таке ретранслятор, ретранслятор — обладнання зв'язку, яке з'єднує два або більше радіопередавачів, віддалених один від одного на великі відстані. У разі використання космічних засобів зв'язку, говорять про супутники зв'язку або про супутники-ретранслятори. Ретранслятори поділяють на активні та пасивні, але повітряних ретрансляторах використовують зазвичай активні ретранслятори.

Зазвичай повітряні ретранслятори виробляють та використовують військові, тому розглянемо приклад розміщення на літаку Ту-214СР.

Ту-214СР — літак-ретранслятор, розроблений спеціально для встановлення зв'язку у складних місцях дислокації військ.

Літак Ту-214СР є спеціальним літаком-ретранслятором, створеним на базі звичайного пасажирського Ту-214. На відміну від базової моделі Ту-214СР оснащений додатковими паливними баками, завдяки яким дальність його польоту збільшена до 10 тис. кілометрів, системами енергопостачання

та радіотехнічним комплексом. Ту-214СР оснащений радіотехнічним комплексом, що забезпечує через супутникові системи зв'язок із наземними об'єктами та іншими повітряними судами. Військові користуються радіорелейним зв'язком. Однак такий зв'язок працює тільки в межах прямої видимості, тому для неї потрібна система наземних радіостанцій, літаків-ретрансляторів та супутників.

Але у ретранслятора встановленого на літаку є свої плюси, так і мінуси в виді часу його роботи, оскільки літак має обмежений запас топлива, тому розглянемо варіант розміщення ретранслятора на повітряній кулі.

Для військових створено перший аеростатний комплекс ретрансляції. піднята на висоту кількох кілометрів система здатна передавати великі обсяги інформації та оперативно доводити до військ команди штабів. Пристрій обсягом близько 3 тис. кубометрів зможе піднімати на висоту до 3,5 км. апаратуру масою 300 кг.

Апарат здатний до півмісяця безперервно працювати на висоті без заряджання газом на землі. Комплекс можна використовувати, наприклад, для організації дальнього радіозв'язку та забезпечення загоризонтної радіолокації. У поєднанні з іншими засобами зв'язку новинку можна використовувати для координації дій військової авіації.

Враховуючи вище зазначене можемо визначити що у кожного із видів розміщення існують як і плюси так і мінуси, але визначити кращий не являється можливим, так як різні ситуації потребують різних технічних рішень, тому зазвичай використовують всі вище зазначені методи одночасно.

Список використаних джерел:

Takamasa Y. Висотна куля - High-altitude balloon [Електронний ресурс] / Yamagami Takamasa // wikijaa. – 2021. – Режим доступу до ресурсу: https://uk.wikijaa.ru/wiki/High-altitude_balloon.

Думітраш В. Аналіз напрямків розвитку систем радіозв'язку НАТО [Електронний ресурс] / В. Думітраш // Ukrainian Military Pages. – 2020. – Режим доступу до ресурсу: https://www.ukrmilitary.com/2020/08/signal.html.

Ретранслятор [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/

УДК 004.032.2:621.391

МОДЕЛЬ ПРОГНОЗУ ДЛЯ ДАНИХ ПРО ПРОДАЖІ НА ОСНОВІ КЕРОВАНИХ ВЕБ-СЕРВІСІВ AMAZON

Юр'єв Я.В.
Науковий керівник – к.т.н., доц. Кривенко С.А.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Науки, 14, каф. IMI,
тел. +38(095) 553-95-71, e-mail: yaroslav.yuriev@nure.ua.

This paper describes the use of machine learning to predict data and the use of artificial intelligence algorithms to predict sales. To achieve this goal, it is proposed to use Amazon services: SageMaker (machine learning modeling and placement service) and Forecast (high-precision forecasting service based on machine learning technologies).

Дані часових рядів фіксуються в хронологічній послідовності протягом визначеного періоду часу. Введення часу в модель машинного навчання має позитивний вплив, оскільки модель може отримати сенс із зміни точок даних з часом. Дані часових рядів, як правило, корелюють, що означає, що існує залежність між точками даних. Оскільки у нас є проблема з регресією, а також оскільки регресія передбачає незалежність точок даних, нам необхідно розробити модель обробки залежності даних. Метою розробки цієї моделі і відповідного методу є підвищення достовірності прогнозів для даних про продажі.

Машинне навчання (Machine Learning) — це тип штучного інтелекту (Artificial Intelligence), який дозволяє програмним додаткам стати більш точними в прогнозуванні результатів, не будучи явно запрограмованим на це. Алгоритми машинного навчання використовують історичні дані як вхідні дані для прогнозування нових вихідних значень. Прогнозування є важливою областю машинного навчання. Це важливо, оскільки багато можливостей для прогнозування майбутніх результатів базуються на історичних даних. Багато з цих можливостей включають часовий компонент. Хоча компонент часу додає більше інформації, він також ускладнює вирішення проблем часових рядів, ніж інші типи передбачень.

Amazon SageMaker — це повністю керована служба машинного навчання. За допомогою SageMaker науковці та розробники даних можуть швидко й легко створювати й навчати моделі машинного навчання, а потім безпосередньо розгортати їх у готовому для виробництва середовищі розміщення. Вона надає інтегрований екземпляр віртуальної машини для розробки Jupyter для легкого доступу до джерел даних для дослідження та аналізу без потреби керувати серверами. Служба також надає загальні

алгоритми машинного навчання, які оптимізовані для ефективної роботи з надзвичайно великими даними в розподіленому середовищі. Завдяки вбудованій підтримці алгоритмів і фреймворків від користувача, SageMaker пропонує гнучкі розподілені варіанти навчання, які адаптуються до конкретних робочих процесів користувачів. Розгортання моделі у безпечному та масштабованому середовищі відбувається за допомогою SageMaker Studio або консолі SageMaker.

Amazon Forecast — це повністю керований сервіс, який використовує машинне навчання для надання високоточних прогнозів. На основі тієї ж технології, що використовується на Amazon.com, Forecast використовує машинне навчання для поєднання даних часових рядів з додатковими змінними для побудови прогнозів. Щоб розпочати створення прогнозу, не потрібен досвід машинного навчання. Користувачу потрібно надати лише історичні дані, а також будь-які додаткові дані, які, на його думку, можуть вплинути на прогнози. Наприклад, попит на певний товар може змінюватися в залежності від сезону та розташування магазину. Цей складний зв'язок важко визначити самостійно, але машинне навчання ідеально підходить для його розпізнавання. Щойно користувач надає свої дані, Forecast автоматично перевірить їх, визначить, що є значущим, і створить модель прогнозування, здатну робити прогнози, які є на 50% точнішими, ніж перегляд лише даних часового ряду. Amazon Forecast автоматизує більшу частину процесу прогнозування часових рядів, дозволяючи зосередитися на підготовці наборів даних та інтерпретації ваших прогнозів. Forecast надає вказані нижче функції.

Автоматичне машинне навчання – Forecast автоматизує складні завдання машинного навчання, знаходячи оптимальну комбінацію алгоритмів машинного навчання для наборів даних. Найсучасніші алгоритми – застосування комбінацій алгоритмів машинного навчання, які базуються на тій же технології, що й на Amazon.com. Forecast пропонує широкий спектр алгоритмів навчання, від широко використовуваних статистичних методів до складних нейронних мереж.

Підтримка відсутніх значень – Forecast надає кілька методів заповнення для автоматичної обробки відсутніх значень у наборах даних. Додаткові вбудовані набори даних – Forecast може автоматично включати вбудовані набори даних, щоб покращити модель. Ці набори даних уже розроблені і не потребують додаткової конфігурації. Запропонована модель і відповідні методи підвищують достовірність прогнозів для даних про продажі [1].

Список використаних джерел:

1. AWS Documentation. Amazon Web Services. URL: https://docs.aws.amazon.com/index.html (дата звернення: 20.02.2022).

АЛФАВІТНИЙ ПЕРЕЛІК

ЗМІСТ

ДЛЯ НОТАТКІВ

«РАДІОЕЛЕТРОНІКА І МОЛОДЬ У XXI СТОЛІТТІ»

МАТЕРІАЛИ 26-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

Відповідальний за випуск: А.В. Снігуров

Комп'ютерна верстка О.І. Ільїна

Матеріали збірника публікуються в авторському варіанті без редагування

Підп. до друку 09.04.2022 Формат 60x84 1/16 Спосіб друку - ризографія

Умов. друк. арк. 10,23 Тираж 99 прим.

Зам. № __-____. Ціна договірна _

ХНУРЕ. Україна. 61166, Харків, просп. Науки, 14

Віддруковано в редакційно-видавничому відділі ХНУРЕ 61166, Харків, просп. Науки, 14

NURE