МАТЕРІАЛИ XXVII МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

# РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ У XXI СТОЛІТТІ

2023

ТОМ 4

ХАРКІВ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЛЕКТРОНІКИ

МАТЕРІАЛИ 27-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ
«РАДІОЕЛЕТРОНІКА І МОЛОДЬ У XXI СТОЛІТТІ»

10 – 12 травня 2023 р.

Том 4

КОНФЕРЕНЦІЯ

# «ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОКОМУНІКАЦІЙ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ ТЕХНОЛОГІЙ»

Харків 2023

УДК 004:[621.317+621.391](06)

27-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. Матеріалів форуму. Т.4. – Харків: ХНУРЕ. 2023. – 192 с.

В збірник включені матеріали 27-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь у XXI столітті».

Видання підготовлено факультетом інфокомунікацій
Харківського національного університету радіоелектроніки

61166 Україна, Харків, просп. 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 004.75

# ХМАРНІ ТЕХНОЛОГІЇ, БАЛАНСУВАННЯ НАВАНТАЖЕННЯ, ТРАФІКУ

Новіченко Є.О.
Науковий керівник – доц. Сабурова О.С.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
тел. +38(096) 552-30-10, e-mail: yelyzaveta.novichenko@nure.ua.

In recent years, cloud technologies have gained popularity both in the daily life of users and in business. This includes different methodologies, tools, and software and hardware. Thanks to the specified mechanisms, the user can implement tasks, goals or projects. The work is performed on a remote server, which allows you to avoid a lot of problems with saving information and configuring the infrastructure. Cloud technologies are a trend that will stay with us for a long time and will only gain momentum. After all, the cloud is not just a useful tool for storing data and performing calculations, it helps companies adapt to changes, the scale and dynamics of which are growing.

Поняття «хмарних обчислень» з’явилося в 1960 році, коли Джон Маккарті висловив припущення, що колись комп'ютерні обчислення будуть проводитися за допомогою загальнонародних утиліт.

Попит на хмарні ресурси зростає з кожним днем. Так, згідно з дослідженнями компанії RightScale, за останні три роки частка бізнесів, що використовують хмарні сервіси, зросла з 89% до 92%. Очікується, що до 2024 року цей показник зросте до 90% [1].

Cloud computing – концепція «обчислювальної хмари», згідно з якою програми запускаються та видають результати роботи у вікно стандартного веб-браузера на локальному ПК, при цьому всі програми та їх дані, необхідні для роботи, знаходяться на віддаленому сервері в Інтернеті .

За архітектурою хмарні технології поділяються на три види – публічна, приватна та гібридна, яка поєднує в собі перші два види хмари.

За принципом взаємодії з користувачем розрізняють три типи хмарних обчислень - інфраструктура як послуга (IaaS), програмне забезпечення як послуга (SaaS), платформа як послуга (PaaS).

Хмарні обчислення, як і будь яка система, повинна безперебійно працювати. Однією з характеристик безперебійної роботи системи є висока доступність, яка забезпечується балансуванням навантаженості.

Балансування навантаженості - це технологія, яка дозволяє розподіляти вхідний трафік між декількома серверами. В хмарних обчисленнях існують три алгоритма балансування навантаження, які представлені на рисунку 1.

1. Round-Robin. Усі сервери в пулі отримують запити по черзі. Наприклад, Server1 обробляє перший запит, Server2 - другий і так далі по колу. Але важливо, щоб усі сервери мали однаковий обсяг ресурсів;

2. Weighted. Оновлена версія попереднього алгоритму. У кожного сервера з'являється свій коефіцієнт продуктивності залежно від його потужності та можливостей. Чим більший цей ваговий коефіцієнт, тим більше навантаження здатний відпрацювати сервер;

3. Least Connections. Цей алгоритм враховує кількість активних підключень, що підтримуються серверами у певний період, тобто він бачить, який сервер активно працює, а який простоює. І наступний запит надсилає саме туди, де обробляється найменший обсяг трафіку [2].

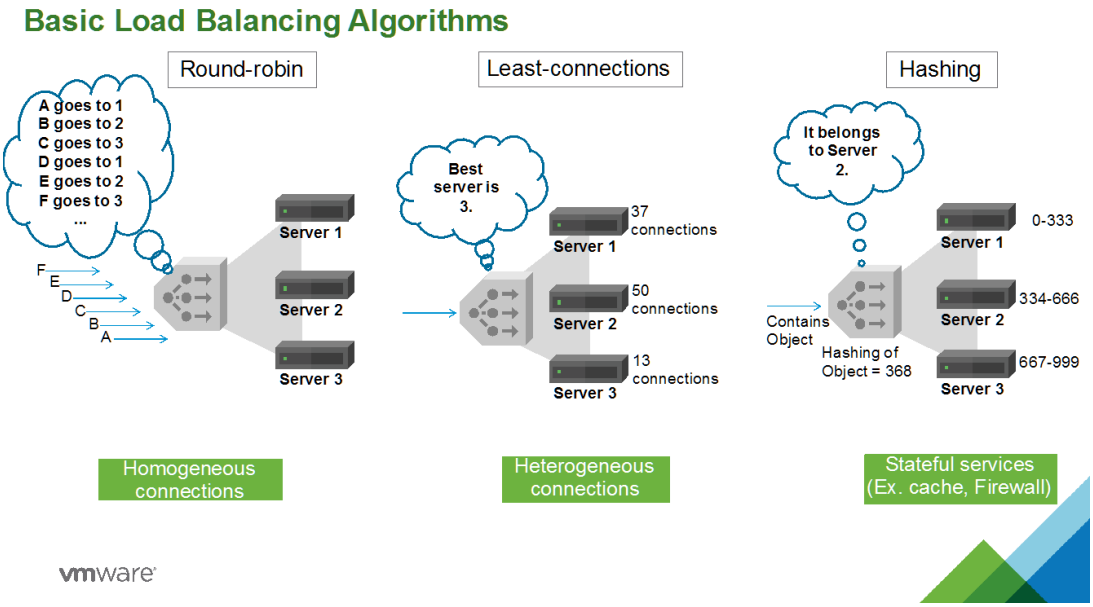



Рисунок 1 – Алгоритми балансування навантаження

Впровадження хмарних технологій дозволяє розширити простір для роботи з інформацією, підвищити надійність, зручність, економічність і мобільність бізнес-процесів без додаткових витрат Сучасні рішення з балансування навантаження дозволяють більш ефективно і дбайливо використовувати серверне обладнання, забезпечуючи стабільність обслуговування. Використання хмарного балансувальника навантаження запобігає перетворенню сервера на єдину точку збою, підвищуючи надійність інфраструктури.

Список використаних джерел:

1. Kmbs. Хмарні тренди. Лідерство і менеджмент. Культура (2021, 17 червня) https://kmbs.ua/ua/article/cloud-trends

2. Cloud4y. Балансування навантаження стає хмарним (2022, 4 травня) https://www.cloud4y.ru/blog/cloud-load-balancing/

УДК 621.396.946

# СХЕМИ МОДУЛЯЦІЇ ДЛЯ СИСТЕМ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ 5G

Петрачков М.О.
Науковий керівник – д.т.н., проф. Коляденко Ю.Ю.
Харківський національний університет радіоелектроніки
каф. ІКІ ім В.В. Поповського,
м. Харків, Україна
тел. +38(097) 034-14-54, e-mail: maksym.petrachkov@nure.ua

The choice of a specific type of modulation depends on such characteristics of the communication system as bandwidth, noise immunity, capacity. Various types of modulation based on subband filtering, pulse shaping, and precoding to reduce out-of-band interference have been proposed to enable communication networks to meet the requirements of 5G networks. This work is devoted to an overview of the main types of modulation for 5G systems.

Для передачі даних у системах зв'язку можуть бути використані дві основні категорії сигналів: сигнали з однією несійною і сигнали з багатьма несійними. У системах зв'язку попередніх поколінь 2G і 3G використовувалися сигнали з однією несійною, а в системах зв'язку 4G (Long Term Evolution, LTE-A) з багатьма. Такі ж сигнали були використовуються в системах зв'язку 5G. Для сигналів з однієї несійною характерно невеликі значення відношення пікової потужності до середньої потужності (Peak-to-Average Power Ratio, PAPR). Область застосування сигналів з однієї несійною - пристрої Інтернету речей (Internet of Things, IoT) з тривалим терміном служби акумуляторної батареї. Крім того, перевага даних сигналів в мінімізації втрат при передачі по радіоканалу стають помітними на високих несійних [1].

Сигнали з багатьма несійними дозволяють гнучко розподіляти ресурси в частотній області, а також забезпечити високу спектральну ефективність при їх сумісному використанні з технологією MIMO (Multiple Input Multiple Output)..Окрім цього, такий вид сигналів легко сумісний з новою технологією неортогонального багаточисельного доступу (Non-Orthogonal Multiple Access, NOMA.). Саме за цими причинами в системах зв'язку 5G, в основному, використовуються сигнали з багатьма несійними.

Для модуляції сигналу на рівні піднесійних в системах зв'язку 5G як на лінії вгору, так і на лінії вниз можуть бути використані наступні схеми модуляції:

• квадратна фазова модуляція (Quadrature Phase Shift Keying, QPSK);

• квадратна амплітудна модуляція (Quadrature Amplitude Modulation, QAM) різної кратності (16-QAM, 64-QAM, 256-QAM).

Крім того, для лінії вгору також можливе використання модуляції 1024-QAM з метою забезпечення більш високих швидкостей передачі

даних, а для лінії вниз в сценарії mMTC з метою підвищення ефективності передачі при низьких швидкостях може бути використана модуляция BPSK (Binary Phase Shift Keying) [1,2].

Як відомо, збільшення порядку модуляції вимагає підвищення відношення сигнал-шум (ВСШ) для досягнення прийнятних показників завадостійкий. У таблиці 1 наведені потрібні значення ВСШ для різних типів модуляції без завадостійкого кодування, при якому рівень коефіцієнта бітових помилокк (Bit Error Rate, BER) складає порядка $10^{-3}$.

Табл. 1. Необхідні значення відношення сигналів/шум для передачі з різними типами модуляції при BER= $10^{-3}$

| Модуляція | BPSK | QPSK | 16-QAM | 64-QAM | 256-QAM |
|---|---|---|---|---|---|
| ВСШ | 7 | 10 | 17,5 | 24 | 30 |

З табл. 1 можна побачити, що діапазон змін зміни ВСШ в залежності від типу модуляції становить близько 23 дБ, а спектральна ефективність при цьому змінюється в 8 разів через застосування різних типів модуляції.

Ймовірно, що при дальшому розвитку мережі зв'язку набор підтримуваних типів модуляції буде розширений, а також нові види модифікації для різних категорій будуть включені в специфікації 3GPP [3].

Вибір типу модуляції впливає, в першу чергу, на швидкість передачі даних в каналах з фіксованою смугою частот.

Параметри модуляції для кожного користувача слід налаштовувати незалежно і гнучко, щоб підтримувати користувачів з різними вимогами до швидкості передачі даних.

Для зменшення позасмугового випромінювання можуть бути використані типи модуляції, які засновано на піддіапазонній фільтрації. Два основні з них це: багаточастотна передача з універсальною фільтрацією UFMC (Universal Filtered Multi-Carrier) і так звана модиляція OFDM з фільтрацією (f-OFDM).

Список використаних джерел:

1. Mosa Ali Abu-Rgheff. 5G Physical Layer Technologies/ Mosa Ali Abu-Rgheff / Wiley-IEEE Press. – 2019. - 592 p.

2. Mladen Bozanic. Mobile Communication Net-works: 5G and a Vision of 6G/ Mladen Bozanic, Saurabh Sinha / Springer. – 2021. - 348 p.

3. Harri Holma. 5G Technology: 3GPP New Radio/ Harri Holma, Antti Toskal, Takehiro Nakamura / Wiley.- 2020. - 536 p.

УДК 621.391

# ОСОБЛИВОСТІ ОПТИМІЗАЦІЇ БІЗНЕС-ПРОЦЕСІВ CALL CENTER

Радченко Р.В.
Науковий керівник – доц. 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.

Features of CALL CENTER business process optimization are presented on the basis of the proposed model, which includes directions for ensuring the parameters of efficiency and quality of user service. Achieving high KPI performance has allowed companies to maximize the productivity of their agents, expand their reach and, most importantly, deliver higher quality of customer service on an unprecedented scale. Taking into account all the methods implemented on the basis of theoretical research, it is possible to separate the main strategic directions that will help to improve the qualitative and qualitative parameters of the effectiveness of their activities.

Оптимізація бізнес-процесів CALL CENTER відноситься до тих дій, які виконуються для підвищення параметрів KPI: продуктивності, ефективності та результативності обслуговування клієнтів. Ці оптимізації можуть бути пов’язані з внутрішніми процесами або особистим досвідом, що використовують оператори при взаємодії з абонентами [1].

Для бізнес-процесів CALL CENTER зазвичай виділяють 7 основних способів оптимізації: інтеграція каналів зв’язку; використання баз даних; якісне програмне забезпечення; використання інтелектуальної маршрутизації викликів; автоматизація повторень завдань; збільшення кількості запитів; використання внутрішньої системи комутації.

Інтеграція каналів з клієнтами. Телефонний зв’язок залишається ключовим елементом обслуговування клієнтів, хоча передавати інформацію можна через різноманітні цифрові канали. Інвестування в багатоканальне програмне забезпечення (ПЗ) має важливе значення для оптимізації роботи CALL CENTER. Співробітникам надається допомога при роботі з кількома каналами та складною взаємодією з клієнтами, що робить безшовний робочий процес, коли всі канали інтегровані і координуються як єдиний канал.

Використання баз даних значно покращує роботу операторів служби підтримки. Це допомагає уникнути направлення дзвінків до інших відділів або тривалого пошуку інформації за запитом. Якісне програмне забезпечення для CALL CENTER може допомогти у роботі з деякими зручними функціями, як наприклад маршрутизація дзвінків, переадресація, запис дзвінків, тощо.

Використання інтелектуальної маршрутизації викликів за допомогою IVR-системи спрямовує трафік співробітника або тих, хто телефонує в

потрібний відділ, ґрунтуючись на функціях голосового меню. Інтелектуальна маршрутизація означає, що запити клієнтів з більшою ймовірністю будуть оброблені першим агентом, з яким клієнт заговорить. Це покращить якість обслуговування і прискорить роботу.

CALL CENTER все більше покладаються на автоматизацію повторень завдань. Оператори мають великий обсяг завдань, з якими не завжди встигають впоратись, тому автоматизація типових задач є чудовим рішенням. ПЗ дає можливість знизити кількість помилок при обробці дзвінків та переадресувати повідомлення в інші служби компанії. Збільшення кількості запитів, які вирішуються при першому дзвінку.

Завдяки таким вирішенням збільшується потік і швидкість інформації, що обробляється, підвищується лояльність клієнтів, скорочується кількість повторних звернень та зростають продажі. Використання внутрішніх систем комутації дозволяє операторам зв’язуватись з колегами, менеджерами або технічною службою з корпоративного чату в момент розмови і не переадресовувати дзвінки. Враховуючи всі вищесказані методи, можна відокремити основні стратегічні напрями, які допоможуть підвищити якісні та кількісні параметри ефективності діяльності CALL CENTER, що запропоновано на рис. 1.


Рисунок 1 – Модель підвищення якісних та кількісних параметрів ефективності CALL CENTER

Висновки:

1. Оптимізація бізнес-процесів підвищує рівень задоволеності клієнтів та продуктивність співробітників CALL CENTER.
2. Технології нових поколінь бізнес-процесів дозволяють компаніям забезпечувати більш високу якість обслуговування клієнтів у безпрецедентних масштабах.
3. Відстеження останніх тенденцій важливо, щоб залишатись на крок попереду.

Список використаних джерел:

1. Корнєйцова Н.В., Модель забезпечення якості роботи CALL CENTER, / Корнєйцова Н.В. //24-й молодіжний форум «РАДІОЕЛЕКТРОНІКА І МОЛОДЬ В XXI СТОЛІТТІ» – 2021 – С.32-33.

УДК 621.316.729

# ЗАМКНУТІ ТАКТОВІ СИНХРОНІЗАТОРИ

Усатий Д.О.
Науковий керівник – д.т.н., проф. Коляденко Ю.Ю.
Харківський національний університет радіоелектроніки
каф. ІКІ ім В.В. Поповського,
м. Харків, Україна
тел. +38(066) 475-90-29, e-mail: denys.usatyi@nure.ua

Analysis of the shortcoming of open symbol synchronizers, indication of the solution to the shortcoming. Analysis of the scheme and operation of a closed clock (symbol) synchronizer. Analysis of clock (symbol) synchronization.

Основним недоліком розімкнутих символьних синхронізаторів є наявність помилки супроводу з ненульовим середнім. Замкнуті символьні синхронізатори порівнюють вхідний сигнал з локально генеруючими тактовими імпульсами з наступною синхронізацією локального сигналу з переходами у вхідному сигналі [1]. Серед найпоширеніших замкнутих символьних синхронізаторів можна виділити синхронізатор з випереджальним і запізненим стробуванням (рис. 1) [1].

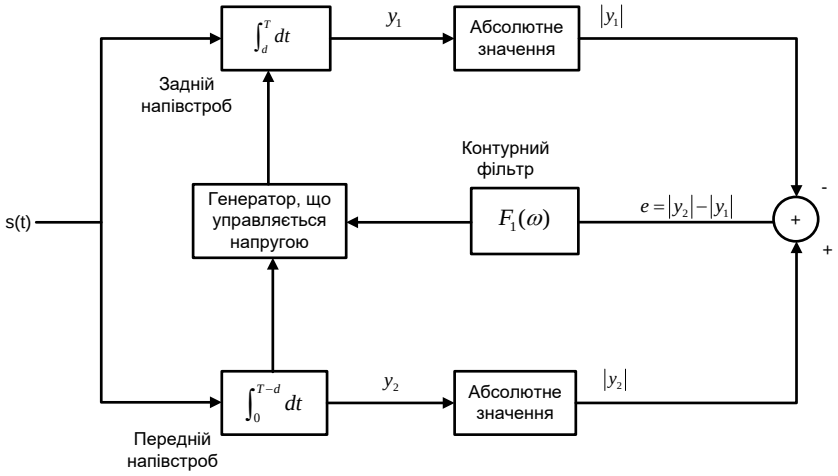



Рис. 1. Схема замкнутого тактового (символьного) синхронізатора

Робота синхронізатора полягає у виконанні двох окремих інтегрувань енергії вхідного сигналу по двох різних проміжках символьного інтервалу тривалістю ($T$—$d$) секунд.

Різниця абсолютних значень виходів інтеграторів $y_1$ і $y_2$ є мірою помилки синхронізації символів приймача й може подаватися назад для корекції прийому.

Робота синхронізатора з випереджальним і запізнювальним стробуванням пояснюється епюрами, наведеними на рис. 2 [2].

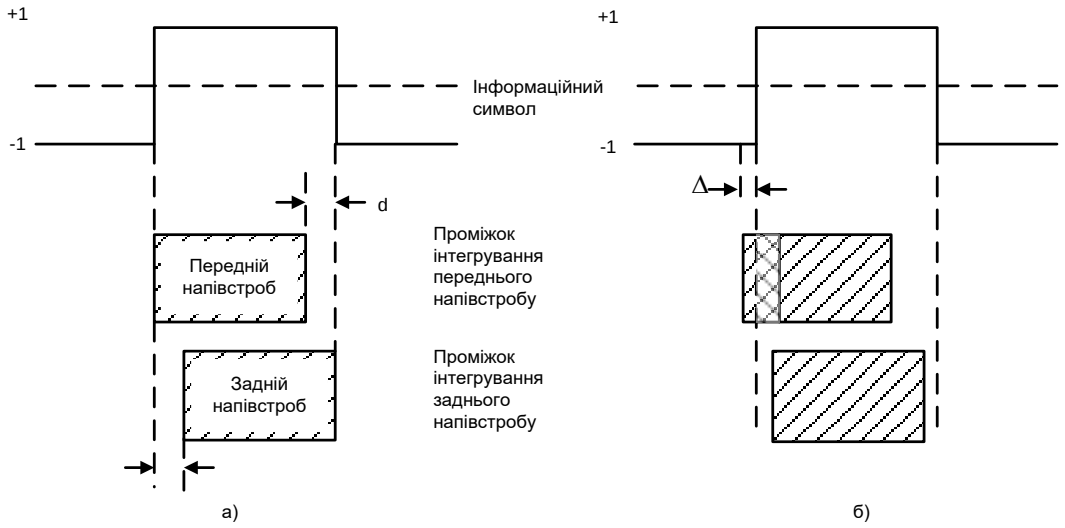



Рис. 2. Тактова (символьна) синхронізація: *а* — тонка синхронізація приймача; *б* — синхронізація з випередженням

При ідеальній синхронізації (рис. 2, *а*) показано, що обидва періоди стробування потрапляють в інтервал передачі символу. У цьому випадку обидва інтегратори одержать однаковий обсяг енергії сигналу й різниця відповідних сигналів дорівнюватиме нулю. На рис. 2, *б* показаний приклад для приймача, генератор тактових імпульсів якого функціонує з випередженням. У цьому випадку початок інтервалу випереджального інтегрування попадає на попередній інтервал передачі біта, що тоді як запізнювальне інтегрування, як і раніше, виконується в межах поточного символу [2].

При запізнювальному інтегруванні енергія накопичується за інтервал часу ($T$—$d$), як і у випадку, зображеному на рис. 2, *а*, але випереджальне інтегрування накопичує енергію тільки за час $[(T - d) - 2\Delta]$, де $\Delta$ — частина інтервалу випереджального інтегрування, що припадає на попередній інтервал передачі біта. Отже, для цього випадку сигнал неузгодженості дорівнюватиме $e = -2\Delta$, що призведе до зниження вхідної напруги ГУН (рис. 1). Це, у свою чергу, призведе до зниження вихідної частоти ГУН і сповільнить відлік часу приймача для узгодження із вхідними сигналами.

Список використаних джерел:

1. Бойко В.І. Цифрова схемотехніка./ В.І. Бойко, В.В. Багрій. – К: ІЗМН, 2001.- 228 с

2. Коляденко Ю.Ю. Анализ характеристик систем цикловой синхронизации с использование протокола PTP (IEEE1588v2)/ Ю.Ю. Коляденко, И.С. Шостко, Д.В. Агеев / Радіоелектроніка, інформатика, управління. ISSN 1607-3274. 2019. № 3 (50) с. 99-107. DOI 10.15588/1607-3274-2019-3-11

УДК 621.396.6

# МЕТОД ЗМЕНШЕННЯ ЧАСУ ДОСТУПУ ДО КАНАЛУ ПЕРЕДАЧІ В КОГНІТИВНІЙ МЕРЕЖІ

Дробяз М.О.
Науковий керівник – д.т.н., проф. Коляденко Ю.Ю.
Харківський національний університет радіоелектроніки
каф. ІКІ ім В.В. Поповського, м. Харків, Україна
тел.+38(066)-823-87-61, e-mail: mykhailo.drobiaz@nure.ua

By applying these models, it is possible to reduce the time that the RED SU spends on accessing the channel. This reduction is achieved by creating a probabilistic model of the behavior of the RED PU, which allows you to start preparing for channel occupation in advance (for example, pre-configuration of SDR devices and loading of the necessary control applications at the MAC level), which increases the effective time of using the channel on the RED SU side.

При розподілі канальних ресурсів в рамках процедур динамічного доступу до каналів передачі в когнітивних мережах необхідно зменшити час доступу до каналу для вторинних радіокористувачів. Для вирішення проблеми зменшення часу доступу до каналу на MAC-рівні в когнітивних мережах необхідно забезпечити пріоритет доступу первинного радіокористувача. Іншими словами, на відміну від багатоканальних бездротових мереж, які не що використовують когнітивні методи та технології, первинний користувач РЧС, канальний ресурси якого використовується в когнітивній мережі, має необхідний канал, який повинен бути завжди доступним [1].

Отже, якщо первиниий користувач РЧС виявляє будь-яким доступним способом факт початку роботи на зайнятому каналі, вторинний користувач РЧС повинен від’єднатися від працюючого протягом найближчого достатньо короткого часу (реальний час або розумна затримка). З іншого боку, як тільки первинний користувач РЧС припине роботу, вторинний користувач може знову зайняти звільнений канал і продовжити процесу обміну інформацією з відповідним пристроєм [2].

Припустимо, що кожен РЕЗ PU містить приймально – передавальний пристрій, що має доступ до позасмугового або внутрішньосмугового каналу управління. РЕЗ SU також має пристрій прийому-передачі інформації, який може бути налаштований на роботу на будь-якому каналі в ліцензійній зоні радіочастотному спектору, в першу чергу, для визначення того, які канали були звільнені від роботи РЕЗ PU.

Для виявлення тимчасово вільних каналів для РЕЗ SU, пропонується використовувати два можливих способи зондування:

1. Метод аналізу випадково обраних ділянок РЧС для виявлення наявность вільних робочих каналів.

2. Методи, що використовують бази даних геолокації для координації вибору ліцензованих користувачів та каналів РЧС.

Канальна модель когнітивних комунікацій описується двома станами, позначеними як «ON/OFF», де стан «OFF» означає, що канал зайнятий РЕЗ PU, стан «ON» означає, що канал вільний для РЕЗ SU [1]. Модель використання каналу ON/OFF описує стан каналу, коли РЕЗ PU займає або звільняє канал, а РЕЗ SU може приймати і передавати інформаці, використовуючи канал у стані ON. Далі, час початку і закінчення кожного стану синхронізується для всіх РЕЗ SU і для всіх n-каналів (рис.1).

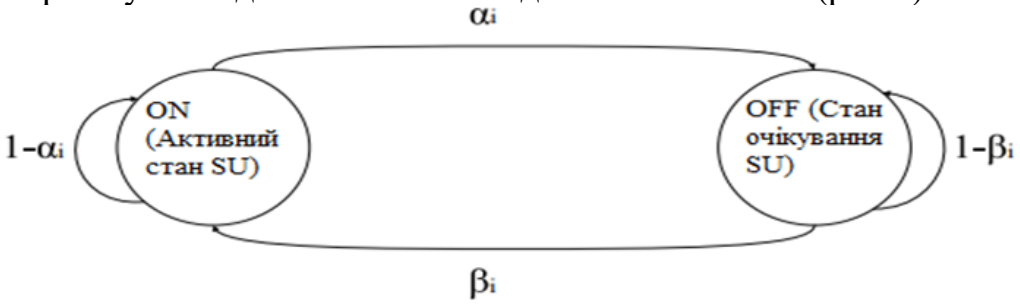



Рисунок 1 - Модель використання каналу ON/OFF для РЕЗ SU

Рисунок 2 показує тимчасову діаграму подій заняття та звільнення каналів у ліцензійнії зоні РЧС.

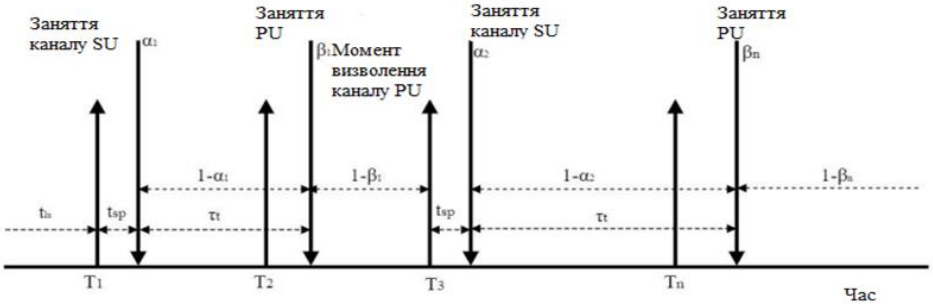



Рис. 2 - Тимчасова діаграма подій заняття та звільнення каналу когнітивної мережі

Момент «Заняття PU» відповідає моменту, коли від первинного користувача РЧС, надходить запит на обслуговування і в результаті обробки цього запиту канал повинен бути оперативно звільнений РЕЗ SU. «Момент звільнення каналу PU» означає момент, коли РЕЗ PU завершує свою роботу на каналі.

Список використаних джерел:

1. Кирик М.І. Модель оцінки ефективності методів спектральної мобільності для когнітивних радіомереж. Львів, 2016 - 202 с.

2. Сабурова С.О., Коляденко Ю.Ю, Холод Л.М. Метрологічне забезпечення в телекомунікаційних системах та мережах: навч. посібник для студентів ВНЗ. Харків :СМІТ, 2017. – 172 с.

УДК 621.391

# ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ ПАРАМЕТРАМИ ЯКОСТІ ПОСЛУГ NB-IoT4G МЕРЕЖ

Сізов Я.А.
Науковий керівник – доц. 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: yaroslav.sizov@nure.ua.

The study of the quality parameters of 4G and 5G mobile communication networks, as well as the analysis of big data (BigData) and the Internet of Things (Narrow Band- IoT, NB-IoT and Broad Band-IoT, BB-IoT), which are designed to become one of the foundations of the digital economy, the main driving force prospects for the development of artificial intelligence. A scheme of a schematic management solution, variants of web applications in terms of interaction at the client-server level and a histogram of management of cloud platform services for the NB-IoT4G network have been developed.

Системи управління відіграють важливу роль у запобіганні мережних катастроф та збереженні якості функціонування об’єктів, елементів фіксованих та мобільних мереж. Можливість системи управління в забезпеченні високої надійності та загальної бездоганної інтеграції з NB-IoT 4G та BB-IoT 5G мережами призводить до розробки и впровадженню ефективних форм контролю та онлайн моніторингу за параметрами якості послуг, які надаються споживачам та суспільству згідно вимог системи QoS (Quality of Service) [1].

NB-IoT 4G-мережі можна розглядати в якості глобальної мережної інфраструктури, що складається з безлічі підключених пристроїв, які використовують сенсорні, комунікаційні, мережні та інформаційні технології.

На основі системи управління мережними елементами, яка забезпечує end-to-end вимоги до трафіку передачі і прийому інформації, реалізується ефективна підтримка послуг і додатків в NB-IoT 4G мережах.

Концепція IoT-мереж базується на схемі схематичного рішення управління, варіантів веб-додатків в умовах взаємодії на рівні клієнт-сервер та гістограми управління послугами cloud платформ.

Веб-речі (WEBofThings, WoT), які забезпечують взаємодію, управління та контроль різних інтелектуальних об'єктів («речей») з використанням стандартів і механізмів Інтернет мережі є складовою частиною IoT: URI (UniformResourceIdentifier), уніфікований ідентифікатор ресурсу; HTTP (Hyper Text Transfer Protocol), протокол передачі гіпертексту; REST (Representational State Transfer), стиль побудови архітектури розподіленого застосунка та ін.

На прикладному рівні з використанням вже існуючого архітектурного рішення, орієнтованого на розробку web-застосування, WoT передбачає реалізацію Концепції IoT. Управління та контроль за web-додатками мають бути доступні черезWWW-сторінки, як дані з розумних речей. Наприклад, використовуючи спеціальну сторінку в Інтернеті через браузер, можна управляти та контролювати рахування даних з датчика світла у в NB-IoT4G-мережі або зміну коліру четвертого індикатора в сенсорі, як показано на схемі варіантів (рис.1).

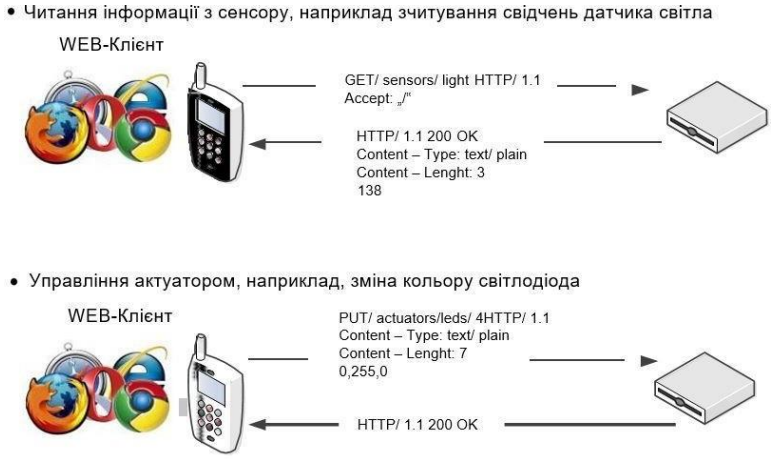



Рисунок 1 – Схема варіантів управління послугами та веб-взаємодії в NB-IoT4G-мережі

Висновки:

1. Особливості WoT не в якості транспортного механізму передачі даних, як він застосовується за протоколом HTTP для традиційних WWW-послуг, а як інструмент управління послугами в реальному часі.

2. WoT забезпечує синхронну роботу інтелектуальних (смарт) об'єктів через прикладний програмний інтерфейс – REST (RESTful API) і в цілому відповідає ресурсно-орієнтованій архітектурі – ROA (Resource - Oriented Architecture).

3. З використанням значною мірою стандартних Web- технологій, таких як Atom, що містить формат для опису ресурсів на веб-сайтах і протокол для їх публікації, WoT надає асинхронний режим роботи інтелектуальних об'єктів, або Web-механізмів передачі даних, таких як модель роботи веб-застосування Comet, при якій постійне HTTP – з'єднання дозволяє без додаткового запиту зі сторони браузера веб-серверу відправляти дані браузеру.

Список використаних джерел:

1. Радченко В.В., Сабурова С.А., Дослідження методів забезпечення параметрів якості послуг IoT 5G//24-й// Міжнародний молодіжний форум «Радіоелектроніка та молодь в XXI столітті. сб. Матеріалів форуму – Харків, ХНУРЕ, 2020р. – С. 34-35.

УДК 004:621.391]:658.7

# ЛОГІСТИКА В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ

Бондаренко В.С.
Науковий керівник – д.т.н. Шостко І.С.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-55-92)
E– mail: vadym.bondarenko@nure.ua

Logistics in infocommunication systems is a complex and critical aspect of modern business operations. As the world becomes increasingly connected and digitized, the management of logistics in the infocommunication industry is becoming more challenging. With so many factors at play, including supply chain management, inventory control, shipping and delivery, and customer service, businesses operating in the infocommunication industry must be strategic and efficient in their logistics management to remain competitive. Artificial intelligence (AI) can help automate routine tasks in logistics, improving efficiency and reducing errors.

Однією з найбільших проблем в управлінні логістикою в інфокомунікаційних системах є складність ланцюга поставок. З такою кількістю постачальників, які беруть участь у виробництві та розповсюдженні продукції, може бути важко підтримувати контроль над запасами та забезпечувати своєчасну доставку. Щоб вирішити цю проблему, компанії повинні прийняти стратегічний підхід до управління ланцюгом поставок, включаючи оптимізацію кількості постачальників, покращення зв’язку та співпраці з постачальниками, а також використання сучасних технологій для відстеження запасів і поставок.

Ще одна сфера, де можна покращити управління логістикою в інфокомунікаційних системах, це контроль запасів. Управління товарними запасами може бути складним, оскільки впливають такі фактори, як коливання попиту, життєвий цикл продукту та відносини з постачальниками. Спрощуючи управління запасами за допомогою централізованого контролю запасів, підприємства можуть зменшити витрати та підвищити ефективність. Цього можна досягти за допомогою технології відстеження рівня запасів у режимі реального часу, оптимізації процесу замовлення та оптимізації розташування запасів для зменшення витрат на доставку та зберігання.

Відвантаження та доставка також є критичними компонентами управління логістикою в інфокомунікаційних системах. Використовуючи технології для відстеження відправлень і оптимізації маршрутів доставки, компанії можуть скоротити час і витрати, пов’язані з доставкою. Це також може покращити задоволеність клієнтів, забезпечуючи швидші та надійніші варіанти доставки.

Щоб покращити управління логістикою в інфокомунікаційних системах пропонується задіяти вже добре відомий штучний інтелект (Artificial intelligence (AI)). AI може допомогти автоматизувати рутинні завдання, такі як аналіз даних, маршрутизація та планування, звільняючи людські ресурси для зосередження на більш складних завданнях. Наприклад, алгоритми AI можна використовувати для прогнозування мережевого трафіку та оптимізації маршрутизації, зменшуючи затримку та покращуючи час відповіді. AI також може допомогти виявити аномалії та потенційні проблеми, перш ніж вони стануть серйозними проблемами, забезпечуючи проактивне обслуговування та покращуючи надійність логістикі в інфокомунікаційних системах. Ще однією перевагою використання AI в інфокомунікаційних системах є зменшення кількості помилок. Завдання ручної логістики схильні до людських помилок, таких як помилки при введенні даних, які можуть мати серйозні наслідки. Штучний інтелект можна використовувати для перевірки даних, гарантуючи, що вони відповідають певним критеріям перед введенням у систему. Це допоможе зменшити ймовірність помилок і покращити якість даних.

Впровадження AI в інфокомунікаційних системах вимагає ретельного планування та розгляду. Головною проблемою у впровадженні штучного інтелекту залишається розмір бази даних, на яких навчався AI. Інфокомунікаційні системи постійно розвиваються, змінюються технології та обладнання. Моделі штучного інтелекту потребують великих наборів даних для навчання, а дані мають бути точними та відповідати поточному стану інфокомунікаційної системи. Іншою проблемою є складність самих систем (кількість нейронів, які взаємодіють між собою). Інформаційні системи можуть бути дуже складними [1], з багатьма взаємопов’язаними компонентами, що ускладнює розробку моделей AI, які можуть ефективно керувати всіма аспектами логістики.

Незважаючи на ці проблеми, переваги використання AI в управлінні логістикою роблять його привабливим варіантом для підприємств і організацій будь-якого розміру. Тому в доповіді пропонується метод для систематизації збору даних щодо поточного стану інфокомунікаційної системи для навчання AI, що допоможе прискорити впровадження AI для управління логістикою в інфокомунікаційних системах.

Список використаних джерел:

1. The method of controlling the wireless sensor network of optical-electronic stations using LoRa technology, Shostko I., Shloma O., Tsybulnykov D. // IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2022. P. 1 - 6. Scopus.

УДК 621.391:004.383.3

# ФІЗИЧНІ ОСНОВИ ОБРОБКИ ТА ФІЛЬТРАЦІЇ СИГНАЛІВ

Котенко К.О.
Науковий керівник – Приймачов Ю.Д.
Харківський національний університет радіоелектроніки, каф. фізики
м. Харків, Україна
тел. +38(050) 883-84-98, e-mail: kyrylo.kotenko@nure.ua.

Signal processing and filtering techniques are essential components of radio electronics and instrumentation systems. Signal processing involves the manipulation of signals to extract useful information or improve their quality, while filtering is used to remove unwanted noise from signals and improve their quality. Sampling, quantization, and digital signal processing are the basic principles of signal processing. Frequency domain analysis, transfer functions, and filter design are the basic principles of filtering. Signal processing and filtering techniques are used in various applications, including wireless communication systems, audio and video processing, medical imaging systems, and control systems.

Методи обробки та фільтрації сигналів є важливими компонентами радіоелектроніки та приладобудування. Вони використовуються для вилучення корисної інформації з сигналів, видалення небажаних шумів і покращення співвідношення сигнал/шум. У цій роботі ми обговоримо принципи обробки та фільтрації сигналів, їх застосування та різні типи методів обробки та фільтрації сигналів.

Обробка сигналів передбачає маніпуляції з сигналами для вилучення корисної інформації або покращення їхньої якості. Основні принципи обробки сигналів включають дискретизацію, квантування та цифрову обробку сигналів. Дискретизація – це процес перетворення сигналу безперервного часу в сигнал дискретного часу шляхом вимірювання сигналу через регулярні проміжки часу. Квантування – це процес перетворення неперервного амплітудного сигналу в дискретний шляхом присвоєння кожному відліку найближчого рівня квантування. Цифрова обробка сигналів передбачає маніпуляції з цифровими сигналами за допомогою алгоритмів для вилучення корисної інформації або покращення їхньої якості.

Фільтри використовуються для видалення небажаного шуму з сигналів та покращення їх якості. Основні принципи фільтрації включають аналіз частотної області, передатні функції та проектування фільтрів. Частотний аналіз передбачає представлення сигналів у частотній області за допомогою аналізу Фур'є. Передавальні функції використовуються для опису зв'язку між вхідним і вихідним сигналами фільтра. Проектування фільтрів передбачає вибір відповідного типу фільтра і оптимізацію його параметрів для досягнення бажаних характеристик.

Методи обробки та фільтрації сигналів використовуються в широкому спектрі застосувань, включаючи системи бездротового зв'язку, обробку аудіо та відео, системи медичної візуалізації та системи управління. У системах бездротового зв'язку методи обробки і фільтрації сигналів використовуються для вилучення корисної інформації з сигналів і усунення перешкод. В обробці аудіо- та відеосигналів ці методи використовуються для покращення якості сигналу та видалення шумів. У системах медичної візуалізації методи обробки та фільтрації сигналів використовуються для покращення якості зображень та зменшення шуму. У системах керування ці методи використовуються для фільтрації небажаних сигналів і підвищення продуктивності системи.

Існує кілька типів методів обробки та фільтрації сигналів, включаючи аналогову та цифрову фільтрацію, фільтрацію в часовій та частотній області, а також адаптивну фільтрацію. Аналогові фільтри розроблені з використанням пасивних компонентів, таких як резистори, конденсатори та котушки індуктивності. Цифрові фільтри розроблені з використанням алгоритмів цифрової обробки сигналів. Часові фільтри працюють з представленням сигналу в часовій області, тоді як частотні фільтри працюють з представленням сигналу в частотній області. Адаптивні фільтри призначені для підстроювання своїх параметрів на основі характеристик вхідного сигналу.

Отже, методи обробки та фільтрації сигналів відіграють життєво важливу роль у роботі радіоелектроніки та контрольно-вимірювальних систем. Використовуючи ці методи, інженери та науковці можуть витягувати корисну інформацію з сигналів, видаляти небажані шуми та покращувати якість сигналу. Різні типи обробки та фільтрації сигналів надають інженерам та науковцям широкий спектр можливостей для оптимізації роботи їхніх систем. З розвитком технологій методи обробки та фільтрації сигналів ставатимуть все більш важливими у проектуванні та розробці радіоелектроніки та контрольно-вимірювальних систем.

Список використаних джерел:

1. Мітра, С. К. (2004). *Цифрова обробка сигналів: Комп'ютерний підхід*. McGraw-Hill.
2. Оппенгейм, А. В., & Шафер, Р. В. (1999). *Обробка сигналів у дискретному часі*. Prentice Hall.
3. Проакіс, Дж. Г., & Манолакіс, Д. Г. (2006). *Цифрова обробка сигналів: Принципи, алгоритми та застосування*. Pearson Prentice Hall.
4. Хеммінг, Р. В. (1983). *Цифрові фільтри*. Prentice-Hall.
5. Чен, В.-К. (2005). *Довідник з електротехніки*. CRC Press.

УДК 621.396:[004.738.5:004.722]

# ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ FRONTHAUL У ЦЕНТРАЛІЗОВАНІЙ АРХІТЕКТУРІ МОБІЛЬНОЇ МЕРЕЖІ

Акіменко А.С., Ворончихін О.А.
Науковий керівник – к.т.н., доц. Токар Л.О.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
тел. +38(063)8655002, +38(093)3614948, e-mail: andrii.akimenko@nure.ua, oleksii.voronchykhin@nure.ua

An analysis of the concept of centralized baseband processing in the LTE mobile network has been carried out. It was found that when using a centralized scenario, maintenance and modernization are simplified. This concept requires an expensive FH network, but with lower requirements. This is related to the distribution and processing of signals of the physical layer in the mobile network BS. Options for solving the FH problem are considered, taking into account the centralization of RAN functions.

Альтернативою концепції децентралізованої архітектури мобільних мереж LTE (Long Term Evolution) є централізація функцій мережі радіодоступу RAN (Radio Access Network). Такий варіант побудови мережі передбачає використання архітектури централізованої RAN або хмарної – C-RAN (Cloud Radio Access Network). При цьому забезпечується скорочення функціональності BS до віддалених головних радіостанцій RRH (Remote Radio Head), які виконують лише аналогову обробку та пересилають цифрові дані між RRH та BBU (Battery Backup Unit).

Відомо, що ранні розгортання C-RAN побудовано на централізованих модулях основної лінії частот BBU, які складаються зі спеціалізованого обладнання. Централізована архітектура вже використовується в деяких мережах 4G та активно розглядається для майбутніх мобільних мереж.

Переваги централізованої архітектури полягають у наступному: зниження експлуатаційних та капітальних витрат; централізація BBU значно полегшує реалізацію способів спільної обробки; досягнення в галузі процесорних технологій та віртуалізації дозволили реалізувати обробку основної смуги частот на процесорах загального призначення GPP (Green Power Processor). Однак, такий підхід спричиняє організацію більш вимогливої та дорогої транспортної мережі FH (fronthaul).

На рис. 1 показано архітектуру централізованої мобільної мережі та стеки протоколів [1]. У централізованій архітектурі мобільної мережі вся обробка основної смуги частот відбувається лише на рівні PHY і MAC, а конвергенція пакетних даних PDCP (Packet Data Convergence Protocol) виконується не так на BS, а в хмарному центрі обробки, підключеному до ядра через BH (backhaul).

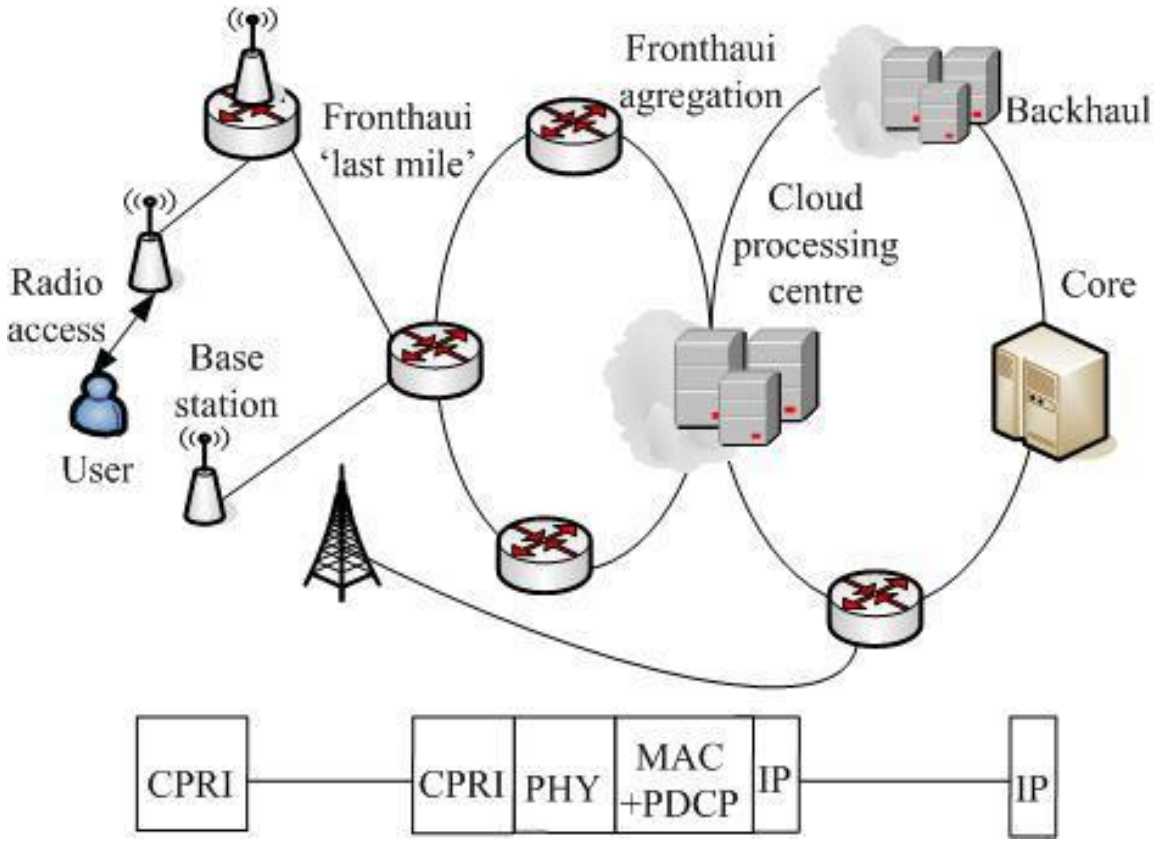



Рисунок 1 - Архітектура і стек протоколів централізованого сценарію мобільної мережі

Чим централізованіше обробка, тим простіше реалізувати спільну обробку. При цьому вище потенційна економія витрат та простіше обслуговування та модернізація. Однак, такий підхід компенсується вимогливою та дорогою мережею FH. Централізований сценарій відповідає розподілу, який використовується в C-RAN. Інтерфейс FH стандартизований у CPRI. У DL вся обробка основної лінії частот проводиться централізовано, а цифрові дані пересилаються на BS. В UL отримані сигнали лише оцифровуються, фільтруються і потім пересилаються.

Централізований варіант розподілу відзначає межу між аналоговими та цифровими сигналами. Таким чином, дані обмінюються за допомогою FH та відповідають оцифрованому набору вибірок комплексного сигналу I/Q.

Список використаних джерел:

1. Токар, Л.О., & Сучков, О.В. (2022). Аналіз транспортного сегменту мобільної мережі LTE. IV International Scientific and Theoretical Conference «SCIENTIA», November 11, Vilnius, Republic of Lithuania, 105-110. http://doi 10.36074/scientia-11.11.2022.

УДК 004:621.391

# ОСОБЛИВОСТІ ВИКОРИСТАННЯ СТЕКУ ПРОГРАМ ELASTIC STACK В ОБОЛОНЦІ UNIX-ПОДІБНОЇ СИСТЕМИ

Муха Р.В.
Науковий керівник – к.т.н., доц. Токар Л.О.
Харківський національний університет радіоелектроніки,
кафедра ІКІ ім В.В. Поповського,
м. Харків, Україна
тел. +38(099) 556-76-02, e-mail: rostyslav.mukha@nure.ua

The problems when working with logs were analyzed, the main points that hinder the quality analysis of log files were identified. General provisions on the open source product - the Elastic Stack (ELK) program stack, which is proposed to be used for transparent analysis of log files in real time, are provided. The purpose and method of using ELK when working with Unix-like systems are given. The possibilities and features of using rsyslog in combination with ELK to improve data monitoring and analysis have been revealed.

Адміністраторам різних сфер діяльності необхідно переглядати лог-файли. Це може стосуватися різних галузей, таких як інформаційна безпека, IT-інфраструктура, розробка програмного забезпечення, аналіз трафіку та веб-аналітика, фінансова аналітика, медицина, енергетика, телекомунікації, IoT, автоматизоване виробництво. Перегляд лог-файлів дозволить вирішити проблеми виявлення помилок, захищення від зловмисної активності та збір статистики відвідувань й аналізу подій. Для досягнення максимальної гнучкості та ефективності в роботі використано стек програм Elastic Stack на Unix-подібній системі.

Аналіз лог-файлів у інфокомунікаціях створює ряд проблем, що ускладнюється через велику кількість різноманітних журналів. У кожного додатку різні формати, що робить процес читання лог-файлу досить складним, незручним, монотонним заняттям. Відсутність централізованого збірника інформації призводить до виникнення проблеми знаходження місця зберігання лог-файлів, необхідного застосунку, а також визначення формату. Крім того, слід відмітити, що для кожного окремого застосунку існують різні програми для обробки лог-файлів.

Це й робить використання комплексного інструменту – стеку програм ELK (Elasticsearch, Logstash, Kibana) доцільним.

Використання Elastic Stack дозволить не тільки подолати вказані проблеми, а ще й принести додаткову користь, що полягає в використанні єдиного додатку для всіх лог-файлів, любого текстового формату та можливості зберігання в єдиному місці – сховищі лог-файлів. Крім того, можливість розробити свої аналізатори дозволить прискорити роботу в пошуках в декілька разів. Візуалізація дозволить значно спростити аналіз даних. Інформацію можна представляти наглядно у формі графіків,

кругових та стовпчикових діаграм. Веб-додатки надають можливість виконувати різноманітні дії з любого пристрою, на любій операційній системі. Оскільки стек ELK є open source програмним забезпеченням, то це є важливою перевагою для перегляду, використання та модифікацій тощо.

Стек програм Elastic Stack встановлюється на різних операційних системах (Windows, MacOS, Linux), що вимагає деяких попередніх налаштувань, наприклад, встановлення віртуальної машини Java. Однак, ELK Stack першочергово розроблено для роботи з Unix-подібними операційними системами, таким чином встановлення його на Ubuntu може бути більш природнім та оптимальним.

Для покращення моніторингу та аналізу даних в роботі запропоновано використати інструмент збору логів даних rsyslog. Він стандартно встановлюється на дистрибутивах Linux і може збирати дані з різних джерел та пересилати їх на централізований сервер логування. В поєднанні з Elastic Stack rsyslog може збирати дані та передавати їх у форматі JSON, необхідному для Elasticsearch. При цьому налаштовується сервер для використання шаблону JSON та створення нового конфігураційного файлу на rsyslog-server, який буде форматувати лог-файли в JSON перед їх передачею до інструментів Logstash та Elasticsearch.

Архітектуру Elastic Stack для Unix-подібних систем наведено на рис. 1.

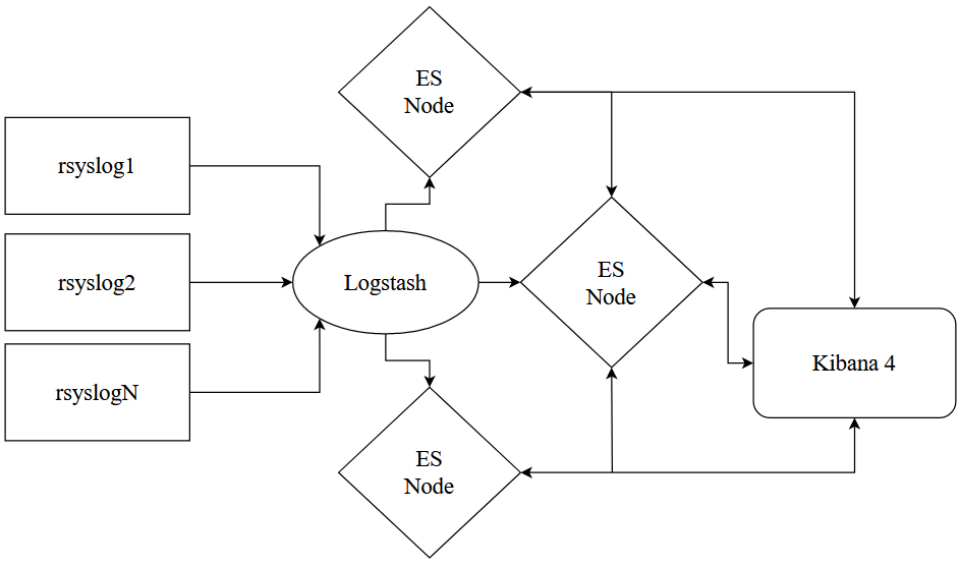



Рисунок 1 – Архітектура Elastic Stack для Unix-подібних систем

Текстові дані у вигляді лог-файлу надходять до програми-сервісу rsyslog, в свою чергу rsyslog надсилають дані в програму Logstash, яка може фільтрувати вхідні дані й розподіляти їх по іншим вузлам, де встановлено Elasticsearch. Після цього отримані результати можна переглянути за допомогою графічного інтерфейсу програми Kibana.

УДК 621.396.946:[004.738.5:004.722]

# ОСОБЛИВІСТЬ ПРОТОКОЛУ B.A.T.M.A.N ДЛЯ ОРГАНІЗАЦІЇ WI-FI MESH МЕРЕЖ

Ворончихін О.А., Акіменко А.С.
Науковий керівник –к.т.н., доц. Токар Л.О.
Харківський національний університет радіоелектроніки, кафедра ІКІ ім В.В. Поповського,
м. Харків, Україна
Тел. +38(093) 361-49-48, e-mail: oleksii.voronchykhin@nure.ua;
Тел. +380638655002, e-mail: andrii.akimenko@nure.ua

The advantages of the wireless Mesh network compared to other networks are shown. The features of the 802.11s standard for the organization of a Mesh network are analyzed. An overview of the features of using the B.A.T.M.A.N protocol, which is divided into protocols of the second and third routing levels, was conducted. The main parameters on which the B.A.T.M.A.N protocol is based and the principle of its action are considered.

Безпроводова мережа Wireless Mesh Network утворюється на основі безлічі з'єднань вузлів «точка-точка», що знаходяться в зоні радіопокриття один одного. Ключова властивість самоорганізації сітчастих мереж полягає у наступному: з'єднання між вузлами встановлюються автоматично; будь-який вузол може виконувати функції транзитної передачі пакетів маршрутизації інших учасників мережі [1].

Мережа на основі сітчастої топології характеризується високою надійністю, великою пропускною здатністю та зниженим енергоспоживанням. Висока надійність забезпечується надмірністю вузлів. При відмові одного вузла дані будуть передаватися в обхід, іншим шляхом. Використання кількох альтернативних маршрутів підвищує пропускну спроможність мережі. Зниження енергоспоживання досягається зниженням потужності сигналів за допомогою передачі даних через більше вузлів, розділених меншими відстанями.

В концепції Mesh мереж слід виділити стандарт IEEE 802.11s, який дозволяє повністю децентралізувати архітектуру мережі та збільшити зону дії. Стандарт IEEE 802.11s забезпечує автоматичну маршрутизацію між вузлами мережі Wi-Fi, в якій кожен вузол для передачі інформації здатний задіяти сусідні, використовуючи стрибковий механізм перерозподілу трафіку і більше 5% пропускної спроможності каналу [2]. Стандарт IEEE 802.11s регламентує протоколи виявлення, ідентифікації та з'єднання між сусідніми пристроями. Сукупність пристроїв, що працюють у мережі стандарту IEEE 802.11s, утворює Mesh-мережу.

Особливістю архітектури Mesh є використання спеціальних протоколів, які дозволяють кожній точці доступу створювати таблиці абонентів мережі з контролем стану транспортного каналу та підтримкою

динамічної маршрутизації трафіку за оптимальним маршрутом між сусідніми точками. На даний час найпопулярнішім для організації Wi-Fi Mesh мереж є протокол B.A.T.M.A.N.

B.A.T.M.A.N. - це протокол проактивної маршрутизації, який використовує дистанційно-векторний підхід і метрику маршрутизації. B.A.T.M.A.N не підтримує таблиці з повними маршрутами до пункту призначення, натомість кожен вузол уздовж маршруту зберігає лише інформацію про наступне посилання, через яке вузол може знайти найкращий маршрут [3]. При цьому максимізується ймовірність доставки повідомлення. B.A.T.M.A.N перевіряє не якість кожного посилання, а його існування. Протокол робить ці перевірки періодично шляхом надсилання пакетів привітання, які відомі як вихідні повідомлення (OGM). Структуру пакета OGM представлено на рис.1[3].

<table>
<tr><td>Версія</td><td>Заголовок</td><td>Час життя</td><td>Порт шлюзу</td></tr>
<tr><td colspan="2">Порядковий номер</td><td colspan="2">Заголовок шлюзу</td></tr>
<tr><td colspan="4">Адреса відправника</td></tr>
<tr><td colspan="4">Попередній відправник</td></tr>
</table>

Рисунок 1 - Формат пакету OGM

У протоколі B.A.T.M.A.N відсутнє поширення топологічних повідомлень. Кожен вузол виконує наступні операції: надсилання періодичних рекламних повідомлень, званих OriGinator Message (OGM). Розмір цих повідомлень складає всього 52 байти, що містять: IP-адресу відправника, IP-адресу вузла пересилки, значення часу життя (TTL) і порядковий номер (SQ); перевірку кращого однокрокового сусіда для кожного (відомого) пункту призначення в мережі за допомогою ранжування; ретрансляцію OGM, отриманого через найкращого односкачкового сусіда.

Список використаних джерел:

1. Guido, R. Hiertz et al. (2010). IEEE 802.11s: the Wlan mesh standard. IEEE Wireless Communications, 104-111. http:// doi:10.1109/MWC.2010.5416357.

2. Експериментальна оцінка протоколів маршрутизації B.A.T.M.A.N і B.A.T.M.A.N-Adv (2018). https://ieeexplore.ieee.org/document/8650222.

3. Seither, D., Knig, A., & Hollick, M. (2011). Routing Performance of Wireless Mesh Networks: A Practical Evaluation of B.A.T.M.A.N-Advanced, IEEE 36th Conference on Local Computer Networks, 897–904. https://doi:10.1109/LCN.2011.6115569.

УДК 681.7:004.7]:614.2

# ПРОЄКТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ ПІДЗЕМНОЇ ЛІКАРНІ

Усов О.О.
Науковий керівник – ас. Штих І.А.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. «Інформаційно-мережної інженерії»,
тел. (057) 702-14-29)
тел. +38(050) 400-55-56, email: oleksandr.usov@nure.ua.

This work is devoted to the construction of a local network of underground critical infrastructure, namely, the construction of a local network of an underground hospital is considered. The main principles of the underground type of network construction are considered. An analysis of the complex conditions in which this network will have to be built and the most effective options for equipment and location of vulnerable network objects has been carried out. The relevance of this building for the city of Kharkiv is also considered. It has been established that under such conditions, such a wired connection of the entire network is the most efficient and will be able to quickly process all available information.

Зважаючи на ситуацію, яка складається останній рік у країні, та саме у Харкові, є необхідність яка полягає у створенні ефективної медичної інфраструктури з ключових складових є забезпечення надійного та безперебійного зв’язку у медичних закладах. У цьому контексті підземні дротові локальні мережі лікарень може стати незамінним рішенням, особливо в умовах збільшення кількості витрат та потреби в оперативному обміні медичною інформацією.

Підземні дротові локальні мережі лікарень забезпечують високу швидкість передачі даних, максимальну стійкість до зовнішніх впливів, надійність та безпеку обміну інформацією, що є особливо випадком екстрених ситуацій, коли критично важливо швидко та ефективно реагувати на зміни.

Підземні дротові локальні мережі лікарень мають і свої недоліки, зокрема високу вартість інсталяції та підтримки, потребу в спеціально обладнаному та кваліфікованому персоналі.

В цілому, побудова локальних підземних мереж критичних об'єктів на базі дротового підключення є складним завданням, але це необхідне забезпечення ефективної роботи медичних установ. Якісне проектування мережі, використання захищених кабелів та розміщення серверів в окремих приміщеннях допоможуть забезпечити стабільну та надійну роботу мережі.

Основу підземної локальної мережі складають сервер та комутатори. Сервер є центральним вузлом мережі, на якому зберігаються та обробляються дані. Комутатори виконують функцію передачі даних між

комп'ютерами мережі. Для забезпечення швидкої та ефективної роботи мережі необхідно вибрати правильний сервер та комутатори [1].

Для побудови такої локальної мережі можна використовувати кабель категорії 6 або вище, який забезпечує високу швидкість передачі даних. Для зменшення загасання сигналу необхідно використовувати короткі кабелі завдовжки не більше 100 метрів. Комутатори повинні підтримувати швидкість передачі не менше 1 Гбіт/с.

Важливим аспектом при побудові є правильне налаштування мережного обладнання. Необхідно визначити правильні налаштування IP-адрес, підмереж та шлюзів за промовчанням для серверів, комутаторів та комп'ютерів у мережі [1]. Це дозволить забезпечити правильну маршрутизацію даних та запобігти конфліктам IP-адрес.

Схема для локальної мережі підземної лікарні представлена на рис. 1. Дана схема розроблена з урахуванням характерних особливостей побудови. Кабелі будуть розташовані уздовж стіни, в спеціально відведених для них каналах.

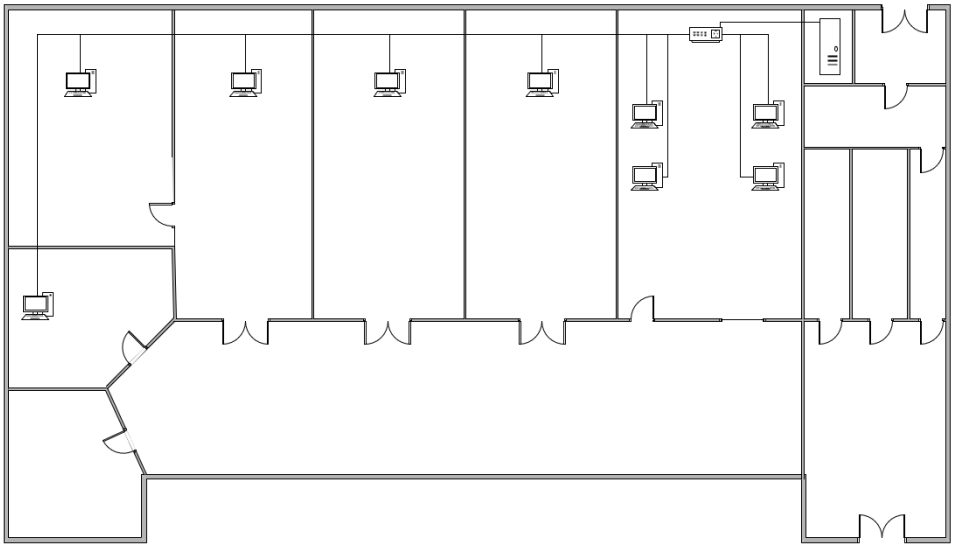


Рисунок 1 – Схема підземної лікарні та приклад розташування обладнання для ефективної роботи в складних умовах

У результаті побудова дротової локальної мережі такого типу у підземній лікарні є надійним та ефективним рішенням для забезпечення своєчасної та якісної обробки даних.

Список використаних джерел:

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010. – 944 с. – ISBN 978-5-49807-389-7.

УДК 004.738.5:004.722

# ВАЖЛИВІСТЬ ЗАСТОСУВАННЯ ХМАРНИХ ОБЧИСЛЕНЬ В IT ІНФРАСТРУКТУРІ

Геворк`ян Л.А.
Науковий керівник – ас. Холєв В.О.
Харківський національний університет радіоелектроніки, каф. ЕОМ
м. Харків, Україна
тел. +38(050) 604-72-68, e mail: luiza.hevorkian@nure.ua

Cloud computing is one of the most important technologies in the modern world, as it allows efficient use of computing resources and storage of data in the Internet cloud. This technology uses Internet infrastructure to communicate between the client and the server side service applications. Apart from this, cloud computing has cloud service providers that offer cloud platforms for their customers to create and use web oriented services. This technology is becoming increasingly common on a large scale of industries.

Хмарні обчислення є однією з найважливіших технологій в сучасному світі, оскільки вони дозволяють ефективно використовувати обчислювальні ресурси та зберігати дані в інтернет-хмарі. Ця технологія забезпечує доступ до ресурсів, що дозволяє їх ефективне використання у різних сферах діяльності. Хмарна модель обчислень складається з п'яти основних характеристик, а саме: самообслуговування, широкий доступ до мережі, незалежне об'єднання ресурсів, швидка еластичність та вимірювальний сервіс. Одна з областей, де застосовуються хмарні обчислення, які переживають активний ріст та розвиток, є штучний інтелект (AI), тобто комп'ютерні системи, здатні виконувати завдання, які зазвичай потребують людського інтелекту. AI може бути дуже ресурсоємним і вимагати великих обчислювальних потужностей. Хмарні обчислення дозволяють використовувати обчислювальні ресурси великих масштабів для розв'язання складних задач в галузі машинного навчання та глибинного навчання. Це дозволяє розробляти більш ефективні моделі нейронних мереж та зменшувати час, необхідний для їх навчання. Також важливим є використання таких обчислень в глибинному навчанні для тренування моделей. Такі обчислення можуть забезпечити розподіл обчислювального навантаження між різними комп'ютерами, що дозволяє прискорити обробку даних та зменшити час тренування моделей. Задачі на обчисленні можуть бути різноматнітними, наприклад, класифікація даних, регресійний аналіз, кластеризація тощо. Використання хмарних обчислень дозволяє значно прискорити цей процес навчання мережі. Найпоширеніші хмарні платформи, які використовуються в глибинному навчанні, це Amazon Web Services, Microsoft Azure та Google Cloud Platform. Такі обчислення виконуються на серверах, комп'ютерах, IoT пристроях, блокчейн платформах та на суперкомп`ютерах.

Модель хмарних обчислень - це архітектурна модель, яка описує різні рівні та компоненти хмарних обчислень. Вона включає в себе технології, протоколи та інструменти для розробки, розгортання та управління хмарними сервісами. Зазвичай моделі представляють собою послугу для зберігання даних, розгортання, доступу та управління. Отже, хмарні обчислення можуть бути використані в різних сферах, насамперед в корпораціях, пов`язаних з інформаційними технологіями, а також в інших сферах де так чи інакше потрібно втручання обчислення на цифрових пристроях з Інтернетом, а саме:

- Зберігання та обробка даних: хмарні сервіси, такі як Google Drive або Dropbox. Наприклад, це отримання доступ до своїх даних Google-пошти на будь-яких пристроях.
- Веб-розробка: хмарні сервіси надають різноманітні ресурси для веб-розробки, такі як віртуальні сервери, бази даних, мережеві сервіси та інші.
- Інтернет-речей (IoT), оскільки ця сфера включає в себе велику кількість підключених до Інтернету пристроїв, від медичних пристроїв та промислового обладнання до домашніх розумних пристроїв, які збирають та обробляють величезні обсяги даних.
- Онлайн-ігри: хмарні сервіси, такі як Google Cloud Platform або Amazon Web Services, можуть бути використані для масштабування гри, віртуалізація серверів, реалізації онлайн-магазину тощо.
- А також обробка медичних даних, аналіз фінансових даних та для забезпечення безпеки даних клієнтів. Віртуальна робоча станція є також прикладом обчислень через хмару, бо вона замінює традиційний комп'ютер, тому що все необхідне для роботи софт та файли зберігаються на віддаленому сервері.

Як і будь-яка технологія, хмарні обчислення мають свої недоліки, такі як залежність від Інтернету, ризик втрати даних, залежність від постачальника послуг. Отже, досліджувана технологія може більше піддаватися вторгненням в порівнянні з локальними обчисленнями, оскільки вона залежить від мережі Інтернет.

Список використаних джерел :

1.Vijayarani Mohan, Sharmila Sathyanathan (2015). Research in Cloud Computing-An Overview, International Journal of Distributed and Cloud Computing. 3. https://doi.org/10.21863/ijdcc/2015.3.1.002.

2. Lizhe Wang, Gregor von Laszewski, Andrew J. Younge (2010). Cloud Computing: a Perspective Study, New Generation Comput. 28, 137-146, https://doi.org/10.1007/s00354-008-0081-5.

УДК 621.396.946

# МОБІЛЬНІ ІНФОКОМУНІКАЦІЙНІ СИСТЕМИ ТА БЕЗПРОВОДОВІ ТЕХНОЛОГІЇ 4G та 5G

Євсюкова О.О.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківський національний університет радіоелектроніки
каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
тел. +380 98 853 34 57 e-mail: olena.ievsiukova@nure.ua

Mobile information and communication systems are a set of technologies that enable data transfer and communication between mobile devices and the Internet. 4G and 5G wireless technologies are the latest advances in mobile communications, providing faster and more reliable data transfer than previous standards. The development of mobile information and communication systems and wireless technology is not only increasing the possibilities for mobile communications but is also having a positive impact in many areas of life.

Мобільні інфокомунікаційні системи є невід'ємним елементом сучасного світу, де люди постійно використовують мобільні пристрої для спілкування, роботи, розваг та інших цілей. Бездротові технології 4G і 5G є останніми досягненнями в галузі мобільного зв'язку та пропонують більш швидку і надійну передачу даних, ніж попередні стандарти.

Технологія 4G дозволяє досягти швидкості передачі до 100Мбіт/с. Це дозволяє миттєво завантажувати контент, мати більш швидке та стабільне з’єднання та підвищити ефективність вашого мобільного пристрою. Однак технологічні розробки не стоять на місці, і сьогодні 5G розглядається як новий етап розвитку мобільного зв’язку.

Нова мобільна мережа не була б новою, якби фундаментально не відрізнялася від існуючих. Одна з принципових відмінностей у тому, що 5G працює в іншому діапазоні радіочастот, щоб досягти цілей, з якими 4G не справляється. Радіоспектр розбитий на смуги, характеристики яких змінюються із зростанням частоти. 4G працює на частотах нижче 6 ГГц, у той час як 5G використовує вкрай високі частоти в діапазоні від 30 до 300 ГГц. Також до основних відмінностей між 4G та 5G відноситься швидкість, затримка при передачі даних, покриття, пропускна здатність.

Завдяки технології 5G відкриваються нові можливості для інтернету речей (IoT), збільшується пропускна спроможність мережі та зменшується затримка сигналу, що дозволяє використовувати різні нові технології, такі як доповнена та віртуальна реальність. 5G потенційно може бути у 100 разів швидше, ніж 4G, з максимальною теоретичною швидкістю близько 20 Гбіт/с та поточними реальними швидкостями від 50 Мбіт/с до 3 Гбіт/с. Існує три основні види 5G, і кожен з них має свою швидкість. Так званий низькосмуговий 5G трохи швидше, ніж 4G, з продуктивністю близько 50-

250 Мбіт/с. Найшвидша версія 5G, яка називається high-band 5G, - це версія, швидкість якої досягає 3 Гбіт/с.

Затримка – це міра часу, який потрібний пакету інформації, щоб пройти між двома точками. Затримку відчувають всі засоби передачі, незалежно від швидкості лінії. В даний час затримка в мережах 4G становить близько 50 мілісекунд, але очікується, що в мережах 5G вона знизиться до 1 мілісекунди. Наприклад, у самоврядних автомобілях 5G дозволить хмарному штучному інтелекту приймати навігаційні рішення у режимі реального часу.

Мережам 5G потрібно кілька років, щоб досягти рівня покриття, аналогічного покриттю мереж четвертого покоління. При цьому новий стандарт матиме різні рівні (високо-, середньо- та низькочастотний 5G), кожному з яких буде властива своя швидкість та смуга пропускання.

Зважаючи на ці відмінності в принципах роботи технології, стає ясно, що 5G-це майбутнє мобільних пристроїв зв'язку. 5G як домашня мережа дозволяє більшій кількості пристроїв одночасно підключатися до Інтернету без проблем з пропускною здатністю. У домашній мережі 5G смартфони, ігрові приставки, розумні двері, гарнітури віртуальної реальності, бездротові камери відеоспостереження, планшети та ноутбуки можуть одночасно підключатися до одного маршрутизатора.

У той час як 4G не може вмістити по постійно зростаючу кількість мобільних пристроїв, 5G відкриває шлях для технологій, орієнтованих на підключення, таких як «розумні» світлофори, бездротові датчики, пристрої, що носяться, і пристрої зв'язку між автомобілями.

Транспортні засоби, які отримують дані GPS та інструкції з навігації (наприклад, сповіщення про дорожній рух), вимагають дуже швидкого інтернет-з'єднання – нереалістично вважати, що 4G впорається з цими вимогами.

Оскільки швидкість передачі у 5G набагато вище, ніж у 4G, є ймовірність того, що для передачі даних не буде потрібно попереднього стиснення. Це дозволить ще швидше отримати доступ до інформації, адже тепер її не потрібно розпаковувати перед використанням.

Список використаних джерел:

1. Dave Johnson. (2020). 4G vs. 5G: The key differences between the cellular network. https://www.businessinsider.com/guides/tech/4g-vs-5g

2. habr.com. Почему и как 5G изменит все: технологии, поэтапное внедрение и элементная база для абонентского оборудования. https://habr.com/ru/post/490404/

3. habr.com В чем разница между 4G и 5G? https://habr.com/ru/post/439136/

УДК 621.396.94

# МЕТОДИ ЕФЕКТИВНОГО ТЕРИТОРІАЛЬНОГО ПЛАНУВАННЯ МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ 5G

Шумков І.М., Андрущенко О.В.
Науковий керівник – д.т.н., проф. Москалець М.В.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського, м. Харків, Україна
тел. +38(067) 849-66-93, e-mail: ivan.shumkov@nure.ua
тел. +38(099) 388-15-09, e-mail: oleh.andrushchenko@nure.ua.

The issues of territorial planning of the mobile communication network are being developed 5G based on the use of frequency cluster models in order to create an effective spatial plan with a high reuse rate of the frequency resource and a low percentage of non-compliance with the quality indicator of the level of mutual internal system interference.

Ефективне територіальне планування мереж мобільного зв'язку 5G – це процес розміщення базових станцій та іншого обладнання мережі для забезпечення покриття території, що забезпечує найкращу якість обслуговування для клієнтів.

Основними методами ефективного територіального планування мереж мобільного зв'язку 5G є:

Аналіз території: перш за все, необхідно провести детальний аналіз території, для того, щоб з'ясувати, які зони потребують особливого покриття. Такі зони можуть бути місцями підвищеної концентрації населення, великих промислових підприємств, а також туристичних та інших об'єктів.

Визначення типів мереж: розробник повинен визначити типи мереж, які будуть використовуватися в різних зонах. Наприклад, в зонах з великою концентрацією населення може бути доцільно встановлювати високопотужні базові станції, а в менш залізничних районах - менш потужні станції.

Планування маршрутів проводів: детальне планування маршрутів проводів є не менш важливим етапом. Оптимальні маршрути допоможуть скоротити витрати на будівництво і експлуатацію мережі.

Моделювання покриття: засоби моделювання дозволяють визначити зони покриття мережі та ефективність її роботи на різних відстанях. Вони дозволяють спрогнозувати, які зони можуть мати проблеми з покриттям, і розробити відповідні заходи.

Методи ефективного територіального планування мереж мобільного зв'язку 5G є важливим елементом розвитку мобільного зв'язку на сучасному етапі. Оскільки мережі 5G потребують більшої щільності станцій зв'язку та використання нових діапазонів частот, планування мереж стає складнішим та вимагає використання новітніх технологій та методів.

Один з основних методів територіального планування мереж 5G - це аналіз покриття зв'язку та його щільності на різних ділянках території. Для цього використовуються різноманітні математичні та геоінформаційні методи, що дозволяють моделювати розподіл мережевих ресурсів та щільність розташування станцій зв'язку на території. Такий аналіз дозволяє визначити найбільш оптимальне розташування станцій зв'язку та забезпечити максимальне покриття зв'язком при мінімальних витратах на будівництво та експлуатацію мережі.

Іншим методом є використання алгоритмів машинного навчання та штучного інтелекту для підвищення ефективності мережі та її планування. Застосування таких методів дозволяє розраховувати оптимальні параметри мережі, такі як щільність розташування станцій зв'язку, потужність передачі сигналу та швидкість передачі даних, на основі аналізу великих обсягів даних.

Також використовуються методи моделювання трафіку зв'язку на території, що дозволяють визначити найбільші точки зосередження користувачів та забезпезпечити їх відповідним рівнем обслуговування. Це дозволяє оптимізувати розташування станцій зв'язку та розподіл мережевих ресурсів на території.

Крім того, до методів ефективного територіального планування мереж 5G належить використання розумних антенних систем, що дозволяють максимально використовувати доступні ресурси мережі та забезпечити максимальне покриття зв'язком на території з мінімальними витратами на будівництво та експлуатацію мережі.

Список використаних джерел:

1. Андрущенко, О.В., Шумков, І.М., Москалець, М.В., (2022). Оцінка про-дуктивності алгоритмів адаптивного формування променю Smart-антени для систем мобільного зв’язку 5G. Матеріали восьмої Міжнародної науко-во-технічної конференції «Проблеми електромагнітної сумісності перспек-тивних безпроводових мереж зв’язку (ЕМС-2022)». 01-04.

https://openarchive.nure.ua/server/api/core/bitstreams/c85b3240-d1f3-4d67-bd4f-170ff7330afc/content

2. Шумков, І. М., Москалець, М. В., Андрущенко, О. В., (2022). Розробка ефективних моделей частотно-територіального планування мережі мобіль-ного зв’язку LTE. Матеріали восьмої Міжнародної науково-технічної кон-ференції «Проблеми електромагнітної сумісності перспективних безпрово-дових мереж зв’язку (ЕМС-2022)». 05-09. https://openarchive.nure.ua/server/api/core/bitstreams/cb3a40c2-b7b3-4137-a37b-f14b7ffa1ea3/content

УДК 621.396.49

# ПЕРСПЕКТИВИ ВИКОРИСТАННЯ SMART-АНТЕН В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ 5G

Андрущенко О.В., Шумков І.М.
Науковий керівник – д.т.н., проф. Москалець М.В.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського, м. Харків, Україна
тел. +38(099) 388-15-09, e-mail: oleh.andrushchenko@nure.ua.
тел. +38(067)849-66-93, ivan.shumkov@nure.ua.

This work is devoted to the assessment of the perspective of using Smart antennas in 5G networks. The advantages of using smart antennas are given. Technologies used in Smart-antennas are listed in the article. The synthesis of a Smart antenna in the form of a linear uniform antenna array is developed. The methods of adaptive formation of the directional pattern of the Smart antenna, namely the least mean squares (LMS) method and recursive least squares (RLS) algorithm, which are used to calculate the weight coefficients of the linear antenna array, are analyzed.

Поява мереж 5G відкриває нові можливості для передачі даних з великою швидкістю та забезпечення стабільного зв'язку в умовах високої щільності користувачів. Однією з ключових технологій, яка дозволяє досягнути цих цілей, є використання Smart-антен [1]. Smart-антени – це нове покоління антен, що забезпечують більш ефективний передачу сигналу в мережі 5G, за допомогою використання різних технологій формування променів та оптимізації напрямку передачі.

У 5G MIMO використовуються кілька типів Smart-антен, зокрема [2]:

1. Beamforming – це технологія, яка використовує smart-антени для передачі радіосигналу в певному напрямку, замість того, щоб передавати сигнал на всі боки. За допомогою налаштування фази та амплітуди сигналу на кожній антені, можна створити вузький промінь світла, який спрямований у потрібному напрямку.

Smart-антени, що використовуються для «beamforming», можуть бути як аналоговими, так і цифровими. Аналогові smart-антени можуть бути налаштовані на певну частоту і напрямок, але вони не можуть змінювати напрямок швидко, що обмежує їх застосування в динамічних умовах. Цифрові smart-антени, з іншого боку, можуть швидко змінювати напрямок сигналу, що робить їх більш гнучкими у використанні.

2. MMIMO (Massive MIMO) – це технологія, яка використовує велику кількість антен (зазвичай більше 64) на базовій станції для одночасного обслуговування набагато більшої кількості користувачів (часто сотень або навіть тисяч) [3]. Кожному користувачеві призначається унікальний вектор формування променя для оптимізації якості сигналу і зменшення завад. MMIMO призначений для підвищення спектральної ефективності, збільшення пропускної здатності мережі та покращення якості обслуговування.

3. MU-MIMO (Multi-User MIMO) – це технологія, яка використовує кілька антен на базовій станції для одночасного обслуговування декількох користувачів, зазвичай до чотирьох. Вона використовує просторове мультиплексування для передачі різних потоків даних кожному користувачеві в одній і тій же смузі частот, мінімізуючи при цьому перешкоди між користувачами. MU-MIMO призначений для збільшення пропускної здатності мережі та покращення загального користувацького досвіду [1].

В данному дослідженні показано основні принципи синтезу лінійної антенної решітки з рівноамплітудним та синфазним збудженням та було проведено аналіз методів адаптивного формування діаграми спрямованості Smart-антени на основі алгоритмів найменшого середньоквадратичного відхилення LMS та рекурсивного алгоритму найменших квадратів RLS.

При порівнянні враховувалися різні критерії, включаючи амплітудний відгук (коефіцієнт решітки), час збіжності, отримання та відстеження бажаного корисного сигналу.

Загалом, використання Smart-антен може призвести до створення більш ефективної, надійної та економічно вигідної системи бездротового зв'язку з покращеною якістю сигналу, більшою пропускною здатністю та кращим покриттям.

Список використаних джерел:

1. Андрущенко, О.В., Москалець, М.В., & Шумков, І.М. (2022). Оцінка продуктивності алгоритмів адаптивного формування променю Smart-антени для систем мобільного зв’язку 5G. Матеріали восьмої Міжнародної науково-технічної конференції «Проблеми електромагнітної сумісності перспективних безпроводових мереж зв’язку (EMC-2022)». 01-04. https://openarchive.nure.ua/server/api/core/bitstreams/c85b3240-d1f3-4d67-bd4f-170ff7330afc/content

2. Шумков, І. М., Москалець, М. В., & Андрущенко, О. В. (2022). Розробка ефективних моделей частотно-територіального планування мережі мобільного зв’язку LTE. Матеріали восьмої Міжнародної науково-технічної конференції «Проблеми електромагнітної сумісності перспективних безпроводових мереж зв’язку (EMC-2022)». 05-09. https://openarchive.nure.ua/server/api/core/bitstreams/cb3a40c2-b7b3-4137-a37b-f14b7ffa1ea3/content

3. Muliar, B., Koliadenko, Y. U., & Moskalets, M., Loshakov, V., Martynchuk, O., Ageyev, D. (2022). Interaction Model and Phase States at Frequency Resource Allocation in a Grouping of Radio-Electronic Equipment of 5G Mobile Communication Network. 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), pp. 1-7. https://doi.org/10.30837/ITSSI.2021.16.089

УДК 621.396.96

# ВИКОРИСТАННЯ ТЕХНОЛОГІЇ SDR В МЕТОДАХ ПАСИВНОЇ РАДІОЛОКАЦІЇ ТА РАДІОРОЗВІДКИ

Білик О.С.
Науковий керівник - к.т.н., доц. Мартинчук О.О.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
тел. +38(095) 737-22-99, e-mail: oleksandr.bilyk@nure.ua

The current development of radar and radio surveillance systems requires the implementation of new technologies, capable of increasing efficiency and functionality. One of these technologies is SDR (Software-Defined Radio), which allows to increase velocity of setting, flexibility and adaptability of radio receivers and radio transmitters. In this work was considered the use of SDR technology in the methods of radar and radio surveillance, as well as the advantages and possibilities for improving the system.

SDR (Software-Defined Radio) - це технологія, яка дозволяє програмно налаштовувати та керувати радіообладнанням з використанням звичайних комп'ютерів. Використання SDR для пасивної радіолокації може забезпечити високу гнучкість та точність вимірювань, оскільки може бути здійснене програмне налаштування параметрів радіоприймача та передача, автоматичного аналізу отриманих сигналів за допомогою розподілених обчислювальних систем.

Було розглянуто один з найдешевших і доступніших SDR - HackRF One. Він являє собою відкритий проект, вихідний код його доступний. Апаратні характеристики: 1 MHz to 6 GHz operating frequency, half-duplex transceiver, up to 20 million samples per second, 8-bit quadrature samples (8-bit I and 8-bit Q), compatible with GNU Radio, SDR#, software-configurable RX and TX gain and baseband filter, software-controlled antenna port power (50 mA at 3.3 V), SMA female antenna connector, SMA female clock input and output for synchronization, convenient buttons for programming, internal pin headers for expansion, USB-powered, open source hardware.

Через USB кабель модуль підключається до ПК, через який отримує живлення та виконується передача даних. В HackRF One мається мікроконтроллер LPC4320FBD144 с ARM Cortex-M4 ядром, стоїть CPLD XC2C64A-7VQG100C, з'єднана з мікросхемою MAX5864, яка представляє собою два АЦП та два ЦАП в одному корпусі. Разрядність АЦП = 8 біт, разрядность ЦАП = 10 біт. Характеристики саме цих АЦП и ЦАП достатньо слабкі. Відповідно до теореми Котельникова, їх максимальна тактова частота складає 22 МГц. Для збільшення широти полоси передатчика можна замінити мікросхему АЦП-ЦАП на іншу, більш швидкісну та передавати дані напряму з CPLD, в обхід мікроконтроллеру, але наступним слабким місцем буде максимально припустима ширина перелаштовуємого фільтру (30 МГц), розташованого в мікросхемі передавача MAX2837 (інтегрований

напівдуплексний РЧ передавач, виконаний за архітектурою прямого перетворення з нульовою проміжною частотою).

Якщо розглядати більш потужні SDR, то їх робота можлива на частотах до 6 ГГц. В пристроях з більш високими робочими частотами проблема високоякісного оцифровування ВЧ сигналів вирішується їх перенесенням на більш низьку частоту. Для цього використовуються змішувач і опорний генератор.

Для пасивної радіолокації з використанням SDR можуть бути використані різні методи та алгоритми, такі як методи обробки сигналів, фільтрації та аналізу, а також методи машинного навчання та штучного інтелекту. Відповідні програмні пакети дозволяють використовувати ці методи для знаходження та визначення місцеперебування об'єктів на основі аналізу відбитих сигналів.

Таким чином, використання SDR для пасивної радіолокації може забезпечити високу точність та гнучкість вимірювань, а також дозволяє використовувати різні методи та алгоритми для досягнення потрібної точності та надійності вимірювань. Використання технології SDR в методах пасивної радіолокації та радіорозвідки стало дуже актуальним завдяки його гнучкості та адаптивності. SDR дозволяє замінити апаратні компоненти радіосистем та радарів програмним забезпеченням, що в свою чергу дозволяє прискорити внесення змін, знижує вартість розробки та реалізації нових систем радіолокації та радіорозвідки.

Для роботи з SDR було розглянуто вільне і відкрите програмне забезпечення GNURadio. Воно забезпечує можливості програмного радіомовлення, його можна використовувати для створення додатків, отримання даних з цифрових потоків або передавати дані в цифрові потоки. GnuRadio має фільтри, канальні кодери, елементи синхронізації, еквалайзери, демодулятори, вокодер, декодери має можливість передачі даних від одного блоку до іншого. При створенні програмних симуляторів, для розробки можливо використовувати бібліотеки, написані на мовах C ++ і Python.

Список використаних джерел:

1. RTL – SDR приймач https://habr.com/ru/post/373465/
2. HackRF One https://habr.com/en/articles/499376/
3.Software Defined Radio https://habr.com/ru/post/451674/

УДК 004.056:004.77

# ДОСЛІДЖЕННЯ БЕЗПЕКИ МЕСЕНДЖЕРІВ

Маслакова Н.Ю.
Науковий керівник – доц. Золотарьов В.А.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
тел. +380662506777, e-mail: nataliia.maslakova@nure.ua

This paper focuses on the security of five messengers used by Ukrainians since the beginning of the war in Ukraine. The five messengers that are most used by Ukrainians are considered: Signal, Threema, WhatsApp, Viber and Telegram. A comparative table of the security and safety features of messengers, which are used in the Armed Forces of Ukraine in particular, is provided. It was concluded that none of the listed messengers is safe and cannot be used during the war.

В умовах сучасного інформаційного суспільства використання месенджерів розвинулися до неймовірних масштабів. До банального процесу обміну повідомленнями додалися відео та аудіо дзвінки, канали з величезною кількістю підписників, інтеграція з іншими вебсистемами для зосередження взаємодії в одному додатку за допомогою ботів, рекламні послуги для бізнесу та ще багато іншого.

Київський міжнародний інститут соціології (КМІС) провів опитування щодо найбільш популярних серед українців месенджерів. Виявилося, що найбільш поширеним засобом для комунікацій є Viber, яким користується 73,6% опитаних. Другим за популярністю є месенджер Threema – 42,7%. На третьому-четвертому місцях знаходяться Телеграм (використовують 31,6% опитаних) та WhatsApp (25,3%) [1].

Найчастіше, ми повністю впевнені в тому, що спілкуючись із співрозмовниками в чатах наше листування залишається конфіденційним. Однак варто розуміти, що подібна думка дуже помилкова і, навіть, наївна.

Метою доповіді є дослідження безпеки п’яти месенджерів, які використовуються українцями з початком війни в Україні. Ситуація із безпекою віртуального спілкування особливо загострилася після повномасштабного вторгнення РФ до України. Останнім часом значно зросла кількість кібератак на гаджети українців, а також почастішали зламування персональних сторінок у соцмережах.

Щоб убезпечити користувачів, експерти ІТ-компанії GlobalLogic визначили список найбезпечніших месенджерів для особистого та професійного спілкування (табл. 1[2]). За словами Орхана Гасимова, Technology Director, GlobalLogic, найбезпечнішим безкоштовним месенджером є Signal. Месенджер використовує технологію наскрізного шифрування - тобто, повідомлення доступні тільки для відправника й одержувача, їх не можна прочитати, навіть перехопивши [3].

Таблиця 1 - Порівняльна таблиця функцій захисту та безпеки месенджерів, які зокрема використовуються в ЗСУ

| | **Signal** | **Threema** | **WhatsApp** | **Viber** | **Telegram** |
|---|---|---|---|---|---|
| Місцезнаходження керуючого офісу | США | Японія | США | США | Швейцарія |
| Чи захищає застосунок повідомлення та медіа | Ні | Ні | Ні | Так | Так |
| Вбудовані можливості для збору даних | Ні | Ні | Ні | Ні | Ні |
| Розкриття даних для спецслужб | Частково | Так | Так | Ні | Ні |
| Збір даних користувачів (можливо для органів влади РФ) | Так | Так | Так | Ні | Ні |
| Шифрування за замовчуванням | Так | Так | Ні | Так | Так |
| Анонімність реєстрації | Ні | Ні | Ні | Ні | Так |
| Хешування особистих даних | Ні | Ні | Ні | Вибірково | Так |
| Шифрування метаданих | - | Ні | Ні | Так | Так |
| Двофакторна автентифікація | Ні | Так | Так | Ні | Так |

Виходячи з цього можна зробити висновок, що жодний з перерахованих месенджерів не є безпечним і не може використовуватися під час війни.

Список використаних джерел:

1. Сергій Кулеш. (2021, 19 листопада). Дослідження. Найпопулярніші серед українців месенджери за даними опитування КМІС. https://itc.ua/news/doslidzhennya-najpopulyarnishi-sered-ukrayinczіv-mesendzheri-za-danimi-opituvannya-kmis/.

2. Цифрова трансформація (2022, 25 січня). Використання месенджерів, як елементів цифрової розвідки: проблематика та шляхи вирішення. https://intelmag.com/digitalization/17454-vykorystannya-mesendzheriv-yak-elementiv-czyfrovoyi-rozvidky-problematyka-ta-shlyahy-vyrishennya/ .

3. Анна Нестерова. (2022, 16 листопада). Найбезпечніші месенджери 2022 року. https://gloss.ua/ua/lifestyle/139268-najbezpechnishi-mesendzheri-2022-roku.

**УДК 004.056:355.451**

# УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

УДК 004.056:003.27

# ВИКОРИСТАННЯ СТЕГАНОГРАФІЇ ДЛЯ ЗБЕРЕЖЕННЯ ТА ПЕРЕДАЧІ ІНФОРМАЦІЇ

Капуста Р.Д., Горяінова К.О.
Науковий керівник – ст. викл. Волотка В.С.
Харківський національний університет радіоелектроніки,
кафедра ІКІ ім. В.В. Поповського, м. Харків, Україна
тел. +38(095) 30-771-72, e-mail: roman.kapusta@nure.ua
тел. +38(097) 95-610-28, e-mail: karyna.horiainova@nure.ua

This work is dedicated to the study of the method of increasing the security of data storage and transmission by using a tool for steganographic file modification. The rapid development of information storage and transmission technologies entails a certain list of challenges related to the security of users' personal data. However, a potential thief can also use steganography to hide and transfer harmful software code, leading to undesirable consequences.

Ще давно людство використовувало різноманітні шифри для захисту інформації та недопущення розкриття даних у разі потрапляння інформації у інші руки. Сьогодні шифрування та кодування інформації стало звичайною справою без якої неможлива передача інформації у будь-який спосіб по мережі інтернет. Проте окрім класичних зашифрованих даних, які мають досить явний вигляд, використовується також і приховані повідомлення, що досягаються завдяки стеганографії.

Сучасна стеганографія відрізняється своїм різноманіттям інструментів та можливостей, одним з яких є приховування текстової інформації у вигляді зображення. Розглянемо використання програмного продукту "Outguess", який можливо використовувати на базі Linux-подібних операційних систем у нашому випадку це Kali Linux.

Функціонал даного програмного продукту дозволяє вставляти приховану інформацію в надлишкові біти джерел даних, а також природа джерела даних не має значення для роботи. Програма покладається на специфічні для даних обробники, які витягують надлишкові біти і записують їх назад після модифікації та підтримуються формати JPEG, PPM і PNM.

Для прикладу, створюємо простий скрипт, який дозоляє робити знімки екрану користувача без його відома та зберігати їх у відповідній папці. Назвемо цей файл «vir.py». Наступним кроком завантажуємо зображення під назвою «File1.jpg» та розміщуємо його у одній папці разом зі шкідливим програмним кодом. Використовуючи програмний продукт "Outguess" проводимо злиття файлів для отримання кінцевого зображення, яке містить у собі файл скрипту. Результат виконання перетворення файлів та відповідні результати приведено на рис. 1.

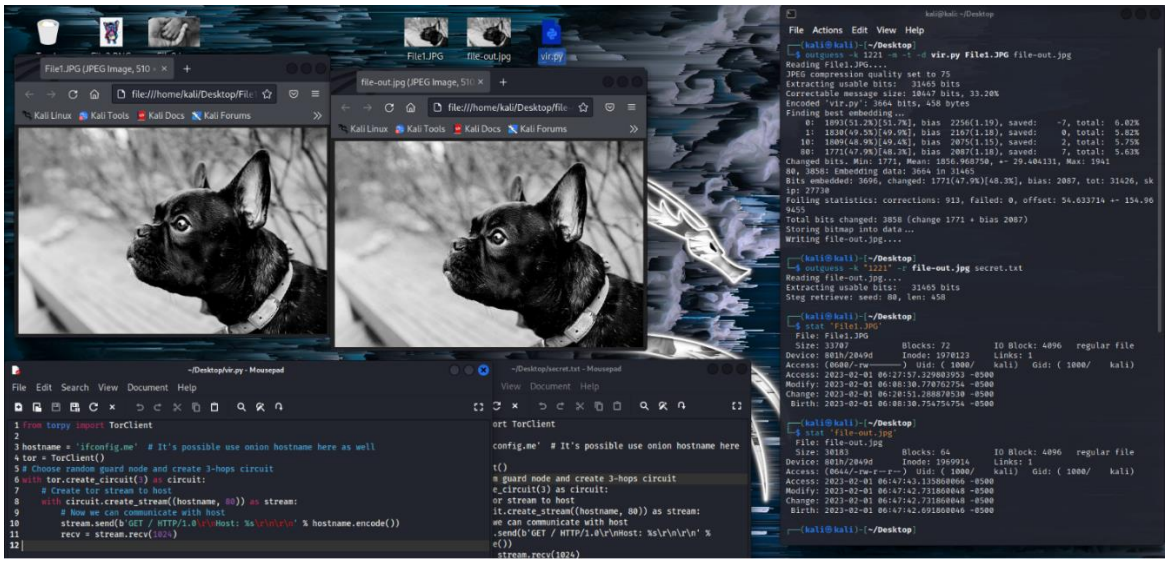


Рисунок 1 – Виконання перетворення

Розглянемо послідовність дій в консолі. Для початку встановимо ключ «пароль», в нашому випадку це “1221” та дані «vir.py» помістимо в зображення «File1.jpg». Ключ встановлюється для того, щоб в подальшому вилучити інформація с файлу без ключа було неможливо. Далі витягнемо повідомлення з даних в файл «secret.txt» за допомогою ключа. Відтепер можемо розглянути дані які були зашифровані.

Слід звернути увагу на те, що розмір зображення змінився. Спочатку 33707 байтів, а після внесення та шифровки даних 30183 байтів, а також кількість блоків – спочатку 72, а потім 64. Тобто оригінал виходить більше, ніж з тими даними, які були усередині.

Спираючись на отримані результати ми можемо дійти висновків, що стеганографія може бути використана зловмисником для передачі шкідливого програмного скриту у зображені, яке зовнішньо майже нічим не буде відрізнятися від оригіналу. Найкращій метод збереження власних даних від подібних пасток шахраїв - ігнорування підозрілих файлів від невідомих відправників, а також перевірка версій зміни файлів.

Ваша пильність та обачність – запорука безпеки персональних даних!

Список використаних джерел:

1. Martin, K. (2020, 27 січня). Що таке стеганографія та чим вона відрізняється від криптографії? instagalleryapp.com. https://instagalleryapp.com/informacijna-bezpeka/shho-take-steganografija-ta-chim-vona/.

2. Semilof, M., & Clark, C. (2021, 6 липня). What is Steganography? - Definition from SearchSecurity. Security. https://www.techtarget.com/searchsecurity/definition/steganography

УДК 57.087.1:621.391.26

# АНАЛІЗ НАПРЯМКІВ УДОСКОНАЛЕННЯ СИСТЕМ ГОЛОСОВОЇ АВТЕНТИФІКАЦІЇ

Петраченко М.О., Пастушенко М.С.
Науковий керівник – к.т.н., проф. Пастушенко М.С.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В.Поповського
м. Харків, Україна
тел. +38(097) 133-66-05, email: maksym.petrachenko@nure.ua.

This work evaluates how digital pre-processing techniques affect voice authentication systems. Voice biometrics are critical for information security, so improving recording quality is essential. Noise reduction methods, like the Wiener filter, improve audio quality and automatic speech recognition accuracy. Other pre-processing methods, such as spectral thresholding and the Hilbert transform, help determine the envelope of the signal and estimate the original signal as closely as possible to the noisy signal. These methods utilize the linear nature of phase change to detect and correct errors, improving the overall performance of authentication systems.

Біометричні технології стали критично важливим аспектом інформаційної безпеки, а голосова біометрія набуває все більшої популярності. Незважаючи на постійну роботу над підвищенням якості голосових систем, необхідно звернути увагу на попередню цифрову обробку голосових записів. Ця обробка може мати значний вплив на подальші процедури та автентифікацію користувача, що вимагає додаткового простору для попередньої обробки з метою зменшення шумів у голосових сигналах, враховуючи унікальні особливості обробки реєстраційних матеріалів у системах голосової автентифікації [1-4].

Традиційні методи шумозаглушення зазвичай використовують звичайні та спектральні порогові методи, а також такі моделі, як оцінка Вінера. Для усунення артефактів сигналу після операцій фільтрації шуму застосовується згладжування за допомогою таких фільтрів, як фільтр Гауса. Алгоритми машинного навчання також можуть допомогти у зменшенні шуму, дозволяючи як відокремлювати дикторів, так і посилювати сигнал [4].

Звук людської мови характеризується коливаннями як амплітуди, так і частоти, причому семантичний зміст зазвичай знаходиться в діапазоні від 200 Гц до 5 кГц. Шум можна розділити на три типи: випадковий, систематичний і аномальний, але статистичні методи обробки можуть допомогти усунути його. У контексті систем автентифікації метою постобробки записаних мовних сигналів є знаходження оцінки вихідного сигналу, максимально наближеної до зашумленого сигналу. Одним з ефективних способів досягти цього є застосування методів цифрової попередньої обробки, які передбачають використання методу перетворення

Гільберта, який може працювати як з фазою, так і з аналітичною огинаючою сигналу [1]:

$$S_m(t) = \frac{1}{\pi}\int_{-\infty}^{\infty} \frac{S(\tau)d\tau}{t-\tau},$$

де $\tau$ являє собою змінну інтегрування. У сфері обробки сигналів метод перетворення Гільберта зарекомендував себе, оскільки він полягає у визначенні огинаючої U(t) сигналу S(t) як модуля відповідного аналітичного сигналу. Змінна інтегрування, представлена через τ, відіграє вирішальну роль у цьому процесі. Якщо зосередитися на голосових сигналах, то помітимо, що їхня фаза має своєрідну пилкоподібну форму невизначеної тривалості. Амплітуда цього патерну лінійно змінюється в межах від 0 до 360 градусів, представляючи собою захоплююче явище для аналізу [2]. Однак, коли виникають випадкові помилки вимірювання, фаза сигналу відхиляється від його очікуваної лінійної поведінки. За наявності аномальних помилок можуть також відбуватися різкі зсуви фази на понад 10 градусів. Щоб вирішити цю проблему, лінійний характер зміни фази можна використовувати як апріорну інформацію для попередньої обробки голосового сигналу системи аутентифікації. Враховуючи очікувану поведінку фази, можна більш ефективно виявляти та виправляти помилки, покращуючи загальну продуктивність системи [4].

Список використаних джерел:

1. Pastushenko, M., Pastushenko, V., Pastushenko, O. (2019), "Specifics of Receiving and Processing Phase Information in Voice Authentication Systems", International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kyiv, Ukraine, 2019, pp. 621-624. **DOI:** 10.1109/PICST47496.2019.9061260

2. Pastushenko, M., Krasnozheniuk, Ya., Lemeshko, O. (2020), Analysis of voice signal phase data informativity of authentication system // Zaporizhzhia, Ukraine, April 27-May 1, 2020. Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020). PP 1040-1053.URI: http://openarchive.nure.ua/handle/document/11843

3. Pastushenko, M., Krasnozheniuk, Ya., Zaika, M. (2020), "Investigation of Informativeness and Stability of Mel-Frequency Cepstral Coefficients Estimates based on Voice Signal Phase Data of Authentication System User," International Conference "Problems of Infocommunications. Science and Technology" (PIC S&T′2020), pp. 1-5. **DOI:** 10.1109/PICST51311.2020.9468083

4. Камені Н.Г.Б., Пастушенко М.С. (2022), Обґрунтування та вибір простору попередньої обробки голосового сигналу в системі автентифікації, Проблеми телекомунікацій, Випуск №1 (30), 2022, С. 57-70. **DOI:** https://doi.org/10.30837/pt.2022.1.04

УДК 004.056:519.17

# АНАЛІЗ МОДЕЛЕЙ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ, ПОБУДОВАНИХ З ВИКОРИСТАННЯМ ТЕОРІЇ ГРАФІВ

Румянцева О.В
Науковий керівник – к.т.н., с.н.с. Пшеничних С.В.
Харківській національний університет радіоелектроніки,
каф. Інфокомунікаційної інженерії ім. В.В. Поповського,
м. Харків, Україна
тел+38(099) 029-93-20, e-mail: olha.rumiantseva@nure.ua

The report reviews the analysis of information security models that utilize graph theory. Graph theory is an essential tool for visualizing and analyzing complex systems, and its application to information security has resulted in models such as Attack Graphs, Defense Graphs, and Threats and Countermeasures. The strengths and limitations of each model are explored, and it is emphasized that the choice of an appropriate model depends on the specific security goals and the size of the system. The analysis highlights the potential for graph theory to contribute to the development of robust information security systems.

Моделі систем захисту інформації, що побудовані на основі теорії графів, дозволяють візуалізувати структуру інформаційної системи та виявляти вразливі місця, що дозволяє оптимізувати процеси керування доступом та керування вразливостями. У доповіді розглядається декілька таких моделей.

1. Модель управління доступом на основі графа. Дана модель використовується для визначення того, які суб'єкти мають доступ до об'єктів в інформаційній системі. Граф у цій моделі є набір вузлів (суб'єктів та об'єктів) та ребер (прав доступу). Вузли можуть бути пов'язані один з одним кількома ребрами, що представляють різні види доступу (читання, запис, видалення тощо) [1].

Ця модель полегшує процес управління доступом, дозволяючи визначати та змінювати права доступу для кожного суб'єкта окремо. Однак, необхідно враховувати, що ця модель може бути неефективною, якщо інформаційна система має великий розмір та складну структуру.

2. Модель оцінки ризиків на основі графів. Ця модель використовується для визначення ризиків, пов'язаних із компонентами інформаційної системи, та для вжиття заходів для зниження рівня цих ризиків. У цій моделі інформаційна система представлена у вигляді графа, де вершини відповідають компонентам, а ребра позначають зв'язок між ними.

Ця модель дозволяє виявити критичні компоненти системи та зосередити зусилля на їхньому захисті. Крім того, вона може бути використана для оцінки ефективності різних заходів щодо зменшення рівня

ризику. Однак, ця модель може бути неповною, якщо не враховувати всі можливі загрози.

3. Модель управління вразливістю на основі графів. Ця модель використовується для виявлення вразливостей в інформаційній системі та визначення заходів щодо їх усунення. У цій моделі інформаційна система представлена у вигляді графа, де вершини являють собою уразливості, а ребра - зв'язки між вразливостями та компонентами системи, які можуть на них вплинути [2]. Наприклад, вразливість в одному компоненті може призвести до розкриття інформації в іншому компоненті, з яким вона пов'язана.

Ця модель дозволяє виявляти вразливості та оцінювати їхню критичність для інформаційної системи. Крім того, вона може використовуватися для визначення оптимальної стратегії управління вразливістю. Однак, дана модель може бути складною для аналізу у випадку, якщо інформаційна система має велику кількість компонентів та вразливостей, що може призвести до складнощів при прийнятті рішень щодо управління вразливостями.

4. Модель загроз і контрзаходів (Threats and Countermeasures - TAM). Ця модель заснована на поданні інформаційної системи у вигляді графа, в якому вузли являють собою загрози, а ребра - контрзаходи, що спрямовані на запобігання цим загрозам.

Ця модель дозволяє визначити найбільш ймовірні загрози для інформаційної системи та вибрати найбільш ефективні контрзаходи для їх запобігання [2]. Крім того, вона може використовуватися для оцінки ефективності наявних контрзаходів та визначення того, які покращення слід внести до системи захисту. Однак, ця модель також може бути складною для аналізу у випадку, якщо є велика кількість загроз та контрзаходів, що може призвести до складнощів при ухваленні рішень щодо управління інформаційною безпекою.

Загалом моделі систем захисту інформації, що побудовані з використанням теорії графів, є ефективними інструментами для аналізу та управління інформаційною безпекою. Однак, для досягнення найкращих результатів необхідно враховувати особливості конкретної інформаційної системи та обирати ту модель, що найбільше підходить для даної системи та її цілей.

Список використаних джерел:

1. Кіровоградський, М. І., & Куренков, О. С. (2016). Теорія графів: Навчальний посібник. Логос.

2. Коваленко, В. О., & Куренков, О. С. (2018). Аналіз інформаційних систем з використанням методів теорії графів. Виддавництво «Видавництво Полтавського університету економіки і торгівлі».

УДК 004.056:004.94

# ЗАСТОСУВАННЯ ІГРОВОЇ МОДЕЛІ ДЛЯ ДОСЛІДЖЕННЯ ОПТИМАЛЬНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Румянцева О.В
Науковий керівник – к.т.н., с.н.с. Пшеничних С.В.
Харківській національний університет радіоелектроніки,
каф. Інфокомунікаційної інженерії ім. В.В. Поповського,
м. Харків, Україна
тел+38(099) 029-93-20, e-mail: olha.rumiantseva@nure.ua

The report reviews the application of a game model to investigate the optimality of information security systems. The report also highlights the importance of considering multiple stakeholders and their competing interests when designing a secure system. It outlines the steps involved in developing a game model, including identifying players, defining strategies. The report described how simulation and optimization techniques can be used to evaluate different scenarios and identify the optimal solution. Ultimately, the report concludes that game models can provide a useful tool for designing secure systems and highlights its potential to improve decision-making in the field of information security.

У доповіді розглядаються особливості застосування ігрової моделі як інструменту моделювання при оптимізації систем захисту інформації.

Ігрова модель – це математичний інструмент, що використовується для аналізу стратегічних ситуацій, у яких приймають рішення кілька учасників (гравців), кожен із яких прагне максимізувати свою вигоду. Ігрова модель складається з гравців, правил гри та набору стратегій, які кожен гравець може вибрати. Гравці можуть приймати рішення одночасно чи послідовно, залежно від типу гри. Кожен гравець намагається вибрати найбільш вигідну стратегію з огляду на стратегії інших гравців [1].

У контексті захисту інформації гравцями можуть виступати зловмисники, які намагаються отримати несанкціонований доступ до захищеної інформації, та захисники, які намагаються запобігти таким атакам та захистити інформацію. Ігрова модель може бути використана для визначення оптимального балансу між захистом інформації та її доступністю для легітимних користувачів. Під час створення ігрової моделі необхідно враховувати різні фактори, такі як можливості нападаючого, вартість захисту та ризики порушення безпеки. На основі цієї моделі можна проводити симуляції, в яких гравці приймають рішення та взаємодіють один з одним, щоб визначити оптимальний проект системи захисту інформації [2].

Одним із прикладів ігрової моделі, яка може бути використана для дослідження оптимальності проекту системи захисту інформації, є модель «Stackelberg», яка включає двох гравців – лідера та послідовника. Лідер є

захисником, який приймає рішення про ступінь захисту інформації, а послідовник – нападника, який намагається проникнути в систему.

У цій моделі лідер ухвалює рішення першим, а послідовник реагує на це рішення. Лідер може вибирати різні рівні захисту, а послідовник може вибирати різні способи атаки. Мета кожного гравця – максимізувати свою вигоду. Результати симуляції можуть показати оптимальний рівень захисту інформації та оптимальні стратегії захисту від атак. Таким чином, ігрова модель може бути корисним інструментом для дослідження оптимальності проекту системи захисту інформації, дозволяючи враховувати різні фактори та знаходити баланс між захистом та доступністю інформації. Ігрова модель дозволяє оцінити ефективність різних стратегій захисту інформації та вибрати найкращу. Також вона може використовуватись для аналізу впливу зміни параметрів системи захисту інформації на її ефективність. В ігровій моделі можуть бути використані різні критерії оцінки, наприклад, час проникнення зловмисника, рівень шкоди, можливість виявлення та запобігання атаки тощо. Оцінка проводиться з урахуванням усіх можливих сценаріїв дій як зловмисників, так і адміністраторів системи захисту інформації.

У результаті аналізу ігрової моделі можна виявити вразливості системи та вжити заходів щодо їх усунення. Також можна визначити оптимальне співвідношення між витратами на захист та можливим збитком від атаки, що дозволить вибрати найбільш оптимальний варіант захисту інформації. Також використання ігрової моделі для аналізу оптимальності проекту системи захисту інформації дозволяє ухвалити обгрунтовані рішення, які зменшать ймовірність витоку інформації та захистять систему від можливих атак. Крім того, використання ігрової моделі дозволяє розглянути різні сценарії атаки та оцінити ступінь їхнього впливу на систему захисту інформації. Це може допомогти виявити слабкі місця в системі та покращити її захист. В цілому, використання ігрової моделі для дослідження оптимальності проекту системи захисту інформації є потужним інструментом, який може допомогти розробникам проекту прийняти більш обгрунтовані рішення та створити більш ефективну систему захисту інформації.

Список використаних джерел:

1. Петров, В. Г. (2019). Використання ігрових технологій для дослідження вразливості інформаційних систем. Проблеми захисту інформації, (2), 47-54.

2. Баранова, Н.І. (2011). Методи і засоби захисту інформації в комп'ютерних системах. Київ: ВПЦ «Київський університет». (с. 272)

УДК 005.7:519.83]:004.056

# СТРАТЕГІЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ МАТЕМАТИЧНОГО АПАРАТУ ТЕОРІЇ ІГОР

Фукс М. А.
Науковий керівник – к.т.н., доцент Добринін І.С.
Харківський національний університет радіоелектроніки,
каф. інфокомунікаційної інженерії імені В.В. Поповського,
м. Харків, Україна
тел. +38(066) 163-90-04, e-mail: maksymillian.fuks@nure.ua.

The aim of the work is to analyze the possibilities of the implementation of the mathematical model of a bimatrix game between the security administrator and attacker for determining an optimal security information strategy against possible attacks with a limited budget for the company. Different methodologies for implementing ISMS reflect the need to deploy and implement information security measures but do not present recommendations on how to conduct the selection. Therefore, CISO has to rely on its experience only. To assist him in defining the best strategy, the implementation of a bimatrix game was considered.

Інформаційна безпека займає помітне місце у інвестиціях компаній, адже все більше учасників бізнесу розуміють, що завдяки досягненню певного рівня безпеки та впровадження необхідних методів захисту від атак можна запобігти втратам. Насправді, інвестиції у механізмі захисту неспроможні принести прямий приріст прибутку, бо забезпечується скоріш мінімізація втрат від можливих атак. Отже, запобігання можливих втрат може розглядатися як економія різноманітних ресурсів усієї бізнес-системи.

Проблемі визначення ефективності проведених інвестицій у кібербезпеку присвячено доволі багато літератури, публікацій та певних методів, наприклад, метод аналізу ієрархій Томаса Сааті, теорія корисності або використання математичного апарату теорії ігор. У роботі [1] досліджується можливість застосування нечіткого багатокритеріального методу на основі парних порівнянь альтернатив для проведення аналізу при виборі кращого варіанту СЗІ. Також згадується принцип Беллмана-Заде, який стверджує, що найкращою може вважатися та альтернатива, яка найбільш серед інших відповідає усім створеним критеріям, а також не допускається нестача одних показників надлишком інших. Робота [2] зосереджується на пропонуванні теоретико-ігрового методу, що оптимально розподіляє ресурси направлені на кібербезпеку. Пропонується біматрична гра, що представляє імітацію середовища кібербезпеки, де доказується, що стратегія Неша для захисника є мінімаксною. Також пропонується застосування методу сингулярного розкладання SVD для знаходження приблизного значення точки рівноваги.

Існує велика кількість підходів, на основі яких компанія може розгорнути власну СМІБ, наприклад, стандарти International Organization for

Standardization (ISO) та Federal Information Processing Standard (FISP), публікації The National Institute of Standards and Technology (NIST), серія стандартів 8500.x, Security Technical Implementation Guide (STIG), документи The European Union Agency for Cybersecurity (ENISA), нормативно-правові акти, методологія IT-Grundschutz, тощо. Процес визначення прийнятного ризику та вибір оптимальних стратегій для використання CISO – нелегка задача, адже навіть у вищезазначених методологіях відображена лише необхідність розгортання та впровадження засобів захисту інформації, але не представлені рекомендації щодо того, як саме провести оптимізацію вибору. Зазвичай наявне також обмежене фінансування, а тому необхідно поєднувати виділені фінансові можливості, потрібні методи захисту і принцип розумної достатності для отримання у результаті ефективної та якісної СМІБ.

Вирішення висвітленої проблеми лежить у представленні взаємовідносин між учасниками, які мають різні чи навіть протилежні мотиви, за допомогою математичного апарату теорії ігор. Використання теоретико-ігрового підходу для моделювання процесу боротьби за реалізацію власних інтересів між CISO та зловмисником є резонним, адже вони обидва є раціональними, розумними і некооперативними, та мають на меті максимізацію власних функцій виграшу шляхом застосування певних стратегії. Тактика кожного з гравців детермінується ходами іншого.

Наявні різноманітні типи ігор, які розкривають моделювання по-різному. Найчастіше для моделювання використовують антагоністичну гру, де некооперативні гравці мають повністю протилежні виграші. Але у цьому випадку, насправді, робиться припущення, що втрати організації дорівнюють виграшу зловмисника, що і є грубим спрощенням усієї гри. Для уникнення подальших проблем та некоректних результатів наявна можливість застосування дещо іншого типу ігор, а саме біматричних ігор.

Використання біматричних ігор у моделюванні взаємодії CISO та зловмисника не суперечить наявним публікаціям та методологіям і може використовуватися як альтернатива, що використовує більше вхідних даних, адже вона розглядає як інтереси CISO, так і зловмисника, а тим самим спроможна представити більш точний результат.

Список використаних джерел:

1. Шматко О. В. Багатокритеріальний вибір систем захисту інформації за допомогою нечітких парних порівнянь альтернатив / О. В. Шматко, Є. В. Сичев. // ХПІ. – 2011. – С. 161–164.

2. Andrew Fielder. Game Theory Meets Information Security Management / Andrew Fielder, Emmanouil Panaousis, Pasquale Malacaria. // IFIP International Federation for Information Processing. – 2014. – С. 15.

УДК 004.056:[004.738.5:004.722]

# 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 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 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 використаних джерел:

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

УДК 004.056:[004.738.5:004.722]

# СУЧАСНІ КІБЕР-РИЗИКИ ІНТЕРНЕТУ РЕЧЕЙ ТА МЕТОДИ ЗАХИСТУ ВІД НИХ

Качан В.Є
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

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 ресурсу: 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 004.056:355.451

# ТЕХНОЛОГІЇ І МЕТОДИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Дригач К.В., Показій.К.О
Науковий керівник – ас., Бондаренко М.Е.
Харківський національний університет радіоелектроніки, кафедра ЕОМ
м. Харків, Україна
тел. +38(050) 952-26-48, email: kyrylo.dryhach@nure.ua.

Every year, more and more companies face growing threats to information security. Inadequate data security can lead to personal information leaks, reputational damage, financial losses, and even legal violations. In this regard, information security management is a critical component of any company. This paper presents the analysis of solutions, their implementation and comparison. An analysis of the spread of threats in recent years was also carried out.

Система управління інформаційною безпекою є сучасним процесом забезпечення безпеки інформаційних ресурсів організації, яка побудована на кращих світових практиках [1]. Шифрування даних є одним із прикладів такого пристрою. Шифрування даних захищає інформацію, перетворюючи її на код, який можна розшифрувати лише за допомогою унікального ключа. Для захисту даних використовуються різні техніки, включаючи симетричне та асиметричне шифрування.

Інша техніка – це управління доступом до інформації. Керування доступом до інформації дозволяє гарантувати безпеку інформації, обмежуючи доступ лише схваленим користувачам. Це можна зробити, використовуючи систему інсталяції для затвердження та ідентифікації користувачів.

Окрім технології, важливим елементом управління інформаційною безпекою є методи, які використовуються для пошуку, оцінки та обробки ризиків інформаційної безпеки.

Проведення аудиту безпеки комп'ютера – один із більш сучасних способів. Аудит дозволяє оцінити ступінь інформаційної безпеки організації, виявити можливі загрози та ризики, а також створити пропозиції щодо покращення інформаційної безпеки. Формування системи забезпечення, методології управління та методичного інструментарію оцінювання стану захищеності підприємства від небезпек базується не лише на уточненні сутності поняття «економічна безпека», але і на уточненні змістовної сутності поняття «стан» [2].

Інший підхід полягає у впровадженні системи управління інформаційною безпекою (ISMS). СУІБ – це система, яка містить методи, протоколи та політики, які забезпечують інформаційну безпеку організації, дає змогу виявляти, оцінювати та керувати ризиками у сфері інформаційної

безпеки. Навчання та розвиток персоналу є безкоштовною частиною управління інформаційною безпекою.

Управління інформаційною безпекою є важливим елементом будь-якої компанії. Такі технології, як шифрування даних і контроль доступу до інформації, можуть допомогти гарантувати секретність і цілісність інформації, тоді як такі методи, як аудит і впровадження СУІБ, можуть допомогти виявити й усунути загрози інформаційній безпеці. Особливо уразливі від атака є заклади навчання та їх інформаційні та навчальні платформи, національні ресурси надання бюрократичних послуг, а також банківські системи.

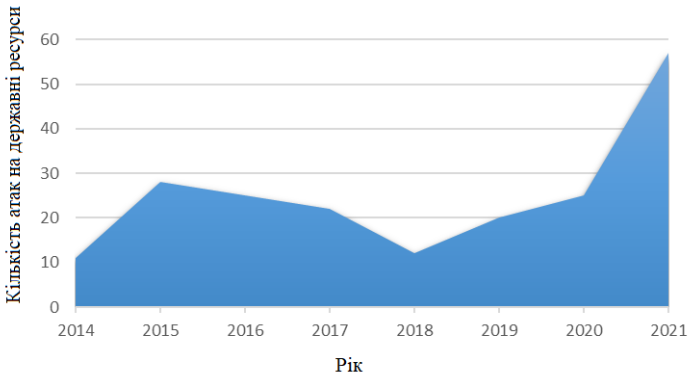



Рисунок 1 – Графік кількості кібератак на державні ресурси

Крім того, підвищується кваліфікація людей у наданні знань і навичок у сфері комп'ютерної безпеки. Загалом ефективне управління інформаційною безпекою вимагає інтегрованої стратегії, яка включає технології, методології, політики та процедури.

З розвитком технологій і збільшенням обсягу даних управління інформаційною безпекою зіткнеться з новими проблемами та вимогами в майбутньому. Однак, знаючи та впроваджуючи найкращі практики інформаційної безпеки, організація може гарантувати безпеку своїх інформаційних операцій, одночасно досягаючи успіху у своїх.

Список використаних джерел:

1. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України. Взято 03.03.2011 з https://zakon.rada.gov.ua/laws/show/v0365500-11

2. Яковенко, Є.І., Журавель, І.М., Горбатий, І.В., Бондраєв, А.П. (2019). Інформаційна Безпека. Львівська політехніка, 156–220.

3. Гаделюка, І. Б. (2015). Комп’ютерні засоби, мережі та системи, №14, 141–150.

УДК 004.056:355.451]:004.946

# ІНФОРМАЦІЙНІ РИЗИКИ ПРИ РОБОТІ З ВІРТУАЛЬНИМ СЕРЕДОВИЩЕМ

Шульга М.Д.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківській національний університет радіоелектроніки, Харків, Україна
тел. (057) 702-13-20, e-mail: mykyta.shulha@nure.ua

As the adoption of virtualization technologies grows, it attracts more attention from potential attackers. Issues such as data leaks, breaches in isolation, and insecure configurations can restrict flexibility and heighten risks linked to specific vulnerabilities. Identifying and addressing these risks help maintain the confidentiality, integrity, and availability of data in the virtual environment. Thus, early detection of information security risks bolsters risk management strategies.

Робота з віртуальним середовищем створює низку інформаційних ризиків, які організації повинні вирішити, щоб забезпечити безпеку та цілісність даних:

Вразливості гіпервізора, який керує віртуальними машинами, може стати мішенню для зловмисників. Таким чином одна з вразливостей може скомпрометувати все віртуальне середовище, це призведе до витоку даних або збоїв у роботі системи. Наприклад, дані що передаються між віртуальними машинами або через віртуальні мережі, можуть бути перехоплені, якщо вони не зашифровані або захищені належним чином.

Відсутність належної ізоляції між віртуальними машинами може призвести до несанкціонованого доступу або витоку даних між віртуальними машинами, порушуючи вимоги конфіденційності та безпеки.

Не відповідність конфігурацій компонентів віртуальної інфраструктури рекомендованим практикам, може наразити середовище на загрози безпеці, втрату даних або зниження продуктивності.

Внутрішні загрози: зловмисні інсайдери, які мають доступ до віртуального середовища, можуть навмисно чи ненавмисно спричинити витік даних, збої в роботі системи або інші інциденти безпеки. Неконтрольоване зростання віртуальних машин може довести до відсутності повного контролю над середовищем, ускладнюючи ефективне керування та охоплення захищеності всіх ресурсів. Нераціональне керування ресурсами може привести до проблем із продуктивністю або атак типу «відмова в обслуговуванні», що впливає на доступність критично важливих систем.

Неповне резервне копіювання або відсутність регулярного послідовного резервного копіювання віртуального середовища може привести до втрати даних, збоїв системи або тривалого процесу відновлення у разі збою або атаки.

Залежність технології віртуалізації від певного постачальника може обмежити гнучкість і збільшити ризики, пов’язані з вразливістю постачальника або обмеженнями підтримки з боку постачальника.

Організації повинні переконатися, що їх віртуальні середовища відповідають відповідним нормам, стандартам або вказівкам, таким як GDPR, або PCI DSS. Наприклад, згідно з GDPR, необхідно запровадження в компанії:

−реєстрів даних з ідентифікацією, які це дані, ким і для чого обробляються й кому передаються;

−призначення спеціального спеціаліста в компанії для дотримання заходів із поводженням із даними (Data Protection Officer), який повинен володіти знаннями в області права та досвідом із захисту даних [1].

Або сертифікат PCI DSS повинні мати будь-які торгово-сервісні компанії та постачальники послуг, що приймають, передають або зберігають дані міжнародних карт користувачів: основний номер карти (PAN), ім'я власника, термін дії та сервісний код. Серед них: банки, держустанови, e-commerce, розробники програмного забезпечення, хмарні оператори тощо.

В Україні отримання цього стандарту не регулюється законом. Але щороку з'являються IT-проекти: електронний та віртуальний банкінг, інтернет-магазини, а з введенням карантину почала активно розвиватися онлайн-торгівля. Питання забезпечення кібербезпеки для них є найбільш важливим, адже це, в першу чергу, питання репутації та статусу на ринку. Компанії, які не мають цього сертифікату, можуть погано захищати дані клієнтів. Тому стають легкою мішенню для шахраїв, і компенсувати збитки клієнтам в разі інциденту доведеться саме їм [2].

Усунення інформаційних ризиків під час роботи з віртуальним середовищем вимагає комплексного підходу, який включає впровадження надійних засобів контролю безпеки, регулярний моніторинг і сильну стратегію управління ризиками.

Список використаних джерел:

1. GDPR для юристів, або як підготуватися до неминучих змін. https://yur-gazeta.com/dumka-eksperta/gdpr-dlya-yuristiv-abo-yak-pidgotuvatisya-do-neminuchih-zmin-.html

2. Як хмара допомагає отримати сертифікат PCI DSS. https://gigacloud.ua/blog/navchannja/jak-hmara-dopomagae-otrimati-sertifikat-pci-dss

УДК 004.056:355.451]:004.946

# ОЦІНКА ІНФОРМАЦІЙНИХ РИЗИКІВ ПРИ РОБОТІ З ВІРТУАЛЬНИМ СЕРЕДОВИЩЕМ

Шульга М.Д.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківській національний університет радіоелектроніки,
Харків, Україна
тел. (057) 702-13-20, e-mail: mykyta.shulha@nure.ua

During an information security audit, a fair evaluation of the virtual environment's data protection level is conducted. The audit results reveal the effectiveness of information security and access control measures within the virtual setting, as well as ways to minimize risks when handling confidential information. Evaluating information security risks and employing a holistic risk management approach in a virtual environment enables organizations to better safeguard their virtual infrastructure, maintain data security, and uphold the integrity of their IT systems. By adopting a proactive stance, companies can stay ahead of emerging threats and adjust to evolving developments in the virtualization landscape.

Оцінка інформаційних ризиків під час роботи з віртуальним середовищем має вирішальне значення для підтримки безпеки та цілісності даних та IT-ресурсів. Нижче представлено ключові кроки для оцінки ризиків віртуальної інфраструктури.

Необхідно здійснювати каталогізацію всіх активів у віртуальному середовищі, включаючи віртуальні машини, гіпервізори, мережі та системи зберігання.

Проводити оцінку потенційних загроз, наприклад, зловмисне програмне забезпечення, несанкціонований доступ, витік даних і внутрішні загрози, які можуть вплинути на віртуальне середовище.

Пропонується систематично проводити регулярну оцінку вразливостей, включаючи сканування та пентест, щоб визначити пріоритети для закриття слабких місць у віртуальній інфраструктурі.

Необхідно проводити оцінку імовірності та потенційного впливу кожної виявленої загрози та вразливості, враховуючи такі фактори, як вартість активів, використані засоби контролю безпеки та потенційні наслідки атаки.

Здійснювати процедури ранжування ризиків на основі їх впливу та ймовірності реалізації, зосереджуючись на розгляді найбільш критичних даних.

Пропонується розробити та запровадити засоби контролю безпеки. Це може включати контроль доступу до даних, шифрування, моніторинг та резервне копіювання іміджів.

Робити перевірку віртуального середовища на наявність несанкціонованих подій та інцидентів у сфері безпеки. Необхідно оновлювати підходи до оцінки ризиків, це необхідно, щоб врахувати зміни в середовищі, оцінити нові загрози або виправити реалізацію організаційних вимог для доступу к даним.

Пропонується проводити безперервне підвищення обізнаності та навчання для співробітників, щоб зменшити ймовірність людських помилок або внутрішніх загроз, гарантуючи, що вони ознайомлені з найкращими практиками та можливими ризиками, пов'язаними з віртуальним середовищем.

Розробити та підтримувати плани реагування на інциденти та безперервності бізнесу, щоб забезпечити швидке аварійне відновлення системи та мінімізувати вплив інцидентів безпеки.

Необхідно провести оцінку безпеки постачальників технологій чи послуг віртуалізації. Оцінити методи безпеки та відповідність галузевим стандартам і правилам [1].

Проводити звітування про виявлені ризики, стратегії пом'якшення та їх вплив на організацію відповідним зацікавленим сторонам, зокрема керівництву, IT-командам і співробітникам.

Також необхідно проводити регулярні оцінки ризиків, щоб виявити нові ризики або ризики, що розвиваються, оцінити ефективність існуючих засобів контролю та за потреби скоригувати стратегію управління ризиками.

Вести повну документацію щодо оцінки ризиків, засобів контролю безпеки та планів реагування на інциденти.

Зберігати записи про події безпеки, інциденти та зміни у віртуальному середовищі, щоб полегшити майбутні оцінки ризиків і перевірки.

Сприяти розвитку культури безперервного вдосконалення, навчання на інцидентах і адаптації стратегії управління ризиками для вирішення нових загроз, вразливостей та змін у цілях або вимогах організації.

Список використаних джерел:

1. Білецький Е. В., Янушкевич Д. А., Шайхлісламов З. Р.. (2015). Управління якістю продукції та послуг

УДК 004.056:004.946

# МЕХАНІЗМИ ЗАХИСТУ ВІРТУАЛЬНОГО СЕРЕДОВИЩА

Шульга М.Д.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківській національний університет радіоелектроніки,
Харків, Україна
тел. (057) 702-13-20, e-mail: mykyta.shulha@nure.ua

As the adoption of virtualization technologies continues to expand, so do the threats to information security, leading to heightened focus on protective measures. Virtual infrastructure is becoming increasingly reliable and capable of addressing a broad spectrum of security issues. However, the primary challenges concerning virtualization platform security lie in the design of the final solutions based on them. It is evident that deploying a virtual infrastructure presents distinct security challenges, such as hypervisor vulnerabilities, virtual machine (VM) isolation, and configuration errors. Identifying and mitigating these risks contribute to preserving the confidentiality, integrity, and availability of an organization's data and IT resources.

Метою управління ризиками IT-проектів є оперативне виявлення факторів, пов’язаних з виконанням інформаційної системи або системи автоматизації, які можуть негативно вплинути на реалізацію проекту, та оптимальне планування дій для мінімізації цих факторів.

Сьогодні багато організацій покладаються на віртуальне середовище як на критичне програмне забезпечення для тестування рішень. Забезпечення захисту даних віртуального середовища є важливим компонентом корпоративної інформаційної безпеки протягом багатьох років розгортання віртуальної інфраструктури. Робота з віртуальними машинами пов'язана з різними ризиками. Механізми захисту у віртуальному середовищі необхідні для забезпечення безпеки та цілісності віртуалізованих систем. Для захисту віртуальної інфраструктури можна використовувати різні методи.

Безпека гіпервізора. Перевіряти чи встановлені останні оновлення ОС, налаштування віртуальних машин відповідають політикам організації, це знизить ризик використання вразливостей.

Ізоляція віртуальної машини. Використання політики ізоляції віртуального середовища, наприклад, ізольованої мережі для тестування рішень з налаштованими брандмауерами, щоб запобігти можливому витоку даних або несанкціонованому доступу.

Безпека мережі. Використання брандмауерів, системи виявлення та запобігання вторгненням (IDPS) і сегментацію мережі для захисту мережевого трафіку віртуального середовища.

Контроль доступу. Реалізація механізмів автентифікації та авторизації для керування доступом до віртуальних ресурсів. Використання

багатофакторної автентифікації (MFA), щоб обмежити доступ до конфіденційної інформації та ресурсів.

Шифрування. Використання шифрування носіїв такими утилітами як Bitlocker, McAfee Drive Encryption.

Моніторинг і аудит безпеки. Необхідно систематично робити аудит віртуального середовища для виявлення потенційних загроз, вразливостей або неправильних налаштувань. Можливе впровадження системи керування журналами та інформацією про безпеку та керування подіями (SIEM), щоб збирати й аналізувати події безпеки.

Керування виправленнями. Проводити оновлення ОС віртуальних машини та програмного забезпечення за допомогою патчів та оновлень безпеки.

Резервне копіювання та аварійне відновлення. Необхідно створити правила резервного копіювання даних і конфігурацій, а також створення іміджів систем для аварійного відновлення, щоб забезпечити доступність і цілісність віртуального середовища у разі збоїв або атак.

Безпечна конфігурація. Необхідно дотримуватись найкращих рекомендацій і практик щодо безпечного налаштування компонентів віртуальної інфраструктури, таких як гіпервізори, віртуальні машини та пристрої віртуальної мережі.

Безпека кінцевих точок. Використовувати антивірусне програмне забезпечення, систему захисту від зловмисного програмного забезпечення та системи запобігання вторгнень на основі хосту (HIPS).

Проводження навчання. Проводити навчання співробітників можливим проблемам безпеки та найкращим практикам, пов’язаним із віртуальними середовищами, це зменшить ймовірність людських помилок або внутрішніх загроз.

Список використаних джерел:

1. Що таке багатофакторна автентифікація та коли доцільно її використовуватиTechnologies. https://yubikey.com.ua/shcho-take-bahatofaktorna-avtentyfikatsiia-ta-koly-dotsilno-ii-vykorystovuvaty

2. Система виявлення вторгнень (HIPS). https://help.eset.com/ees/7/uk-UA/idh_hips_main.html

УДК 004.056.523:621.396.946

# АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АТАК НА БЕЗПЕКУ В БЕЗДРОТОВИХ КОРПОРАТИВНИХ МЕРЕЖАХ WI-FI

Войлов В.І.
Науковий керівник – к.т.н., с.н.с. Калюжний М.М.
Харківський національний університет радіоелектроніки, кафедра IMI ,
м. Харків, Україна
тел. +38(063) 039-06-91, e-mail: vladyslav.voilov@nure.ua

As technology advances, more and more companies are turning to wireless Wi-Fi networks to ensure seamless communication between employees and devices in offices and other workplaces. However, such networks are vulnerable to security attacks that can lead to leaks of confidential information, data corruption, and network disruption. Therefore, in this research publication, we will examine various methods to detect and prevent security attacks on wireless corporate Wi-Fi networks.

Для захисту бездротових корпоративних мереж від атак можуть використовуватися такі методи:

1. Шифрування мережі Wi-Fi

Шифрування є одним з основних методів захисту Wi-Fi мереж від атак. Різні методи шифрування, як-от WPA2 та WPA3, можуть використовуватися для захисту Wi-Fi мереж від атак.

2. Використання аутентифікації за паролем і сертифікатами

Аутентифікація за паролем і сертифікатами є ще одним методом захисту Wi-Fi мереж від атак. Паролі та сертифікати можуть бути використані для перевірки автентичності користувачів, що може запобігти атакам від несанкціонованих користувачів.

3. Фільтрація MAC-адрес

Фільтрація MAC-адрес може використовуватися для обмеження доступу до Wi-Fi мережі тільки для певних пристроїв, у яких є заздалегідь визначені MAC-адреси. Але, цей метод можна обійти за допомогою «прослуховування» етеру та присвоєння MAC-адреси жертви.

4. Використання віртуальної приватної мережі (VPN)

VPN є методом шифрування трафіку між пристроями, що може запобігти проникненню зловмисників у Wi-Fi мережу. Цей метод забезпечує захист даних на більш високому рівні, ніж просте шифрування мережі.

5. Використання фаєрвола

Фаєрвол - це програмне забезпечення, яке може використовуватися для виявлення та запобігання атакам на безпеку в бездротових мережах Wi- Fi. Фаєрволи можуть налаштовуватися для блокування певних типів трафіку або певних IP-адрес, що може допомогти запобігти атакам на безпеку.

6. Моніторинг трафіку

Моніторинг трафіку є одним із методів виявлення атак на безпеку в

бездротових мережах Wi-Fi. Різні програми моніторингу, як-от Wireshark, NetworkMiner можуть використовуватися для аналізу трафіку та виявлення аномальної поведінки в мережі.

7. Використання інтелектуальних систем захисту

Інтелектуальні системи захисту можуть використовуватися для виявлення атак на безпеку в бездротових мережах Wi-Fi. Ці системи можуть аналізувати трафік і визначати аномальну поведінку, що може допомогти запобіганню атак.

Нижче наведено таблицю, яка показує якісну ефективність різних методів захисту Wi-Fi мереж від атак на безпеку:

| | **Метод захисту** | **Ефективність** |
|---|---|---|
| | Шифрування | Висока |
| | Аутентифікація | Середня |
| | Фільтрація MAC-адрес | Мінімальна |
| | VPN | Висока |
| | Фаєрвол | Висока |
| | Моніторинг трафіку | Висока |
| | Інтелектуальний захист | Висока |

З таблиці можна бачити, що найбільш ефективними методами захисту Wi-Fi мереж від атак є шифрування, VPN, фаєрвол, моніторинг трафіку, інтелектуальний захист. Запропоновано використання комбінацій цих методів для гарантованого захисту від атак і шкідників: шифрування, VPN.

Список використаних джерел:

1.Wireless network security / T. Radzik. - Springer, 2018. - 364 p.

2.Wi-Fi security and network management: A practical guide to implementing effective enterprise wireless security / S. Anandarajah, C. Jin. - Packt Publishing Ltd., 2017. - 310 p.

3.Y. Xiao, X. S. Shen, M. Li. - Springer, 2019. - 264 p.

4.Machine learning for wireless networks with artificial intelligence: Principles, challenges and opportunities / D. K. Kim, D. H. Lee, Y. Choi. - Wiley, 2019. - 304 p.

УДК 006.065.3:006.015.8]:657.6

# АНАЛІЗ НАЯВНИХ МЕТОДІВ АУДИТУ ФІЗИЧНИХ ОБ'ЄКТІВ ТА БЕЗПЕКИ ІНФРАСТРУКТУРИ

Пашкова А.В.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського, м. Харків, Україна
тел. +38(099) 044-75-12, e-mail: anhelina.pashkova@nure.ua.

This work is devoted to the analysis of known methods for auditing physical security and infrastructure security. An audit of a physical facility is one of the first mandatory items when setting up a company's physical office. There are many different standards and the question is which one is better to choose. Therefore, an analysis of standards such as ISO / IEC 27002, ITAF, CIP-006 and NIST SP 800-53 has been carried out to find the most suitable one.

Проведення аудиту в компаніях має велике значення, оскільки це дозволяє переконатися у правильності та достовірності фінансової звітності, а також ефективності внутрішнього контролю та управління ризиками. Перше, з чого бажано починати при наявності фізичного офісу компанії, так це фізична безпека та безпека інфраструктури. Тому починати аудит слід саме з фізичної безпеки об'єкту, але стає питання: за яким саме стандартом проводити даний захід.

У роботі проведено аналіз стандарту Асоціації аудиту і контролю інформаційних систем, а саме ITAF (IT Audit Framework), який являє собою вичерпну еталонну модель використання кращих практик, яка встановлює стандарти, що описують ролі та обов'язки фахівців з аудиту, вимоги до проведення аудиту та звітності, методики планування, проведення та звітності за результатами аудиту. Однак після аналізу даного документу, було виявлено, що використання ITAF має багато переваг для організацій, які прагнуть підвищити рівень безпеки своїх інформаційних технологій та покращити якість своїх процесів. Однак ITAF не має достатньої документації для проведення аудиту фізичного об'єкта.

Проаналізовано також стандарт CIP-006 (Critical Infrastructure Protection – Physical Security) від North American Electric Reliability Corporation, який включає вимоги до підготовки та реагування на надзвичайні ситуації, контролю доступу, відеоспостереження та навчання персоналу. Мета CIP-006 – забезпечення захисту критичної інфраструктури від фізичних загроз та забезпечити безперервну роботу систем. Даний стандарт непогано описує фізичний захист об'єкту, але описує дуже докладно сам процес доступу, що не задовольняє цілям даної роботи.

Далі розглянуто міжнародно відомі стандарти ISO/IEC 27002 та NIST SP 800-53, описання проведено одночасно через схожість вимог щодо впровадження аудиту. Наприклад у NIST SP 800-53 є такі вимоги, як

конкретизація доступу без супроводу або посилення охорони в місцях де немає відеоспостереження. У стандарті ISO/IEC 27002 не окреслені дані можливості, тому доцільним буде додати дані пункти. Також цікавими є вимоги окремих вестибюлів або альтернативного робоче місця, що особливо актуально в Україні в даний час. Останнє, було додане, зі стандарту NIST SP 800-53, маркування компонентів. У ISO/IEC 27002 в розділі «Управління ресурсами СУІБ» є пункт про маркування, але він відноситься тільки до інформації, а не до апаратних компонентів. Щодо схожих пунктів, то до них можна віднести наявність фізичних бар'єрів, захист кабелів, окремі зони для транспортування/доставки та інше. Присутні вимоги, які через складнощі перекладу одразу не зрозумілі, поки не будуть розглянуті пояснення. Наприклад пункт корпусів, що замикаються, але при пояснені визначається, що це схоже на безпеку кабельних мереж у ISO/IEC 27002. Стосовно відсутніх пунктів у NIST SP 800-53 то це визначення периметру фізичної безпеки, наявність видимої ідентифікації персоналу, обмеження використання обладнання для запису у зонах безпеки, встановлення захисту від блискавки та інше.

Таким чином був проведений аналіз серед таких стандартів як ISO/IEC 27002, ITAF, CIP-006 та NIST SP 800-53. З цього можна зробити висновок, що у ITAF взагалі недостатньо вимог для проведення аудиту фізичного доступу об'єкту; стандарт CIP-006 має іншу мету, яка відрізняється від поставленої в даній роботі. Щодо NIST SP 800-53, то це непогана альтернатива стандарту ISO/IEC 27002, але являє собою більш грубий аналог ISO/IEC 27002. Тому було вирішено додати деякі вимоги з NIST SP 800-53, щоб покращити процес аудиту. Що стосується самого ISO/IEC 27002, то це найкращій варіант для обраної задачі, який має міжнародне визнання та який дуже поширений на території України.

Список використаних джерел:

1. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls. – URL: https://www.iso.org/standard/75652.html (дата звернення: 01.04.2023).

2. Wilbur L. Ross, Jr. (2020) NIST Secretary Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

УДК 004.056:004.6

# ВИЗНАЧЕННЯ ТА ОСОБЛИВОСТІ ТЕХНОЛОГІЇ БЛОКЧЕЙН У СУЧАСНОМУ СВІТІ

Поліщук В.Г.
Науковий керівник – к.т.н., доцент Куля Ю. Е.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
тел. +38(093) 648-49-05, e-mail: viacheslav.polishchuk@nure.ua.

This work is focused on the blockchain technology, which provides secure data storage and transmission in a decentralized network based on a sequence of connected blocks. The security and reliability of data in the blockchain are ensured by cryptographic functions that guarantee the integrity and immutability of previously recorded information. The text also discusses the decentralized nature of the blockchain and the consensus principle, which allows for data management without a central authority and involves all network participants in the verification and confirmation of new data. The role of cryptographic algorithms in securing data and the importance of network nodes for maintaining a continuously available ecosystem are also highlighted.

Блокчейн - це технологія зберігання та передачі даних в децентралізованій мережі, що базується на послідовному зв'язку блоків. Кожен блок містить унікальний хеш, який відображає весь блок та його вміст, а також хеш попереднього блоку, що підтверджує послідовність блоків та їх зв'язок між собою. Блокчейн забезпечує високу безпеку та надійність даних завдяки використанню криптографічних функцій, які гарантують цілісність та недоступність для зміни або видалення даних, що раніше було записано у блокчейні. Структура блокчейна складається з ланцюжка блоків, кожен з яких представляє собою окрему частину інформації, яка додається до бази даних. Кожен блок має свій унікальний ідентифікатор та інформацію про попередній блок, що формує ланцюг блоків. Інформація в кожному блоку також містить дані про транзакції, дату та час, та інші додаткові дані, що підтверджують правильність блоку. Оскільки блоки пов'язані між собою, записи не можуть бути вилучені, змінені, або відредаговані, так як це призведе до порушення структури блокчейна [1]. Блокчейн працює за принципом децентралізації та консенсусу, тобто він забезпечує зберігання та передачу даних без посередництва центрального органу, а керування мережею відбувається за рахунок взаємодії всіх її учасників. Коли нові дані готові до додавання в блокчейн, вони транслюються всім учасникам мережі. Кожен учасник може взяти участь у процесі перевірки та підтвердження правильності цих даних, використовуючи свої обчислювальні ресурси та криптографічні алгоритми. Якщо більшість учасників підтверджує правильність даних, вони додаються

до нового блоку, який потім підключається до попереднього блоку за допомогою хеш-суми [2].

Щоб перевірити стан блокчейн-мережі особисто, користувач повинен завантажити спеціальне програмне забезпечення. Після установки програми і її запуску на комп'ютері користувача, вона взаємодіє з екземплярами мережі на інших комп'ютерах з метою завантаження або скачування інформації, наприклад інформація про транзакції або блоки. Новий користувач завантажує блок, щоб переконається в тому, що він був створений в рамках правил системи, і передає цю інформацію іншим вузлам мережі. Таким чином виходить екосистема, яка може складатися з сотень, тисяч або десятків тисяч об'єктів, які запускають і синхронізуються з однієї і тієї ж копії бази даних. Такі об’єкти називаються вузли або ноди. Це робить мережу цілодобово доступною. Цілісність блокчейну підривається якщо записати помилкову інформація про фінансові операції. Так як у розподіленій системі відсутній адміністратор або керівник, який міг би підтримувати роботу мережі. Для того щоб дати гарантію того, що всі учасники будуть діяти чесно, було запропоновано використання алгоритму консенсусу. Алгоритм консенсусу в блокчейні являє собою набір певних математичних правил і функцій, які дозволяють досягти згоди між усіма учасниками і забезпечити працездатність мережі [3]. Технологія блокчейн може застосовуватися до широкого кола підприємств і може бути використана у різних випадках. Незалежно від контексту, мережа блокчейн буде побудована на певному протоколі, який визначає правила роботи системи. Усі частини системи та учасники мережі повинні дотримуватись цих правил. Алгоритм консенсусу визначає, які заходи необхідно вжити для дотримання цих правил і отримання бажаних результатів. У контексті блокчейну, алгоритм консенсусу відповідає за валідацію транзакцій та блоків.

Список використаних джерел:

1. Consensus Algorithms: The Root Of The Blockchain Technology. https://medium.com/@malcoded/consensus-algorithms-the-root-of-the-blockchain-technology-24b0a305dbec

2. How Does a Blockchain Work? A Comprehensive Guide https://www.freecodecamp.org/news/how-does-a-blockchain-work-explained-for-beginners/

3. The Ultimate Guide to Understanding Blockchain Consensus Algorithms https://medium.com/swlh/the-ultimate-guide-to-understanding-blockchain-consensus-algorithms-cfe2b107d2c9

УДК 004.056:004.6

# БЛОКЧЕЙН ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ЦИФРОВОМУ СВІТІ

Поліщук В.Г.
Науковий керівник – к.т.н., доцент Куля Ю. Е.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
тел. +38(093) 648-49-05, e-mail: viacheslav.polishchuk@nure.ua.

This work is focused on the importance of security in blockchain technology, highlighting its decentralized nature and resistance to cyberattacks. The text explains the key concepts of consensus and immutability, which play crucial roles in ensuring data integrity and transaction reliability. Additionally, the role of cryptography, specifically hashing, is discussed as an essential element in maintaining the security of data within blockchain technology. The combination of these features contributes to the overall security and dependability of blockchain systems.

Безпека є одним з ключових аспектів технології блокчейн, оскільки вона забезпечує надійність системи і захист від можливих атак. Оскільки блокчейн мережа є розподіленою і децентралізованою, вона має покращену стійкість до кібератак та має високу надійність.

Блокчейни використовують різні механізми безпеки, такі як передові криптографічні методи, математичні моделі поведінки та прийняття рішень. Найважливішими функціями для забезпечення безпеки блокчейну є концепції консенсусу та незмінності. Консенсус забезпечує здатність вузлів у мережі узгоджувати справжній стан мережі та достовірність транзакцій, і його досягнення залежить від алгоритмів консенсусу. Незмінність дозволяє блокчейну уникнути змін у підтверджених транзакціях, що забезпечує цілісність даних та записаних транзакцій. Поєднання цих функцій є основою безпеки даних у блокчейні, яке забезпечує дотримання системних правил та узгодження всіх сторін з поточним станом мережі. Кожен новий блок перевіряється перед його додаванням до блокчейну, що забезпечує цілісність та безпеку даних у блокчейн технології [1].

Блокчейни в значній мірі покладаються на криптографію для забезпечення безпеки даних. Однією з надзвичайно важливих криптографічних функцій у цьому контексті є хешування. Хешування – це процес, при якому алгоритм, відомий як хеш-функція, отримує вхідні дані будь-якого розміру і повертає певний висновок, що містить значення фіксованої довжини.

Незалежно від розміру вхідних даних, вихід завжди має однакову довжину. Якщо вхід зміниться, результат буде зовсім іншим. Однак, якщо вхідні дані не змінюються, отриманий хеш завжди однаковий, незалежно від

того, як часто виконувалася хеш-функція. Наприклад, якшо алгоритмом SHA-256, який використовується у біткойні, захешувати дві майже однакові фрази змінивши тільки регістр першої літери, то в результаті буде отримано зовсім різні результати [2].

У блокчейнах хеші використовуються як унікальний ідентифікатор кожного блоку даних. Кожен блок містить хеш попереднього блоку, тому їх можна зв'язати в один ланцюжок. Крім того, хеш кожного блоку залежить від даних, що містяться в цьому блоку, що означає, що будь-яка зміна даних у блоку призведе до зміни його хешу. Таким чином, хеш-ідентифікатори кожного блоку базуються на даних, які він містить, та хеші попередніх блоків, що дозволяє забезпечити надійність та незмінність всього блокчейну [3].

Окрім захисту та запису транзакцій у регістри, криптографія також відіграє роль у захисті гаманців, що використовуються для зберігання криптовалют. Відкритий та приватний парні ключі, що дозволяють користувачам отримувати та надсилати платежі, створюються за допомогою асиметричного шифрування. Відкриті ключі використовуються для генерації цифрових підписів транзакцій, що дозволяє аутентифікувати право власності. Природа асиметричної криптографії не дозволяє нікому, крім власника приватного ключа, отримати доступ до коштів, що зберігаються в гаманці, тому ці кошти зберігаються в безпеці, доки власник не вирішить їх витратити.

Отже, блокчейн технології мають потенціал вирішувати проблеми безпеки в цифрових транзакціях та забезпечувати високий рівень захисту даних. Завдяки своїй децентралізованій структурі та криптографічним методам захисту, блокчейн може захистити транзакції від змін та фальсифікації даних.

Список використаних джерел:

1. Ensuring data security in the blockchain: principles and techniques https://medium.com/coinmonks/data-security-in-blockchain-principles-and-techniques-dc51e5b5c5a5
2. Cryptography in blockchain technology: how it works https://www.coindesk.com/learn/what-is-cryptography
3. Hashing in Blockchain: Basics and Application Examples https://www.toptal.com/bitcoin/what-is-hash-function

УДК 004.056:004.6

# БЛОКЧЕЙН, ЯК ЗАСІБ ДЛЯ ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ У СУЧАСНОМУ СВІТІ

Поліщук В.Г.
Науковий керівник – к.т.н., доцент Куля Ю. Е.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
тел. +38(093) 648-49-05, e-mail: viacheslav.polishchuk@nure.ua.

This work is devoted to the consideration of the potential of blockchain technology in creating a secure and efficient digital identification system. The decentralized nature of blockchain ensures secure data storage and exchange, as well as reduced transaction costs. The technology can address the challenges of traditional identification systems by storing data in a tamper-proof distributed ledger, thereby ensuring the protection and privacy of personal information. The application of blockchain in digital identity management and document verification holds significant potential for a more secure future.

Технологія блокчейн, може бути використана для створення безпечної та ефективної системи цифрової ідентифікації. Однією з головних переваг технології блокчейн є її децентралізований характер. Блокчейн забезпечує збереження та обмін даними між користувачами, які можуть перевіряти автентичність інформації без посередництва третіх осіб. Це дозволяє знизити вартість проведення транзакцій та забезпечує високий рівень безпеки [1].

Однією з головних проблем традиційної ідентифікації є збереження та обробка персональних даних. Технологія блокчейн може розв'язати цю проблему, оскільки вона забезпечує збереження даних у розподіленому реєстрі, що не може бути змінено або видалено без попереднього погодження всіх учасників мережі. Це забезпечує надійний захист даних та їхню безпеку, а також унеможливлює несанкціонований доступ до них.

Управління цифровою ідентифікацією та перевірка документів є одним з найбільш перспективних напрямків використання технології блокчейн. Це обумовлено тим, що у минулому мільйони людей по всьому світу стали жертвами витоків персональних даних. У зв'язку з цим, на сьогодні існує нагальна потреба у більш безпечних методах зберігання, передачі та перевірки особистої інформації. Блокчейн технології є відповідним рішенням для вирішення цієї проблеми, оскільки вони забезпечують надійний захист даних та їх безпеку, що робить їх відмінним варіантом порівняно з централізованими базами даних. Тому використання технології блокчейн у системах управління цифровою ідентифікацією та перевірки документів має великий потенціал і є важливим кроком до більш безпечного світу [2].

Коли файли записуються в блокчейн, їх достовірність гарантується за допомогою мережі вузлів, які підтримують систему. Це означає, що кожен запис в блокчейн підтверджується користувачами, що гарантує достовірність інформації. В такій системі вузли можуть виконувати роль органів влади чи державних установ, що затверджують цифрову документацію, де кожен вузол має право голосувати і підтверджувати правильність даних. Це забезпечує ще більшу достовірність інформації, оскільки файли в кінцевому підсумку можуть бути використані так само, як і офіційні документи, але з вищим рівнем безпеки [3].

Система цифрової ідентифікації, заснована на блокчейні, дозволяє аутентифікувати цифрові дані без необхідності прямого обміну інформацією між сторонами. Для цього застосовуються криптографічні методи, такі як хеш-функції або цифрові підписи. Будь-який документ може бути перетворений в хеш, який містить всю інформацію, що використовувалась для його створення, виступаючи в ролі цифрового відбитка пальця. Урядові установи та інші довірені організації можуть надавати послугу створення цифрових підписів для надання документу юридичної сили. Така система є відповідним рішенням для підвищення безпеки зберігання, передачі та перевірки особистої інформації, що є особливо актуальним у сучасному світі, де мільярди людей щороку стикаються з витоком їх персональних даних.

Одним із можливих сценаріїв використання технології блокчейн як засобу цифрової ідентифікації може бути передача документу в уповноважений орган для створення унікального цифрового відбитку. Наступним етапом є створення цифрового підпису, який гарантує дійсність хешу, який виступає в якості офіційного документа фізичної особи. Такий підхід дозволяє забезпечити високий рівень безпеки та достовірності інформації, знижуючи ризик її втрати або зловживання. Крім того, цей процес можуть здійснювати не лише урядові установи, але й інші довірені організації, що дозволяє підвищити ефективність та швидкість роботи системи.

Список використаних джерел:

1. Digital Identity Management with Blockchain https://www.researchgate.net/publication/326703726_Digital_Identity_Management_with_Blockchain

2. Blockchain-based Solutions for Personal Data Security https://www.sciencedirect.com/science/article/pii/S1877050919310861

3. Blockchain for Digital Identity: A Comprehensive Review https://ieeexplore.ieee.org/abstract/document/8767713

УДК 004.6:004.056

# РОЗПОДІЛЕНІ ТЕХНОЛОГІЇ ОБЛІКУ

Зражевець К.П.
Науковий керівник – к.т.н., доцент Куля Ю.Е.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
тел. +38(050) 100-20-37, e-mail: kyrylo.zrazhevets@nure.ua

This work discusses various DLTs including blockchain, IOTA's Tangle, Hashgraph, and Holochain. Tangle offers a scalable, high-speed transaction system without the need for miners, while Hashgraph achieves high throughput and reliability through a virtual voting-based consensus algorithm. Holochain, with its innovative architecture and data storage approach, aims to create a scalable, energy-efficient, and decentralized infrastructure for developing a variety of applications and services. Finally, Radix seeks to address scaling and throughput issues inherent in traditional blockchain technologies by utilizing a temporal acyclic graph combined with a commit-based consensus algorithm.

Розподілені технології обліку – це сімейство технологій, які дозволяють створювати та управляти децентралізованими базами даних. Блокчейн є одним з видів DLT, що використовує ланцюг блоків для збереження інформації. Інші види DLT включають протоколи, як-от IOTA, Hashgraph та Holochain.

IOTA використовує унікальний тип DLT, відомий як Tangle. Tangle - це ациклічний спрямований граф, який дозволяє забезпечити масштабування та високу швидкість транзакцій без потреби в майнерах. Замість блоків, Tangle використовує взаємопов'язані транзакції, які перевіряються іншими транзакціями. Ця структура дозволяє зменшити витрати на обробку транзакцій та забезпечити високу пропускну здатність, особливо актуально для інтернету речей [1].

Hashgraph є альтернативною DLT, яка використовує консенсусний алгоритм, заснований на віртуальному голосуванні, замість майнінгу або стейкінгу. Hashgraph використовує ациклічний спрямований граф для зберігання інформації та забезпечення узгодження в мережі. Цей підхід дозволяє досягти високої пропускної здатності та надійності без великих витрат на енергію, які властиві традиційному майнінгу [2].

Holochain – це інноваційна DLT, яка відрізняється від блокчейну за своєю архітектурою та підходами до зберігання даних. Вона використовує розподілений граф, замість ланцюжка блоків, і дозволяє користувачам мати власні незалежні ланцюги, які синхронізуються з іншими ланцюгами за потреби. Holochain покликана створити масштабовану, енергоефективну та децентралізовану інфраструктуру для розробки різноманітних додатків та сервісів [3].

Radix є ще одним прикладом DLT, який намагається вирішити проблеми масштабування та пропускної здатності, властиві традиційним блокчейн-технологіям. Radix використовує темпоральний ациклічний граф та комбінує його з консенсусним алгоритмом, заснованим на коміті. Це дозволяє досягти високої швидкості транзакцій та зменшити затримки в обробці транзакцій. Окрім того, Radix пропонує власну платформу для смарт-контрактів, яка може бути використана для розробки децентралізованих додатків.

Конфіденційні розподілені технології обліку – це сімейство DLT, які фокусуються на забезпеченні конфіденційності та приватності. Ці технології використовують криптографічні методи, такі як нуль-довідкові докази (Zero-Knowledge Proofs) або гомоморфні шифрування, для захисту даних та забезпечення приватності користувачів. Прикладами є Zcash, Monero та Beam, які розроблені з метою забезпечення анонімності транзакцій та захисту фінансової приватності користувачів.

Розподілені технології обліку продовжують розвиватися та пропонувати нові та інноваційні підходи до зберігання та обробки даних. Вони забезпечують можливості для реалізації децентралізованих, масштабованих та безпечних систем, які можуть відповідати різним потребам та вимогам ринку. У майбутньому можна очікувати появу нових видів DLT, які зосереджуються на вирішенні конкретних проблем, таких як енергоефективність, конфіденційність, швидкість обробки транзакцій та інше.

Одним з ключових аспектів розвитку розподілених технологій обліку є можливість взаємодії та інтеграції різних DLT. Це включає розробку механізмів для безпечного та ефективного обміну даними та активами між різними блокчейн-платформами та DLT. Інтероперабельність може допомогти досягти більшої адаптації технології та поширення її використання в різних галузях та серед користувачів.

Список використаних джерел:

1. Popov, S. (2018). The Tangle. IOTA Foundation. https://www.iota.org/research-papers/the-tangle

2. Baird, L. (2016). The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance. Swirlds. https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

3. Brock, A., Harris-Braun, E., & Luck, N. (2018). Holochain: Scalable, Agent-Centric, Distributed Computing. Holochain. https://files.holochain.org/holochain.pdf

УДК 004.6:004.056

# ВАЖЛИВІСТЬ БЛОКЧЕЙН-ТЕХНОЛОГІЙ У СУЧАСНОМУ СВІТІ

Зражевець К.П.
Науковий керівник – к.т.н., доцент Куля Ю.Е.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Пововського,
м. Харків, Україна
тел. +38(050) 100-20-37, e-mail: kyrylo.zrazhevets@nure.ua

This work is an exploration of blockchain technology as a unique type of database that allows for the addition of information but prevents editing, altering, or deletion. It highlights the structure of a blockchain as a chain of interconnected blocks, as well as the decentralized nature of the system. The text also discusses smart contracts, which are self-executing programs embedded within the blockchain, and their potential for automation, error reduction, and cost savings. Additionally, the paper addresses the challenges of scalability and energy efficiency in blockchain technology, noting various solutions such as layering, sharding, sidechains, and alternative consensus algorithms aimed at improving network performance and environmental sustainability.

Блокчейн являє собою особливий вид бази даних, до якої можна вносити інформацію, але не можна видаляти чи змінювати. Структура блокчейну являє собою ланцюг із блоків з інформацією, що містять у собі посилання на попередні блоки, та також деяку інформацію про транзакції, часові мітки та інші метадані, що використовуються для підтвердження його достовірності. Через те що усі блоки взаємопов’язані між собою, записана інформація не може бути відредагована, змінена чи видалена, бо у такому випадку усі попередні блоки стануть недійсними.

Оскільки блокчейн підтримується багатьма пристроями, він функціонує як децентралізована база даних. Це означає, що кожен вузол зберігає у собі копію даних блокчейну та виконує взаємодію з іншими вузлами, для того щоб підтверджувати збіг інформації у блоках.

Блокчейн забезпечує транспарентність, оскільки всі транзакції та інформація доступні для перегляду всіма учасниками мережі. Це створює відкрите та прозоре середовище, яке важко підробити або змінити. Водночас, блокчейн може забезпечувати анонімність, оскільки ідентифікаційні дані користувачів замінюються на унікальні криптографічні адреси.

Смарт-контракти  це самовиконувальні програми, які автоматично виконують умови контракту між сторонами без необхідності додаткового втручання. Вони вбудовані в блокчейн та виконуються автоматично після виконання певних умов. Смарт-контракти можуть використовуватися для автоматизації процесів, зменшення відсотка людської помилки та зниження вартості та часу виконання операцій [1].

Однією з проблем, яка виникає в контексті блокчейну, є масштабованість, оскільки розростання мережі може призвести до зниження швидкості обробки транзакцій. Різні технологічні рішення, такі як шарування (Layer 2), шардинг (sharding) та створення бічних ланцюгів (sidechains), розроблені для розв'язання проблеми масштабованості та підвищення ефективності мережі [2].

Енергоефективність стає дедалі більш актуальною темою у світі блокчейну. Традиційний алгоритм консенсусу Proof of Work (PoW) вимагає значної кількості електроенергії для підтримки мережі, що викликає стурбованість щодо екологічного впливу. Відповідно, розробляються альтернативні алгоритми консенсусу, такі як Proof of Stake (PoS), Delegated Proof of Stake (DPoS) та Proof of Authority (PoA), які спрямовані на зниження енергоспоживання та підвищення екологічної стійкості блокчейн-технологій [3].

Оскільки на ринку з'являється все більше блокчейн-проектів та мереж, забезпечення взаємодії між ними стає однією з ключових проблем. Кросланцюгові рішення, такі як атомарні обміни (atomic swaps), мости блокчейнів (blockchain bridges) та інтероперабельні протоколи (наприклад, Polkadot або Cosmos), спрямовані на спрощення обміну інформації та цінностей між різними блокчейн-мережами.

Регуляція блокчейн-технологій є актуальною проблемою, оскільки уряди та регулятори починають приділяти увагу забезпеченню легітимності цих технологій та їх використання. Стандартизація практик, термінології та процедур сприятиме розвитку та адаптації блокчейну в різних сферах діяльності та індустріях. Організації, такі як Enterprise Ethereum Alliance, Hyperledger Foundation та International Organization for Standardization активно працюють над створенням стандартів для блокчейн-індустрії.

Список використаних джерел:

1. Smart Contracts: The Blockchain Technology That Will Replace Lawyers. https://blockgeeks.com/guides/smart-contracts/
2. Understanding Blockchain Scalability: Layer 1, Layer 2, Sharding, and Sidechains. https://consensys.net/blog/blockchain-explained/understanding-blockchain-scalability/
3. Proof of Work vs. Proof of Stake: A Comparison. https://www.investopedia.com/tech/proof-work-vs-proof-stake-cryptocurrency/

УДК 004.056:004.6

# БЕЗПЕЧНІСТЬ ЗБЕРІГАННЯ КЛЮЧІВ У EVM-БЛОКЧЕЙНАХ

Зражевець К.П.
Науковий керівник – к.т.н., доцент Куля Ю.Е.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
тел. +38(050) 100-20-37, e-mail: kyrylo.zrazhevets@nure.ua

This work is an overview of various solutions for storing and securing private keys in EVM-compatible blockchains. It discusses hardware wallets, which are physical devices storing private keys in a secure environment, hot wallets that store keys on internet-connected devices, and cold wallets that store keys on devices without constant internet connection. The text also covers multi-signature technology, which requires signatures from multiple parties to execute a transaction, and protocol-level security mechanisms that utilize asymmetric encryption or distributed key storage. Additionally, the importance of backup and restoration of keys, different access levels, two-factor authentication, regular software updates, and risk management is addressed.

В EVM-сумісних блокчейнів можуть бути використані різні рішення для збереження та захисту приватних ключів.

1) Апаратні гаманці – фізичні пристрої, які зберігають приватні ключі в безпечному середовищі, відрізняючись від інтернет-з'єднаних пристроїв. Наприклад, Ledger Nano S та Trezor.

2) Гарячі гаманці – це програмні гаманці, які зберігають ключі на пристроях з підключенням до Інтернету, забезпечуючи швидкий доступ до коштів. Наприклад, MetaMask та MyEtherWallet.

3) Холодні гаманці – це програмні гаманці, які зберігають ключі на пристроях без постійного з'єднання до Інтернету, забезпечуючи високий рівень безпеки. Наприклад, Electrum та Armory [1].

Мультипідпис – це технологія, яка вимагає підпису декількох сторін для здійснення транзакції. Це дозволяє створити додатковий рівень безпеки, оскільки зловмисникам потрібно скомпрометувати кілька приватних ключів для доступу до коштів. Такі гаманці зазвичай використовуються для спільного управління активами або корпоративних рахунків [2].

Безпека ключів на рівні протоколу: деякі EVM-сумісні блокчейни можуть використовувати вбудовані механізми безпеки для захисту приватних ключів на рівні протоколу. Це може включати рішення, які використовують асиметричне шифрування, щоб передавати ключі між учасниками мережі, або розподілене зберігання ключів, де кожен учасник мережі зберігає лише частину ключа.

Резервне копіювання та відновлення ключів: безпека приватних ключів також забезпечується шляхом створення резервних копій та можливості

відновлення в разі втрати або пошкодження пристрою. Це може включати використання мнемонічних фраз для відновлення ключів або регулярне створення резервних копій гаманця на безпечному пристрої.

Використання різних рівнів доступу: ще одним способом забезпечення безпеки приватних ключів є створення різних рівнів доступу до коштів. Наприклад, можна створити гаманець з обмеженим доступом для повсякденних витрат, а гаманець з повним доступом використовувати для зберігання великих сум коштів або управління корпоративними активами. Такий підхід дозволяє зменшити ризик втрати великих сум коштів у разі компрометації одного з гаманців, оскільки доступ до основних активів обмежений [3]. Двофакторна автентифікація: для додаткової безпеки приватних ключів, деякі гаманці та платформи можуть пропонувати двофакторну автентифікацію. Найпопулярніші методи 2FA включають одноразові паролі (OTP), які надсилаються через SMS або генеруються спеціальними додатками, та біометричні методи, такі як відбитки пальців чи розпізнавання обличчя.

Регулярне оновлення програмного забезпечення: щоб забезпечити найвищий рівень безпеки для приватних ключів, важливо регулярно оновлювати програмне забезпечення гаманця та пристроїв, на яких він встановлений. Виробники апаратних та програмних гаманців часто випускають оновлення, які включають покращення безпеки та виправлення вразливостей. Слідкування за оновленнями і своєчасне їх встановлення може допомогти запобігти можливим атакам.

Управління ризиками: крім того, важливо розуміти та управляти ризиками, пов'язаними зі зберіганням приватних ключів. Це може включати розподіл активів між декількома гаманцями, використання різних методів зберігання ключів та регулярне перевіряння своїх рішень з погляду безпеки.

Список використаних джерел:

1. ConsenSys: EVM-Compatible Blockchain Security Features https://consensys.net/blockchain-use-cases/evm-compatible-blockchain-security-features/

2. CoinCentral: What is Multisig? https://coincentral.com/what-is-multisig/

3. Crypto Security Best Practices https://www.coindesk.com/learn/bitcoin-101/crypto-security-best-practices

УДК 004.056:004.773.3

# ПІДХІД ЦИФРОВОГО КРИМІНАЛІСТИЧНОГО АНАЛІЗУ ПОВІДОМЛЕНЬ ЕЛЕКТРОННОЇ ПОШТИ

Шедін Д.А.
Науковий керівник – к.т.н., доцент Снігуров А.В.
Харківський національний університет радіоелектроніки,
каф. Інфокомунікаційної інженерії імені В.В. Поповського, м. Харків,
Україна
тел. +38(099) 533-26-57, e-mail: dmytro.shedin@nure.ua.

The increasing prevalence of cyber threats and phishing attacks in our daily lives has made it more crucial than ever to be vigilant about the emails we receive. Even though email services come with built-in security features, they are not always reliable. Analyzing the sender's domain and email headers is an additional way that helps clients quickly identify potential vulnerabilities and take appropriate action. The currently available external tools require more effort from the user to collect this information in one place and do not always show data in an easy-to-read format. My user-friendly and simple-to-install browser extension is the solution that allows to get this information without leaving the email client.

У сучасну епоху цифрових комунікацій, коли електронна пошта є невіддільною частиною нашого повсякденного життя, загрози, що поширюються нею, залишаються значною небезпекою, зростаючи майже на 30% щорічно [1]. Більшість поштових клієнтів мають вбудовані фільтри спаму, які автоматично визначають і переміщують сумнівні листи в спеціальний розділ або видаляють їх. Однак ці методи не завжди ефективні для виявлення складніших загроз, таких як ексфільтрація даних, підробка, шкідливе програмне забезпечення, фішинг та інші. Таким чином, зростає потреба в додаткових рішеннях, які можуть допомогти користувачам визначити потенційно ризиковані електронні листи.

Під час проведення досліджень при написанні кваліфікаційної роботи бакалавра було розроблене розширення для браузера з інструментом, яке надає інформацію про електронне повідомлення одразу у поштовому клієнті, не покидаючи його. Крім зручності, серед інших переваг розробки можна виділити легкість встановлення (використовуючи вебмагазин браузера), безпечність (дані передаються в зашифрованому вигляді та не зберігаються), можливість інтеграції мікросервісу до інших систем (на основі REST API).

Самий підхід базується на обробці та цифровому аналізі домену відправника, заголовків повідомлення та його контенту. На рисунку 1 представлений приклад відображення результатів для тестового повідомлення.

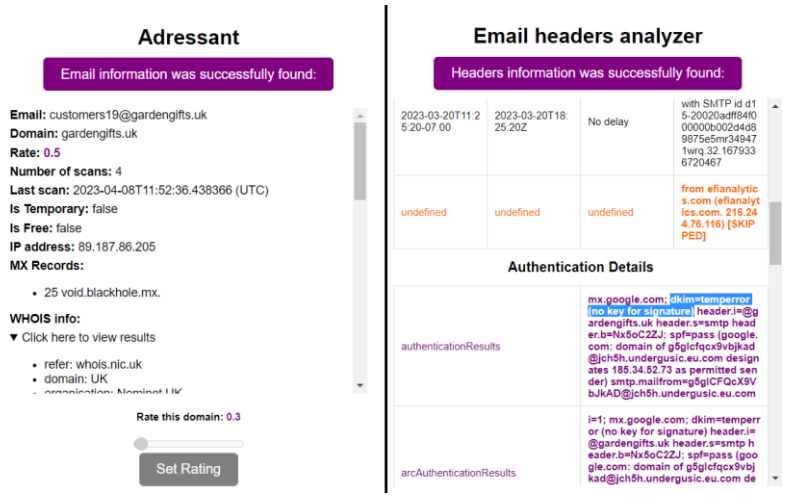



Рисунок 1 – Приклад застосування розширення

Як видно на рис. 1, інструмент складається з двох розділів: «Adressant» та «Email headers analyzer». Перший надає загальні дані про домен відправника, а саме:

- загальний рейтинг на основі досвіду користувачів;
- кількість сканувань та дата останнього;
- чи є він безплатним (тобто поштова адреса може бути вільно створена);
- чи є він тимчасовим (тобто самостійно знищується через певний час);
- IP адреса;
- MX записи (визначають сервер, відповідальний за отримання повідомлень електронної пошти від імені домену);
- WHOIS результати (реєстраційна інформація про власника домену).

Другий розділ дозволяє користувачу переглядати інформацію про:

- відправника та отримувачів;
- шлях повідомлення з моменту відправлення до його прибуття (базуючись на «Received» даних);
- результати автентифікації (DKIM, SPF, DMARC);
- деталі повідомлення та його контенту (ідентифікатори, посилання та інші)
- X-headers (додаткові нестандартні та невідсортовані заголовки).

Розширення автоматично виділяє потенційні вразливості та інші ключові деталі, тому може бути корисним як для звичайних користувачів, так і для спеціалістів з кібербезпеки та криміналістики.

Список використаних джерел:

1. ESET. (2023). ESET Threat Report T3 2022. WeLiveSecurity. https://www.welivesecurity.com/wp-content/uploads/2023/02/eset_threat_report_t32022.pdf

УДК 004.056.55:004.421.5

# ДОСЛІДЖЕННЯ ДИФЕРЕНЦІЙНИХ ВЛАСТИВОСТЕЙ МІНІ-ВЕРСІЇ АЛГОРИТМУ МУХОМОР

Скиба Є.О.
Науковий керівник – к.т.н., доц. Кобилін О.А.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Інформатики, тел.(057) 702-14-19)
Email: yevhen.skyba@nure.ua

The task of the work is the implementation of a software complex for the study of the differential properties of the mini version of the Mukhomor algorithm, and the construction of tables of differential differences for the first 16 bits of the algorithm.

Робота присвячена дослідженню показників різниць шифру Мухомор, зокрема в дослідженні диференціальних властивостей міні-версії алгоритму Мухомор, з метою визначення його стійкості до диференціального криптоаналізу. Актуальність даної теми обумовлена значенням блочних симетричних шифрів в сучасних інформаційних системах та потребою в постійному вдосконаленні алгоритмів шифрування для забезпечення максимальної стійкості до криптоаналізу. Робочою гіпотезою дослідження є те, що міні-версія алгоритму Мухомор є стійким до диференціального криптоаналізу.

На сьогоднішній день розроблено досить багато стійких блокових шифрів. Практично всі алгоритми використовують для перетворень певний набір зворотних математичних перетворень.

Характерною особливістю блокових криптоалгоритмів є той факт, що в ході своєї роботи вони роблять перетворення блоку вхідної інформації фіксованої довжини і отримують результуючий блок того ж обсягу, але недоступний для прочитання стороннім особам, які не мають ключа.

Диференційний криптоаналіз заснований на вивченні перетворення різниць між значеннями, що шифруються, на різних раундах шифрування. Як правило, застосовується операція побітового підсумовування по модулю 2, хоча існують атаки і з обчисленням різниці по модулю $2^{32}$. Є статистичною атакою, в результаті роботи пропонує список найбільш ймовірних ключів шифрування симетричного блокового шифру.

Диференційний криптоаналіз застосовується для злому DES, FEAL і деякі інші шифри, як правило, розроблені раніше початку 90-х. Кількість раундів сучасних шифрів (AES, Camellia та інших.) розраховувалося з урахуванням забезпечення стійкості, зокрема і до диференціального криптоаналізу.

При побудові зменшеної версії шифру Мухомор виникла ситуація, коли шифр містив перетворення, яке не допускає прямого масштабування. До такої операції відноситься SL-перетворення. У цю операцію

оригінальної конструкції входять шар нелінійних перетворень, що реалізується за допомогою чотирибайтових S-блоків, і подальше МДР перетворення, за допомогою якого здійснюється матричне множення байтових виходів чотирьох S-блоків (над полем GF (28)) квадратну матрицю розміру 4x4. (По суті, аналогічне перетворення виконується в шифрі Rijndael за допомогою операції MixColumns, але там при множенні використовується інший поліном.) При масштабуванні цієї операції до 16-бітної моделі вона вийде чотирибітна (в оригіналі вона 32-бітна). Можна будувати різні варіанти міні-шифру – Мухомор. У цьому випадку буде використовувалось перетворення MixColumns на весь текст, SboxAES p4 ={A,4,3,B,8,E,2,C,5,7,6,F,0,1,9,D}.

Таким чином, результати досліджень показали наступні значення максимумів повного диференціала алгоритму міні – Мухомор.

| Міні-Мухомор | |
|---|---|
| S-блок $\delta = 8$ | S-блок $\delta = 4$ |
| 65536 | 65536 |
| 14187,5 | 5770,24 |
| 2496,32 | 1802,24 |
| 542,72 | 125,53 |
| 46,28 | 29,7 |
| 19,48 | 18,88 |

Список використаних джерел:

1. Долгов В.І. Дослідження криптографічних властивостей нелінійних вузлів заміни зменшених версій деяких шифрів / В.І. Долгов, О.О. Кузнєцов, І.В. Лисицька, Р.В. Сергієнко, О.І. Олешко // Прикладна радіоелектроніка. – Харків: ХНУРЕ. – 2009. – Т.8, №3. – С.268 – 277.

2. Горбенко І.Д. Перспективний блоковий симетричний шифр «Мухомор». Основні положення та специфікація / І.Д. Горбенко, В.І. Долгов, Р.В. Олійников та ін. // Прикладна радіоелектроніка. – 2007. – Т. 6, № 2. – С. 147-157.

3. Олійников Р.В. Дослідження диференційних властивостей підстановок / Р.В. Олійников, І.В. Лисицька, О.В. Широков, К.Є. Лисицький // Компьютерні науки та технології: сб. наук. тр. Першої міжнародної науково-технічної конференції - Ч. І. – Б., 2009. - С. 59-63.

4. Олійников Р.В. Диференційні властивості випадкових підстановок /Олешко О.І., Лисицький К. Є., Тєвяшев О.Д.// Прикладна радіоелектроніка., 2010. – Т.9. – № 3. – С. 326–333.

УДК 004.056.53

# ПРОПОЗИЦІЇ ЩОДО ВИКОРИСТАННЯ SPLUNK ДЛЯ АНАЛІЗУ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

Вакуленко Д. В.
Науковий керівник – к.т.н., доцент Добринін І.С.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
тел. +380500002423, e-mail: danyil.vakulenko@nure.ua.

The purpose of this work is to study the automatic retrieval of logs from a Windows server machine and transfer them to the Splunk tool. And the automation of their analysis with the help of Python was also added

This work can be used during the automation of audit in Windows machines.

Відомо, що роботи з забезпечення кібербезпеки потрібно починати з аудиту систем. Щодня у всьому світі проводяться тисячі кібератак, які можуть призвести до втрати конфіденційної інформації. Все більше хакерів отримують доступ до систем до яких вони не повинні мати доступу. Дана тенденція свідчить про те, що довіряти певні дані інтернет сервісам є небезпечно.

З метою аудиту та аналізу функціонування інформаційних систем наразі створені системи, які аналізують лог-файли систем: SIEM/SOAR та їхні похідні.

SIEM/SOAR – «SIEM» називають злиття функцій управління інформацією про безпеку (SIM), тобто процес збору, моніторингу та аналізу даних з комп'ютерних журналів (звітів), які автоматично генеруються, та управління подіями безпеки (SEM) – процес централізації даних журналу комп'ютера з декількох джерел (систем, кінцевих точок, додатків і служб) для поліпшення виявлення інцидентів безпеки та управління цими подіями за допомогою формалізованого процесу реагування. Розвиток SIEM шляхом додавання автоматизації різних кейсів породило новий клас систем – SOAR. Залежно від того, що лежить в основі цієї системи, вона може мати різні назви: дії по забезпеченню безпеки, аналітика і звітність – Security Operations, Analytics and Reporting (SOAR) чи оркестрації подій безпеки та автоматичне реагування – Security Orchestration, and Automated Response. SOAR є спеціальним інструментом для узагальнення відомостей про загрози безпеки, які подаються з різних джерел, з подальшим аналізом цих даних [1].

У доповіді розглядається інформаційна система Splunk, яка може бути використана як SIEM (Security Information and Event Management), так і як SOAR (Security Orchestration, Automation and Response) [2 – 3].

Перевагами використання Splunk можна вважати:

– можливість збирати та аналізувати величезну кількість різноманітних даних із різних джерел, включаючи лог-файли, мережеві пристрої та бази даних;

– надання розширеної аналітики для виявлення патернів та аномалій, що допомагає забезпечити ефективніше виявлення атак та збільшити рівень безпеки.

Пропонується забезпечити ефективне використання Splunk у декілька етапів.

1. Налаштування Splunk на сервері, що являє собою програму, яка дозволяє збирати, зберігати та аналізувати різноманітні лог-файли з різних джерел та додатків. Задля збору даних, пропонується встановити додаток Universal Forwarder, що дозволить пересилати дані до апріорі налаштованого Splunk.

2. Написання Python скриптів, які дозволятимуть виконувати автоматизацію фільтрування даних, що були зібрані на попередніх етапах. Для цього в системі Splunk передбачений спеціальний дашбоард, який надає інформацію про успішне або не успішне виконання скриптів.

3. Перевірка налаштувань надання лог-файлів.

Отже, використання Splunk може бути спрямовано на підвищення ефективності збору та аналізу лог-файлів з ЕОМ з встановленою OS Windows. Враховуючи те, що зазначена система працює за допомогою мови програмування Python [4], що є мовою програмування для роботи з великими об’ємами даних, є можливість підвищення точності прийняття рішень, щодо виявлення вразливостей.

Відзначимо, що робота зі збору лог-файлів Windows-машин за допомогою Splunk дозволяє значно полегшити моніторинг подій, зменшити час, затрачуваний на аналіз та підвищити рівень безпеки інформаційної системи на підприємстві.

Список використаних джерел:

1. Що таке SIEM/SOAR. URL: https://amind.ua/systemy-upravlinnya-inform-bezpekoyu (дата звернення 11.04.2023)

2. Документація системи Splunk. URL: https://docs.splunk.com/ Documentation/Splunk (дата звернення: 11.04.2023).

3. Splunk Universal Forwarder. URL: https://www.splunk.com/ en_us/blog/learn/splunk-universal-forwarder.html (дата звернення 11.04.2023)

4. Integrate the Splunk platform using development tools for Python. URL: https://dev.splunk.com/enterprise/docs/devtools/python (дата звернення 11.04.2023)

УДК 004.056:355.451]:004.75

# НОВІТНІ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ І КЕРОВАНИЙ ЗАХИСТ В ХМАРНІЙ ІНФРАСТРУКТУРІ

Белозьоров С. Ю.
Науковий керівник – к.т.н., проф. Марчук В.С.
Харківський національний університет радіоелектроніки, каф. ІКІ імені В.В.Поповського,
м. Харків, Україна
тел. +380(50)-301-66-25, e-mail: serhii.bielozorov@nure.ua

The presented work is devoted to the analysis of modern intrusion detection systems and managed information protection in cloud infrastructures. Google Corporation has developed Cloud IDS intrusion detection system for its GCP cloud technologies. This system provides detection of intrusion threats, malware, spyware, and command attacks on the network. Peer-to-peer traffic is mirrored and then inspected by Palo Alto Networks threat protection technologies. To act against threats detected by Cloud IDS, Google developed the Google Cloud Armor system.

Хмарні технології в останні роки стають все популярнішими: багато компаній переносять свої сервіси на cloud-сховища і використовують хмари провайдерів для розміщення критично важливої інформації. Таке рішення є максимально практичним та доступним, проте не варто забувати про можливі проблеми, з якими можна зіткнутися у процесі його використання. Хмарна інфраструктура піддається тим самим загрозам, як і традиційна фізична.

Корпорація Google для своїх хмарних технологій GCP розробила систему виявлення вторгнень Cloud IDS [1].

Cloud IDS (Cloud Intrusion Detection System) - це служба виявлення вторгнень, яка забезпечує виявлення загроз вторгнень, зловмисного та шпигунського програмного забезпечення і командних атак у мережі. Cloud IDS працює шляхом створення однорангової мережі, якою керує Google із дзеркальними віртуальними машинами. Трафік у одноранговій мережі віддзеркалюється, а потім перевіряється технологіями захисту від загроз Palo Alto Networks, щоб забезпечити розширене виявлення загроз. Є можливість віддзеркалювати весь трафік або відфільтрований трафік на основі: протоколу, діапазону IP-адрес або його напрямку.

Cloud IDS забезпечує повну видимість мережевого трафіку, дозволяючи відстежувати зв’язок між віртуальними машинами для виявлення переміщення всередині периметра. Це забезпечує інспекційний механізм, який перевіряє трафік у середині підмережі.

Cloud IDS можна також використовувати, щоб відповідати розширеним вимогам щодо виявлення загроз і відповідності існуючим стандартам.

Cloud IDS автоматично оновлює сигнатури вразливостей та антишпигунських програм без будь-якого втручання користувача, що дозволяє користувачам зосередитися на аналізі та усуненні загроз, не керуючи сигнатурами та не оновлюючи їх.

Cloud IDS щодня отримує оновлення від Palo Alto Networks та передає їх на всі існуючі кінцеві точки IDS.

В хмарній системі захисту є можливість встановлювати три рівня серйозності загроз: високий, середній і низький. Окрім того можна відключати не потрібні, з точки зору користувача, ідентифікатори загроз використовуючи прапор --threat-exceptions.

Щоб діяти проти загроз, які виявляє Cloud IDS Google розробив систему Google Cloud Armor [2].

Google Cloud Armor допомагає захистити сервіси Google Cloud від різних типів загроз, включаючи: розподілені атаки типу «відмова в обслуговуванні» (DDoS), атаки на програми, такі як міжсайтовий скриптинг (XSS) та впровадження SQL (SQLi). У Google Cloud Armor є як автоматичні засоби захисту, так і засоби захисту, які потрібно настроїти вручну.

Попередньо налаштовані правила WAF (Web Application Firewall) Google Cloud Armor – це складні правила брандмауера веб-застосунків WAF з десятками сигнатур, складені згідно галузевих стандартів з відкритим вихідним кодом.

У Google Cloud Armor є керована служба захисту програм Managed Protection.

У Google Cloud Armor також вбудовано адаптивний механізм захисту. від розподілених атак типу «відмова в обслуговуванні» (DDoS) за рахунок аналізу шаблонів трафіку серверних служб, виявляючи та попереджаючи передбачувані атаки. Правила WAF можна настроїти відповідно до потреб користувача. Адаптивний захист можна включити для кожної політики безпеки, але для цього потрібна активна підписка Managed Protection.

Список використаних джерел:

1. Google. Cloud IDS overview. https://cloud.google.com/intrusion-detection-system/docs/overview

2. Google Cloud Armor overview. https://cloud.google.com/armor/docs/cloud-armor-overview

УДК 004.056:355.451]:004.75

# БЕЗПЕКА ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ З ВИКОРИСТАННЯМ ХМАРНИХ СЕРВІСІВ

Белозьоров С. Ю.
Науковий керівник – к.т.н., проф. Марчук В.С.
Харківський національний університет радіоелектроніки, каф. ІКІ імені В.В.Поповського,
м. Харків, Україна
тел. +380(50)-301-66-25, e-mail: serhii.bielozorov@nure.ua

The presented work is devoted to the analysis of modern intrusion detection
The work is devoted to the analysis of methods of ensuring information security of telecommunication networks using cloud services. Data center security in a cloud computing environment must be multi-layered. It uses: next-generation NGFW network virtual appliances, WAF web security applications, continuous monitoring, encryption, two-factor authentication, and basic anti-virus software. It is also advisable to use IDS/IPS intrusion detection and prevention systems. One of the methods of effective protection is to use the possibilities of providing protection in the cloud services themselves.

Хмарні обчислення поступово стають однією з найпоширеніших інформаційних технологій.

І, як наслідок, спостерігається значне зростання кількості мережевих атак.

По-перше, загрозам піддаються різні програмні продукти елементів хмари, впровадження в які дозволяють зловмиснику як отримати доступ до системи, так і порушити її функціональність.

По-друге, вразливість хоча б одного елемента хмарної інфраструктури у разі проведення на неї мережевої атаки дає змогу заблокувати всю систему.

По-третє, зловмисник спроможний не тільки забезпечити собі доступ до даних, що зберігаються та оброблюються в хмарному сервісі, а й підкорити його собі таким чином, що хмара та її ресурси функціонуватимуть на користь порушника. Крім того, реалізується можливість здійснювати мережеві атаки по відношенню до конкретних користувачів. Внаслідок реалізації подібних загроз зловмисник може здійснювати такі традиційні атаки на користувачів веб-додатків, як перехоплення мережевих сесій, крадіжка паролів тощо.

Безпека центру обробки даних у середовищі хмарних обчислень має бути багаторівневою, що включає такі аспекти: контроль доступу, ідентифікація працюючого персоналу, моніторинг системи, миттєве сповіщення про вторгнення і т.д.

Щоб захистити хмару від вторгнення, вірусних програм та витоку даних, необхідно насамперед налаштувати контроль доступу. Завдання полягає в тому, щоб не просто налаштувати доступ для користувачів –

вибрати логін та пароль, а не допустити вторгнення ззовні. Для цього використовуються: мережеві віртуальні пристрої Firewall, програми захисту веб-інтерфейсу, безперервний моніторинг.

Важливими елементами захисту також є: шифрування, двофакторна автентифікація та базове антивірусне програмне забезпечення. Вони мають бути реалізовані провайдером.

Основний спосіб коректно відфільтрувати відомості та проконтролювати доступ до ресурсів – це використання багатофункціональних Firewall (брандмауерів). Сучасні Firewall наступного покоління (NGFW) відрізняються інтегрованими функціями безпеки для хмарних сервісів: наявність функції NAT/PAT, глибока перевірка пакетів з підписом поведінки.

Доцільно також використовувати системи виявлення та запобігання вторгненням IDS/IPS, спеціалізовані веб-елементи управління - правила WAF (Web Application Firewall).

Один із методів ефективного захисту - використання можливостей надання захисту у самих хмарних сервісах. У разі використання хмарних технологій PaaS та SaaS, ряд елементів безпеки може надати постачальник. У випадку IaaS (Інфраструктура як послуга) можна організувати повноцінну систему захисту і забезпечити деталізацію та вибір елементів керування захистом.

Для ефективного захисту інформації у хмарі розгортається велика кількість списків контролю доступу у всіх можливих точках входу. Основна проблема – організація управління правилами. Ці питання вирішені розробниками хмарних сервісів Amazon AWS та Microsoft Azure.

Microsoft Azure для захисту даних у хмарі може забезпечити:

• контроль доступу через групи безпеки мережі (NSG);
• балансування навантаження;
• WAF, але без великого набору керованих правил та централізованого керування ними;
• єдиний міжмережевий екран між мережею та Інтернетом;
• кілька брандмауерів на різних рівнях;
• ізоляцію мереж.

Можна також використовувати Amazon AWS. У порівнянні з Microsoft Azure Amazon AWS має більш ефективні механізми захисту, але є складним в налагоджненні і коштує більше.

Список використаних джерел:

1. Microsoft. Azure. Products. Security. Protect your enterprise from advanced threats across hybrid cloud workloads. https://azure.microsoft.com/en-us/

2. Amazon. AWS solutions. Cloud security software. https://aws.amazon.com/marketplace/solutions/security/?nc2=h_ql_mp_sol_sec

УДК 004.056:355.451]:005.7

# ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ

Гапонюк К.В.
Науковий керівник - к.т.н., с.н.с. Пшеничних С.В.
Харківській національний університет радіоелектроніки,
каф. Інфокомунікаційної інженерії ім. В.В. Поповського,
м. Харків, Україна
тел. +38(067) 355-88-54, e-mail: kateryna.haponiuk@nure.ua

One of the main aspects of security issues in the organization is considered. The threat of hacking due to lack of awareness of personnel in the field of information protection, which poses a privacy risk for the company to its employees, was analyzed.

В доповіді розглядається питання забезпечення інформаційної безпеки в офісному приміщенні. Актуальністю даної роботи є необхідність захисту конфіденційних даних, інформації та відомостей, розголошення або спотворення яких може спричинити за собою негативні наслідки для працівників та компанії в цілому.

У результаті опитування Cyber Breaches Survey за 2022 рік, було виявлено існування нестачі розуміння питань кібербезпеки серед найманого персоналу, та відсутність розуміння ефективного управління кіберризиками на рівні управління організації.

Важливо усвідомлювати, що будь-яка організація, яка покладається на цифрові технології, піддається ризику кіберінциденту [1]. Кіберзлочинці намагатимуться використати слабке місце (чи вразливість) у системі, незважаючи на те, кому ця система належить, чи розмір організації.

Більшість кіберзломів не є результатом «складних і витончених атак». Переважна більшість атак все ще базується на добре відомих методах таких як фішингові електронні листи.

Цифрова революція дає величезні переваги, але також приносить нові ризики, які ми повинні розуміти та боротися з ними, враховуючи нашу зростаючу залежність від кіберпростору.

Щоб належним чином забезпечити інформаційну безпеку організації, вона має бути інтегрована в організаційне управління ризиками та прийняття рішень, а всі бізнес-підрозділи організації мають чітко розуміти свої зобов’язання та відповідальність щодо кібербезпеки.

Наприклад:

- технічні команди повинні розуміти важливість безпеки та захисту даних і систем за допомогою відповідних засобів контролю;
- людські ресурси повинні забезпечити кібербезпеку протягом усього життєвого циклу персоналу з відповідними вказівками, політикою та підтримкою для робочої сили;

- комунікаційні та маркетингові команди, які керують даними та маркетинговими службами, повинні співпрацювати з управлінням, щоб підготуватися до спілкування з клієнтами та пресою, щоб вони були готові до ряду інцидентів (таких як втрата операційних можливостей або порушення даних);
- юридичні команди повинні усвідомлювати важливість обробки та захисту контрактів і юридичних документів, щоб вони не потрапили в руки конкурентів, а також повинні гарантувати ризики відповідальності, що виникають через потенційні кіберінциденти під час операцій;
- команди з кібербезпеки повинні розробляти та впроваджувати політики, які захищають дані співробітників і клієнтів від несанкціонованого доступу;
- команди із закупівель повинні враховувати кіберризики під час переговорів із потенційними постачальниками послуг, від програмного забезпечення та апаратного забезпечення до наймання підрядника, і включати управління кіберризиками в управління контрактами в ланцюжку постачання.

Також для забезпечення надійного збереження інформації, управління компанії має визнавати, що злочинець (який може варіюватися від незадоволеного працівника до особи, яка фінансується державою і має намір викрасти інтелектуальну власність) зможе отримати доступ до системи.

Це означає, що потрібно мати засоби контролю, щоб мінімізувати шкоду, яку вони можуть завдати, опинившись усередині. Це можна забезпечити шляхом обмеження їх доступу до послуг та інформації. Моніторинг і ведення журналів є ключовими для можливості якомога швидше виявити ознаки зловмисної діяльності та обмежити шкоду, яку вони можуть завдати.

Список використаних джерел:

1. Інструменти кібербезпеки для плат | Керівництво | Головна сторінка. URL: https://www.ncsc.gov.uk/collection/board-toolkit (дата звернення 09.04.2023)

УДК 004.77:004.056

# РОЗРОБКА ПРОГРАМНОГО МОДУЛЯ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ВИКОРИСТАННІ МЕСЕНДЖЕРА

Майба М.А.
Науковий керівник – д.т.н., проф. Єременко О.С.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
тел. +38(099) 640-59-37, e-mail: mykola.maiba@nure.ua.

This work is dedicated to developing a software module that enhances the security of personal data when using Telegram messenger. Various approaches can be used to create such a software module. This paper examines a hybrid method of information protection that involves the use of data encryption and steganography. By using the software module, protection against intruders who may attempt to intercept transmitted messages is provided. If an intruder intercepts the data or the messenger team cooperates with other entities and transfers data to third parties, the user's security will not be affected since the content of the correspondence will be impossible to read.

Для підвищення безпеки персональних даних користувача було реалізовано програмний модуль для безпечної передачі інформації з використанням відомого месенджеру Telegram, який заздалегідь шифруватиме повідомлення за допомогою стеганографічного алгоритму Steg Cloak [1, 2]. Побудована програма складається з чотирьох основних модулів: MAIN, START, TRANSF та STEG. Модуль MAIN являє собою основу структури програми, яка викликає інші модулі у правильній послідовності. Перший модуль який буде викликаний модулем MAIN – це START. Він створює таблицю MySql, в якій буде зберігатися API нашого клієнта, дані співрозмовника та наші власні дані.

Далі у модулі необхідно ввести реєстраційні дані для генерації клієнта Telegram, а саме API ID та API HASH. Ці дані можна отримати на офіційному вебсайті месенджера. Після цього нам необхідно ввести логін співрозмовника, з яким користувач буде вести діалог. Всі ці дані додаються до бази Info.db. Модуль TRANSF потрібен для обміну повідомленнями між двома користувачами. Після заповнення бази буде створено дві Telegram сесії клієнта. В межах однієї сесії ми зашифровуємо повідомлення та надсилаємо отримувачу, а в межах іншої – розшифровуємо його повідомлення.

Для зашифрування та розшифрування використовується четвертий модуль STEG. Для цього використовується алгоритм стеганографічного шифрування StegCloak, здатний зашифрувати повідомлення за алгоритмом AES256. Потім він стискає отриманий результат і перетворює його на

спеціальні Unicode символи, ці символи вставляються всередину повідомлення та не привертають уваги.

У модулі STEG реалізовано взаємодію з сервісом StegCloak у вигляді командного рядка, а сама зашифровка або розшифровка повідомлення здійснюється за допомогою керування конфігураційними JSON файлами. Алгоритм роботи сервісу StegCloak проаналізовано у [1, 2].

Також під час виконання програми використовуються сторонні бібліотеки, які розширюють стандартний функціонал та дозволяють обробляти великий об'єм даних, серед яких [3, 4]:

1. Бібліотека telethon, яка призначена для спрощення написання програм мовою Python, які можуть взаємодіяти з Telegram. Використовується для відправки повідомлень.
2. Бібліотека Tkinter як стандартний набір інструментів з графічним інтерфейсом для Python. Використовується для графічного виведення повідомлень, які користувач надсилає або отримує.
3. Бібліотека pysqlite3 – бібліотека, яка надає полегшену базу даних на диску, не потребує окремого серверного процесу і дозволяє звертатися до бази даних з використанням нестандартного варіанта мови запитів SQL.
4. Бібліотека lorem-text – бібліотека для генерування супровідного текста.
5. Бібліотека asyncio, що використовується як основа для декількох асинхронних фреймворків Python, які забезпечують високопродуктивні мережні та веб-сервери, бібліотеки підключення до баз даних, розподілені черги завдань тощо.

Тестування розробленого модуля підтвердило його працездатність та ефективність.

Список використаних джерел:

1. Білокуров, О. О., Майба, М. А., Шлома, О. К., & Дробяз, М. О. (2022). Аналіз методів захисту інформації, що знаходять використання у сучасних месенджерах. Матеріали восьмої Міжнародної науково-технічної конференції «Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку (ЕМС-2022)». Харків, ХНУРЕ, 2022. 71–73. https://openarchive.nure.ua/handle/document/21190

2. GitHub – KuroLabs/stegcloak: Hide secrets with invisible characters in plain text securely using passwords. (n.d.). GitHub. https://github.com/KuroLabs/stegcloak

3. Telethon's Documentation – Telethon 1.27.0 documentation. (n.d.). Telethon's Documentation – Telethon 1.27.0 documentation. https://docs.telethon.dev/en/stable/

4. asyncio Asynchronous I/O. (n.d.). Python documentation. https://docs.python.org/3/library/asyncio.html

УДК 004.056:355.451

# ІНФОРМАЦІЙНИЙ ЗАХИСТ ПЕРИМЕТРУ В СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ БЕЗПРОВОДОВИХ МЕРЕЖАХ

Діденко Є.С.
Науковий керівник – к.т.н., проф. Марчук В.С.
Харківський національний університет радіоелектроніки, каф. ІКІ імені В.В.Поповського,
м. Харків, Україна
тел. +380(50)-168-14-18, e-mail: yevheniia.didenko@nure.ua

This work is devoted to the study of information protection of the perimeter of wireless networks. In modern wireless networks, the traditional perimeter is transformed into a virtual one that goes beyond the physical. The network edge dynamically changes and passes through mobile devices and cloud infrastructure. The new model of access to information creates new threats. In this work, possible methods of protecting the virtual perimeter are studied.

Інформаційний захист периметру в сучасних телекомунікаційних безпроводових мережах залишається обов'язковим елементом інформаційної безпеки. Він дозволяє звести до мінімуму зовнішні загрози. Однак сучасні мережі не мають кордонів, Мобільність користувачів, необхідність обміну інформацією через зовнішні мережі, поява технологій хмарних обчислень і різноманітних хмарних сервісів вимагають нових підходів до захисту периметру.

Традиційний фізичний периметр перетворюється в віртуальний, що виходить за рамки об’єкта, що підлягає захисту. Захист фізичного периметру доводиться поширювати як за межі, так і в середину об’єкта. З розширенням способів доступу до інформаційних ресурсів і додатків у мережі більше немає єдиної точки входу. Нові технології вимагають інших підходів до організації захисту мережі.

Традиційний периметр зникає, йому на зміну приходить «нечіткий» периметр. Межа мережі динамічно змінюється і проходить по мобільних пристроях і хмарній інфраструктурі. Нова модель доступу до інформації породжує нові загрози, а значить, вимагає додаткових вимог до засобів захисту. Система захисту стає більш складною.

По-перше, потрібно забезпечити захист «класичного» периметра мережі. По-друге, захистити канали передачі інформації за допомогою технологій VPN для мобільних пристроїв. У віртуальних середовищах необхідне застосування віртуальних шлюзів безпеки.

Таким чином, треба контролювати все, що відбувається в мережі - зовні (в хмарі або на мобільних пристроях), на її межі, в центрах обробки даних, а також у внутрішній локальній мережі. Тільки за такої умови можна розраховувати на ефективний захист від цілеспрямованих і прихованих атак.

Для побудови ефективної системи безпеки необхідно визначити, яка інформація представляє цінність для організації, які сервіси і системи повинні бути доступні кінцевим користувачам, яким методам доступу організація віддає перевагу. Наступним кроком мають стати оцінка існуючого стану інформаційної безпеки і виявлення можливих ризиків. І вже виходячи з цього необхідно розробити концепцію та плани розвитку інформаційної структури мережі і системи інформаційної безпеки, Для рішення цієї задачі потрібно розгорнути систему моніторингу і контролю вхідного і вихідного трафіку на найвищих рівнях моделі OSI, щоб контролювати зміст інформаційних повідомлень і їх кореляцію з подіями безпеки.

Основними блоками в організації системи захисту будуть системи управління мобільними пристроями Mobile Device Management (MDM), додатками Mobile Application Management (MAM) і даними Mobile Information Management (MIM).

При цьому актуальність «класичних» механізмів захисту периметра не знижується. Це шлюзи безпеки Gateway (GW), засоби міжмережного екранування Fire Wall (FW), організація віртуальних приватних мереж Virtual Private Network (VPN), системи виявлення і запобігання вторгнень Intrusion Detection System/Intrusion Prevention System (IDS/IPS).

Більш того, розвиток мережних технологій призводить до подальшого розвитку елементів захисту. Наприклад, використовуються міжмережні екрани наступного покоління NGFW, що забезпечують багаторівневий захист на базі одного пристрою. Вирішувати питання забезпечення безпеки інформації необхідно системно і комплексно.

Все більшого значення набувають системи контентної фільтрації (URL-запитів та вхідного трафіку), як і раніце це важливий захист від спаму. Для захисту Web-додатків стають обов'язковими міжмережні екрани прикладного рівня (Web Application Firewall)».

Важливу роль в цьому відіграють надійні механізми захищеного доступу, в тому числі аутентифікація і захист даних, що передаються. Не менше значення має наявність єдиного центру управління доступом і розмежуванням прав користувачів.

Список використаних джерел:

1. Axel Buecker, Per Andreas, Scott Paisley. Understanding IT Perimeter Security. https://www.redbooks.ibm.com/redpapers/pdfs/redp4397.pdf

2. Mallory Mooney. Best practices for network perimeter security in cloud-native environments. https://www.datadoghq.com/blog/securing-cloud-native-infrastructure-network-perimeter/

УДК 004.056:355.451:005.334

# СЦЕНАРНИЙ ПІДХІД ДО ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ТЕОРІЇ НЕЧІТКОЇ ЛОГІКИ

Діденко Є.С.
Науковий керівник – к.т.н., доц. Снігуров А.В.
Харківський національний університет радіоелектроніки, каф. ІКІ імені В.В.Поповського,
м. Харків, Україна
тел. +380(50)-168-14-18, e-mail: yevheniia.didenko@nure.ua

This work is devoted to the study of the scenario approach to the assessment of information security risks based on the theory of fuzzy logic. The quantity and complexity of cyber threats rises at an equivalent rate to the ever-increasing reliance on information technology systems. Creating scenarios based on prospective risks is a key component of a scenario-based approach to risk assessment. Organizations can use fuzzy logic to make better decisions by accounting for the inherent ambiguity in their risk assessments. This study looks at how the scenario method to risk assessment can be combined with fuzzy logic's mathematical foundation.

Кількість і складність кіберзагроз зростає так само швидко, як і залежність суспільства від інформаційних технологій. Щодня компанії будь-якого розміру знаходять нові способи виявлення та пом’якшення загроз доступності, конфіденційності та цілісності своїх найважливіших інформаційних активів. Метод оцінки ризиків інформаційної безпеки на основі сценаріїв на основі нечіткої логіки є одним із методів, які набули популярності в останні роки.

Створення сценаріїв реалізації потенційних ризиків є ключовим компонентом сценарного підходу до оцінки ризиків. Потім ці сценарії оцінюються на основі ймовірності виникнення загрози та її впливу на активи організації. Цей підхід забезпечує більш повну та реалістичну оцінку ризиків інформаційної безпеки, з якими стикається організація.

Нечітка логіка — це математична теорія, яка дозволяє мати справу з невизначеністю та неоднозначністю даних. Це особливо корисно під час оцінювання ризиків інформаційної безпеки, оскільки багато загроз для організацій не є чітко визначеними або важко піддаються кількісній оцінці. Використовуючи нечітку логіку, організації можуть включити невизначеність у свої оцінки ризиків і приймати більш обґрунтовані рішення.

Факторам, які беруть участь в оцінці ризиків, мають бути призначені ступені інтенсивності за умов використання нечіткої логіки в сценарному підході до оцінки ризиків. Наприклад, сценарій, що передбачає фішингову атаку, можна оцінити з точки зору ймовірності отримання зловмисником доступу до конфіденційної інформації, впливу такої інформації на

компрометацію та ефективності існуючих заходів безпеки для запобігання атаці. Справжній ступінь істинності кожного фактора можна визначити на основі наявних даних і експертних знань.

Після визначення ступеня істинності можна використовувати нечітку логіку для визначення загального ризику, пов'язаного зі сценарієм. Це можна зробити за допомогою різноманітних методів, таких як дерева рішень нечіткої логіки, нечіткі когнітивні карти та системи міркування нечіткої логіки. Ці методи дозволяють більш детально і точно оцінювати ризики, з якими стикається організація, таким чином дозволяючи краще приймати рішення.

Однією з головних переваг підходу, який базується на використанні методу сценаріїв з використанням елементів нечіткої логіки, до оцінки ризику є його гнучкість. Його можна адаптувати до конкретних потреб вашої організації та використовувати для оцінки різних сценаріїв і загроз. Це ідеальний підхід для компаній, які прагнуть розробити комплексну та індивідуальну стратегію управління ризиками.

В доповіді приводиться приклад розрахунку ризику інформаційної безпеки для обраних для дослідження кібератак з використанням сценарного підходу. Також показується, що сценарний підхід до оцінки ризиків інформаційної безпеки на основі теорії нечіткої логіки забезпечує точнішу та всебічну оцінку ризиків, з якими стикається організація. Усуваючи невизначеність і неоднозначність даних, організації можуть приймати більш обґрунтовані рішення щодо стану безпеки та розробляти ефективніші стратегії управління ризиками. У міру розвитку та ускладнення кіберзагроз використання нечіткої логіки в оцінці ризиків стає все більш важливим для забезпечення безпеки критично важливих активів.

Список використаних джерел:

1. Діденко Є.С., Снігуров А.В., Слюсар Н.В. Сценарний підхід до оцінки ризику інформаційної безпеки / Є.С. Діденко, А.В. Снігуров, Н.В. Слюсар // Восьма міжнародна науково-технічна конференція «Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку» (ЕМС-2022), ХНУРЕ, 2022.

2. Потій О. В. Основні положення математичного апарату суб'єктивної логіки та його застосування для оцінки рівня зрілості систем забезпечення безпеки інформації / О. В. Потій, А. В. Лєншин. // Радіотехніка. Тематичний випуск «Інформаційна безпека». – 2005. – С. 144–160.

УДК 004.056:343.98]:004.77

# МЕТОДИКА ЦИФРОВОГО КРИМІНАЛІСТИЧНОГО ДОСЛІДЖЕННЯ МЕСЕНДЖЕРІВ

Рєзніченко Д.Ю.
Науковий керівник – доцент Снігуров А.В.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
тел. +38(099) 790-70-05, e-mail: dymytrii.rieznichenko@nure.ua.

This work is devoted to research in the field of digital forensics, more specifically – forensics of messengers. Three most popular today's messengers were considered, and the possible working methods of obtaining personal information of users from these messengers were investigated and described.

In addition, a list of information that could be obtained from messengers was specified. It is also important to note that all the described methods are relevant for Windows and Android operating systems. Moreover, a prerequisite for all experiments was the presence of a physical device (phone, laptop or computer) of the suspect in the hands of a digital forensic investigator.

Сьогодні месенджери стали невід’ємною частиною нашого життя. За їх допомогою можна безкоштовно та без обмежень спілкуватися з людьми із різних країн, здійснювати швидкий обмін будь-якими файлами (фото, відео, документи тощо), створювати публічні та приватні тематичні групи тощо. Усе вищезазначене є відповіддю на питання величезної популярності месенджерів.

Але така популярність часто привертає увагу не лише нових потенційних користувачів, а й зловмисників (наприклад, хакерів). Крім цього, дослідженням месенджерів часто займаються й правоохоронні органи, оскільки цими додатками нерідко користуються злочинці (наприклад, для планування терактів, обміну забороненими матеріалами тощо). В останньому випадку має місце цифрова криміналістика (пошук, отримання, дослідження та закріплення цифрових доказів).

В рамках написання кваліфікаційної роботи бакалавра було проведено дослідження механізмів цифрового криміналістичного аналізу трьох популярних месенджерів: Viber, WhatsApp та Telegram.

Особливості методики цифрового криміналістичного аналізу месенджера Viber. Цей месенджер можна вважати найбільш небезпечним з усіх вищезазначених, оскільки він зберігає всі дані (переписки, переслані фото, відео, документи та інше) у незашифрованому вигляді на мобільному пристрої чи комп’ютері самого користувача. Щоб прочитати ці дані, необхідно лише знайти файл «viber.db» (зазвичай він зберігається у локальних файлах месенджера) та відкрити його за допомогою програми SQLiteStudio. У «viber.db» можна побачити наступну інформацію: текстові повідомлення з приватних чатів користувача; персональну інформацію контактів користувача (дата народження, номер телефону, імена тощо); перелік публічних та приватних чатів, членом яких є користувач; назви й

ідентифікатори файлів, які було переслано або отримано користувачем через Viber, а також багато іншого. Крім цього, всі фото й відео, які користувач отримав чи переслав через Viber, можна побачити в окремих папках за адресами: «Android\data\com.viber.voip\files» (для Android) і «C:\Users\”користувач”\ AppData\Roaming\ViberPC\”номер телефону”» (для Windows).

Особливості методики цифрового криміналістичного аналізу месенджера WhatsApp. Цей месенджер, як і Viber, зберігає всю інформацію користувача на його власному пристрої. Але ці дані вже є зашифрованими стійким блоковим криптографічним алгоритмом AES-256 (у режимі GCM). Для їх розшифрування з мобільного пристрою потрібно дістати спеціальний ключ, який зазвичай зберігається у «…/data/data/files/key» директорії. Доступ до цієї директорії можливий тільки за наявності на мобільному пристрої root-прав (за замовчуванням їх немає). Якщо ключ є, з WhatsApp можна дістати: тексти листувань, інформацію про голосові та відеодзвінки, технічні дані месенджера, номери телефонів та інші персональні дані контактів користувача тощо. Варто також зазначити, що всі користувацькі дані WhatsApp зберігає в окремому файлі «msgstore.db.crypt14», який можна знайти за шляхом: «…\Android\media\com.whatsapp\WhatsApp\Databases» (для Android) та «C:\Users\”користувач”\AppData\Local\Packages\ 5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalState» (для Windows). Медіафайли (фото, відео тощо) месенджера можна також знайти у цих двох директоріях. Варто також додати, що WhatsApp, як і Viber, видаляє всі метадані медіафайлів (неможливо дізнатися, де було зроблено фото, на який пристрій тощо). Особливості методики цифрового криміналістичного аналізу месенджера Telegram. Telegram є найбільш захищеним месенджером, оскільки всі переписки та персональні дані він зберігає на власних серверах, а не на пристрої користувача. З Telegram можна витягнути лише медіафайли та голосові повідомлення, які зберігаються у відкритому вигляді за адресами: «…\Android\data\org.telegram.messenger \files\Telegram» (для Android) та «C:\Users\”користувач”\Downloads\ Telegram Desktop» (для Windows). Мінусом є те, що Telegram не видаляє метадані медіафайлів.

Список використаних джерел:

1. Viber для Windows и история сообщений [Електронний ресурс] // Habr. – 08.02.2016. – Режим доступу: https://habr.com/ru/articles/276777/. – Назва з титул. екрану.

2. FAQ for the Technically Inclined [Електронний ресурс] // Core.telegram. Режим доступу: https://core.telegram.org/techfaq#q-how-does-end-to-end-encryption-work-in-mtproto. – Назва з титул. екрану.

3. How to decrypt whatsapp crypt14 files [Електронний ресурс] // YouTube. – 12.03.2022. – Режим доступу: https://www.youtube.com/watch?v=TBL72KqemGs&list=LL&index=1&t. – Назва з титул. екрану.

УДК 004.057.4:355.451]:004.75

# ОГЛЯД ВРАЗЛИВОСТЕЙ МЕРЕЖНОГО ОБЛАДНАННЯ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Назаров Байрамалі Аріф
Науковий керівник – д.т.н., проф. Євдокименко М.О.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського
Харків, Україна
тел. +38(068) 420-39-29, e-mail: marina.ievdokymenko@nure.ua

There are currently no secure information systems and networks. This is due to the fact that each network equipment and software has a certain list of vulnerabilities. According to the analysis, it was found that the main causes of vulnerabilities are outdated software and non-compliance with the principles of secure software development. Vulnerability management scenarios (plans) must be developed to effectively eliminate network equipment vulnerabilities. These scenarios will include regular testing of patch management coverage of the IT infrastructure, the use of a proactive approach in the elimination of vulnerabilities, and the schedule of updating operating systems and software. With a developed vulnerability management plan and its periodic updates, each company will have a clear strategy for eliminating vulnerabilities and improving security as a whole.

На сьогоднішній день не існує ідеально захищених та безпечних інформаційних систем, які при цьому не знаходяться в ізольованому просторі, а виконують свою бізнес-функцію. Тому навіть у самій надійній та перевіреній системі можуть виявитися вразливості, виявлені як в комунікаційному мережному обладнанні так і в додатках на кінцевих пристроях. Таким чином, при аналізі ризиків інформаційної безпеки треба враховувати вразливості мережного обладнання для мінімізації ризиків як на етапі проектування так і під час функціонування інфокомунікаційної мережі.

Джерелом багатьох вразливостей є застаріле програмне забезпечення (ПЗ), небезпечні протоколі та недотримання принципів безпечної розробки додатків та ПЗ. Для аналізу та врахування найбільшої кількості вразливостей згідно з міжнародним стандартом NIST 800-53 [2], було створено систему загальних вразливостей та ризиків (Common Vulnerabilities and Exposures, CVE), що надає еталонний метод для загальновідомих вразливостей інформаційної безпеки та впливу.

Для охоплення всіх основних характеристик та числової оцінки вразливостей використовується загальна система оцінки вразливості (Common Vulnerability Scoring System, CVSS). Всі ці системи допомагають організаціям належним чином оцінити та визначити пріоритети своїх процесів управління вразливостями.

Згідно аналітичних даних [1] вразливості розподіляються за наступними категоріями щодо їх використання зловмисниками та реалізацією атаки (Рис. 1).

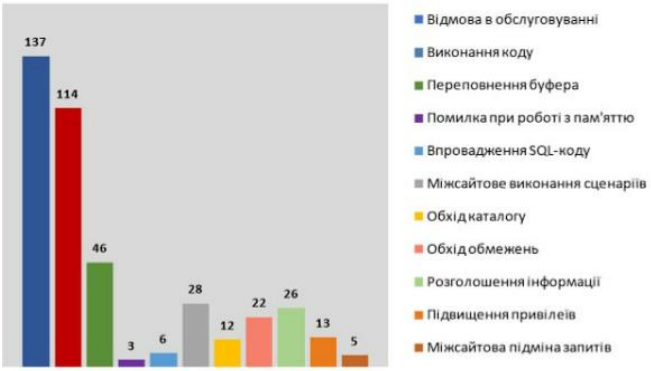



Рисунок 1 – Типи атак, реалізованих за допомогою вразливостей мережного обладнання

Згідно проведеного аналізу, найпопулярнішими та критичними вразливостями в 2022 році є наступні [1,3]:

- Log4j (CVE-2021-44228),
- ProxyNotShell (CVE-2022-41040),
- Spring4Shell (CVE-2022-22965),
- Atlassian Confluence (CVE-2022-26134, CVE-2022-26138),
- Zimbra RCE (CVE-2022-27925, CVE-2022-41352),
- Follina web framework Ruby on Rails (CVE-2022-30190),
- F5 BIG-IP (CVE-2022-1388).

У 2023 році експерти прогнозують, що вразливості Log4Shell, Spring4Shell та подібні до них ще довго залишатимуться загрозою, оскільки системи, що використовують дане вразливе ПЗ, широко поширені.

Висновки: Для ефективного усунення вразливостей мережного обладнання потрібно розробляти сценарії (плани) з управління вразливостями. Дані сценарії включатимуть регулярну перевірку покриття патч-менеджментом ІТ-інфраструктури, застосування проактивного підходу в усуненні вразливостей та графіку оновлення операційних систем та програмного забезпечення. Завдяки розробленому плану з управління вразливостями та його періодичного оновлення кожна компанія матиме чітку стратегію із усунення вразливостей та підвищення безпеки в цілому.

Список використаних джерел:

1. The annual report’22 of the European Union Agency for Cybersecurity, ENISA. The 10th edition, 2023. – 96 p.

2. The NIST Risk Management Framework, NIST Special Publications 800-53, 2022. – 47 p. https://nvd.nist.gov/vuln

3. National Vulnerability Database (NVD). CVSS’22. https://www.nist.gov/

УДК 004.057.4:355.451]:004.75

# ОГЛЯД БАЗ ДАНИХ ВРАЗЛИВОСТЕЙ ДЛЯ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Назаров Байрамалі Аріф
Науковий керівник – д.т.н., проф. Євдокименко М.О.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського
Харків, Україна
тел. +38(068) 420-39-29, e-mail: marina.ievdokymenko@nure.ua

The importance of ensuring the protection of infocommunication networks is due to the need to ensure their stability in the conditions of constant cyber attacks. One of the effective method of ensuring the cyber protection of ICM is a preliminary assessment of information security risk, which can be calculated using the criticality metrics of vulnerabilities specified in the recommendations of the National Institute of Standards and Technology. Criticality metrics of vulnerabilities collected in databases are used to quantify the information security risks of any ICM vulnerabilities. Using these metrics, it is possible to make an accurate assessment of risks, the degree of criticality of vulnerabilities present in ICM, and possible damage due to the use of identified vulnerabilities.

Важливість забезпечення захисту інфокомунікаційних мереж (ІКМ) обумовлена необхідністю забезпечення їх стійкості в умовах здійснення постійних кібератак. Захист будь-якої інфокомунікаційної мережі починається ще на етапі проектування та продовжується під час функціонування. Одним з ефективних засобів забезпечення захисту ІКМ є попередня оцінка ризику інформаційної безпеки, який може розраховуватись за допомогою використання зазначених в рекомендації National Institute of Standards and Technology (NIST) метрик критичності вразливостей [1].

Для оцінки ризику інформаційної безпеки та рівня захищеності ІКМ в цілому можуть використовуватися організаційні стандарти та моніторинг мережі за допомогою мережних сканерів, SIEM-систем та систем виявлення та протидії атакам тощо. Приведені інструменти дозволяють отримати кількісні оцінки безпеки, що базуються на метриках безпеки з прогнозуванням та вимірюванням вразливостей мережі.

На сьогодні існує велика кількість баз даних із вразливостями та пропозиціями щодо їх усунення. Найбільш відомими є 10 баз даних вразливостей, якими користуються для аналізу та оцінці ризику інформаційної безпеки та які представлені нижче [2]:

1. Open Sourced Vulnerability Database є базою із детальну інформацію про всі наявні вразливості та постійним оновленням шляхом реєстрації та валідації нових вразливостей.

2. Vulnerability Intelligence є базою, що пропонує безпеку на основі ризиків для комплексного аналізу вразливостей за допомогою постійного моніторингу в режимі реального часу.

3. Open Vulnerability and Assessment Language є системою звітів про стан інформаційної системи.

4. Exploit Database представляє собою каталог із сценаріями використання вразливостей в інформаційній системи із їх детальним описом.

5. IBM X-Force Exchange представляє собою хмарну платформа обміну розвідувальними даними, що використовується для дослідження останніх загроз, співпраці та консультації з експертами.

6. CXSecurity представляє собою базу даних про вразливості для інформування користувачів про різні помилки в веб додатках.

7. VFeed є базою даних вразливостей, яка використовує специфічну методологію для автоматизованого збору та відстеження та оцінки вразливості для вчасного виявлення, реагування та захисту від кібератак.

8. Secunia Advisory and Vulnerability Database Database представляє собою базу даних з інформаційними бюлетенями, які сформовані експертами Secunia Research та містять відомості про виявлені загрози і вразливості програмного забезпечення.

9. Vulnerability Notes Database (VND) представляє собою базу даних вразливостей мережного обладнання, програмного забезпечення, посилаючись на безліч відповідних CVE ідентифікаторів.

10. Common Vulnerabilities and Exposures – це база даних вразливостей, що містить відомі вразливості обладнання, програмного забезпечення або прошивки, яка допомагає уиувати вразливості, виявляти вторгнення, та управляти інцидентами тощо.

Висновок: Для кількісної оцінки ризиків інформаційної безпеки будь-якої ІКМ використовуються метрики критичності вразливостей, зібраних в бази даних вразливостей у відкритому доступі. Користуючись даними метриками з різних баз можна здійснити точну оцінку ризиків, ступінь критичності наявних в ІКМ вразливостей та можливий збиток внаслідок використання ідентифікованих вразливостей.

Список використаних джерел

1. Hu C. Guidelines for Access Control System Evaluation Metrics [Електронний ресурс] / C. Hu, K. Scarfone // NIST Interagency/Internal Report (NISTIR), National Institute of Standards and T3echnology, Gaithersburg, MD. – 2012. – Режим доступу до ресурсу: https://doi.org/10.6028/NIST.IR.7874 (Accessed March 26, 2021).

2. National Vulnerability Database [Електронний ресурс] – Режим доступу до ресурсу: https://nvd.nist.gov/vuln/data-feeds.

УДК 004.056:355.451]:004.057.2

# ПРОБЛЕМИ І МЕТОДИ ВПРОВАДЖЕННЯ МІЖНАРОДНИХ СТАНДАРТІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Красюкова В.В.
Науковий керівник – доц. Куля Ю.Е.
Харківский національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії імені В.В. Поповського)
e-mail: valeriia.krasiukova@nure.ua

Ensuring information security is one of the most important tasks of the modern world. Every year, the amount of digital data processed by companies and organizations increases, so it is important to protect this information from unauthorized access. To achieve this goal, international standards for ensuring information security were developed. For successful implementation, it is necessary to use different methods and take into account the specifics of the specific organization and the context in which it operates. For successful implementation, it is necessary to use different methods and take into account the specificities of the specific organization and the context in which it operates.

Забезпечення інформаційної безпеки є однією з найважливіших задач сучасного світу. З кожним роком кількість цифрових даних, які обробляються компаніями та організаціями, зростає, тому важливо захищати цю інформацію від несанкціонованого доступу. Для досягнення цієї мети були розроблені міжнародні стандарти забезпечення інформаційної безпеки.

Міжнародні стандарти забезпечення інформаційної безпеки, такі як ISO/IEC 27001 та NIST Cybersecurity Framework, висувають рекомендації та вимоги щодо захисту інформації в організаціях будь-якого типу та розміру. Однак існує кілька проблем та викликів, пов'язаних із впровадженням таких стандартів.

Важливою проблемою впровадження міжнародних стандартів забезпечення інформаційної безпеки є їх складність та розмірність. Багато стандартів містять велику кількість вимог та рекомендацій, що може призвести до великих витрат часу та коштів на їх впровадження.

Іншою проблемою є розбіжності між національними стандартами та міжнародними стандартами. Це може призвести до того, що впровадження міжнародних стандартів буде ускладнено або навіть неможливо в деяких країнах [1].

Крім того важливою проблемою може бути відсутність підтримки керівництва компанії в процесі впровадження стандартів. Успішне впровадження стандартів забезпечення інформаційної безпеки потребує підтримки керівництва організації, але деякі керівники можуть не віддавати цьому пріоритетну увагу.

Також важливо зазначити, що впровадження стандартів безпеки може бути складним через технічні обмеження та необхідність оновлення існуючих інформаційних систем.

Для успішного впровадження стандартів забезпечення інформаційної безпеки необхідно визначити потреби та ризики компанії, розробити стратегію безпеки, встановити контрольні точки та забезпечити виконання всіх вимог стандартів. Крім того, компанії повинні забезпечити навчання персоналу щодо правил та процедур інформаційної безпеки та регулярно оновлювати свої системи захисту від нових загроз [2].

Після впровадження стандарту важливо провести аудит інформаційної безпеки. Аудит дозволяє перевірити, наскільки відповідає організація міжнародним стандартам забезпечення інформаційної безпеки та виявити можливі проблеми та недоліки. Після цього можуть бути запроваджені заходи для вирішення виявлених проблем.

Деякі стандарти забезпечення інформаційної безпеки, передбачають можливість отримати сертифікат на відповідність стандарту. Це може бути важливим для підтвердження відповідності організації міжнародним стандартам та для забезпечення довіри клієнтів та інших сторінок інтересу.

У підсумку, міжнародні стандарти забезпечення інформаційної безпеки є важливим інструментом для захисту інформації в компаніях та організаціях. Впровадження цих стандартів допомагає зменшити ризики порушення безпеки інформації та зберегти репутацію компанії. Проте, успіх впровадження стандартів забезпечення інформаційної безпеки залежить від ретельного аналізу потреб і ризиків компанії, а також від постійного оновлення та удосконалення систем безпеки.

Список використаних джерел:

1. Заболотний, О. В., Кошовий, М. Д., Книш, В. О., & Костенко, О. М. (2010). Основи стандартизації. Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харк. авіац. ін-т".
2. Кириченко, Л. С. (2008). Стандартизація і сертифікація товарів та послуг. Ранок.

УДК 004.056:355.451

# МЕТОДИКА ПРОВЕДЕННЯ ПАСИВНОГО OSINT ЗА ДОПОМОГОЮ ПАКЕТУ KALI LINUX

Гонтарь І. А.
Науковий керівник – к.т.н. доцент Снігуров А. В.
Харківський національний університет радіоелектроніки, каф. Інфокомунікаційної інженерії імені В.В. Поповського, м. Харків, Україна
тел. +38(067) 546-86-35, e-mail: ivan.hontar@nure.ua.

There are many different ways to access the system. Many believe that to gain access to servers or services, you only need to know how to program. It does not. The very first step in attacking or auditing a target is gathering information about the target. Open source intelligence is an intelligence discipline that deals with intelligence generated from publicly available information that is collected, used, and disseminated to appropriate audiences in a timely manner to address specific intelligence and information requirements.

OSINT також являється розвідувальною інформацією, розробленою на основі відкритого збору та аналізу загальнодоступної інформації та інформації з відкритих джерел. OSINT є похідним від систематичного збору, обробки та аналізу загальнодоступної відповідної інформації у відповідь на вимоги розвідки. Два важливі пов’язані терміни – це інформація з відкритого джерела та загальнодоступна інформація [1]:

−відкрите джерело — це будь-яка особа або група, яка надає інформацію без очікування конфіденційності — інформація, стосунки чи те й інше не захищені від публічного розголошення. Інформація з відкритих джерел може бути загальнодоступною, але не вся загальнодоступна інформація є відкритою. Під відкритими джерелами розуміються загальнодоступні носії інформації і не обмежуються фізичними особами;

−загальнодоступна інформація — це дані, факти, інструкції чи інші матеріали, опубліковані або транслюванні для загального користування; доступний на запит для члена широкої громадськості; законно побачений або почутий будь-яким випадковим спостерігачем; або оприлюднити на зустрічі, відкритій для широкої публіки.

Збір даних OSINT зазвичай здійснюється шляхом моніторингу, аналізу даних і досліджень. Виробництво з відкритим кодом підтримує розвідувальну інформацію з усіх джерел і безперервну діяльність процесу розвідки (генерування розвідувальних знань, аналіз, оцінка та поширення).

Сьогодні будь-яка інформація про людину або його життя вже зберігається в глобальній мережі. Виходячи з цих даних, дана особа може стати метою для хакерів і може піддаватися вербовкам або іншим прийомом соціальної інженерії для досягнення цілей злочинців.

Корпоративна пошта є сильним інструментом для нанесення збитку будь-якій компанії. Кожен співробітник може випадково виявитися тією вразливістю, якою можуть скористатися злочинці. Доступ до цього

електронного ящику може виявлятися явно у великих компаніях, де співробітники більше, що означає, велика ймовірність подати до зловмисних цілей. Для аналізу та виявлення подібних цілей існують сервіси, які аналізують, порівнюють і заносять інформацію у свої бази даних. Паролі, як і особисті дані, співробітники можуть використовувати із-за користування ненадійними ресурсами, тощо. Приклади, описані нижче, є рішеннями з відкритим кодом для пошуку співробітників їх корпоративних ящиків для електронних листів [2]:

−hunter.io – пошук корпоративних користувачів;

−bluto - виконує перерахунок адрес електронної пошти на основі цільного домену, в даний час використовуючи пошукові системи Bing і Google, а також збирає дані зі служб Email Hunter і LinkedIn.

Після досягнення цілей, хакер має великий арсенал для можливої атаки на потенційну ціль:

−спам;

−blackmailing;

−крадіжка пароля.

Після визначення списків потенційних цілей хакер збирає дані про цілі:

−соціальні мережі та їх зміст;

−особисті почтові скриньки.

У світі існує величезна кількість злитих паролів користувачів у відкритому доступі. Із-за того, що, в основному, люди ставлять всюди повторюваного пароля, можна методом перебору підібрати потенційний пароль від корпоративного облікового запису. Існує база даних, яка містить у собі понад 1.4 мільярда імейлів і паролів, отриманих з різних ресурсів. Це рішення називається Breach-parse. Breach-parse – відкрита база даних потенційних злитих паролів користувачів різних поштових скриньок та їх доменів. Наприклад, потенційна мета – це провідний програміст у системі авторизації у дослідженій компанії. Доступ до ресурсів, як база даних, є тільки через VPN, до якого можна отримати, через 3rd party авторизацію на корпоративному обліковому записі. Корпоративні облікові записи несуть у собі не тільки інфрмацію, але й доступ до підсистем компанії для розуміння вразливості системи з боку аудитора або зловмисних цілей з боку хакера.

Список використаних джерел:

1. Open Source Intelligence (OSINT). (2023, 28 лютого) OSINT Techniques. https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/

2. 15 top open-source intelligence tools. (2021, 28 червня). https://www.csoonline.com/article/3445357/what-is-osint-top-open-source-intelligence-tools.html

УДК 004.056:355.451

# МЕТОДИКА ПРОВЕДЕННЯ АУДИТУ НА СЕРВЕРАХ ЗА ДОПОМОГОЮ ПАКЕТУ KALI LINUX

Гонтарь І. А.
Науковий керівник – к.т.н. доцент Снігуров А. В.
Харківський національний університет радіоелектроніки, каф. Інфокомунікаційної інженерії імені В.В. Поповського, м. Харків, Україна
тел. +38(067) 546-86-35, e-mail: ivan.hontar@nure.ua.

There are a huge number of programs and operating systems that act as servers for receiving, processing and storing information. Every such system is a potential target for attackers. One of the main problems is the untimely update of the program, operating systems, etc. Such inactivity can cause: gaining access to the system, data theft, infection of the system, etc. This article examines ways to gain control over a server through untimely server updates using Apache as an example.

Виправлення сервера або виправлення сервера оновлює програмне забезпечення сервера для виправлення помилок, оновлення версій або покращення функцій та продуктивності. Виправлення помилок також передбачає усунення вразливостей системи безпеки та усунення помилок, які можуть становити загрозу для даних та інформації компанії.

Таким чином, ми можемо сказати, що є п'ять основних причин для оновлення сервера [1]:

−щоб усунути конкретну помилку чи недолік у коді обробки ядра;

−щоб підвищити стабільність, функції та функції серверної операційної системи чи будь-якої її програми;

−розробники програмного забезпечення та операційних систем випускають виправлення та оновлення щоразу, коли виявляються вразливості; їх слід швидко встановити;

−для видалення розповсюдженого програмного забезпечення – непотрібного коду та програм – для оптимізації розміру та споживання ресурсів основних компонентів операційної системи;

−для удосконалення існуючих процесів виправлення – можливо, служби Windows Server Update Services (WSUS) не працюють чи не працюють належним чином; можливо, він взагалі не працює. Інструмент управління виправленнями третьої сторони може взяти на себе роботу або навіть перевершити такі рідні служби виправлення.

У цій статті як приклад буде розглядатися HTTP-сервер Apache. Apache — це безкоштовне міжплатформне програмне забезпечення веб-сервера з відкритим кодом, випущене згідно з умовами ліцензії Apache 2.0. Apache розробляється та підтримується відкритою спільнотою розробників під егідою Apache Software Foundation [2]. Переважна більшість екземплярів HTTP-сервера Apache працює на дистрибутиві Linux, але поточні версії

також працюють на Microsoft Windows, OpenVMS та широкому спектрі Unix-подібних систем. Попередні версії також працювали на NetWare та інших операційних системах, включаючи порти до мейнфреймів.

Кожна версія програми або операційної системи має потенційно вразливість, яку зловмисник може скористатися. Оновлення систем є не тільки додаванням нових можливостей сервісу, але може в собі нести оновлення системи для перекриття потенційних проломів у безпеці. Хакери намагаються знайти можливі вразливості в безпеці в кожній версії програми для своєї вигоди. Такі дані, як знайдена вразливість або навіть її використання може бути викладена в мережу. Щоб розглянути це питання детальніше, нижче буде розглянуто способи ідентифікації версії операційної системи або програми, використовуючи операційну систему Kali Linux, як інструмент для тестування на проникнення:

−nmap -T4 -A -p- 192.182.131.105 – дана команда шукатиме порти, операційну систему або програму та їх версію в рамках IP адреси 192.182.131.105;

−nikto -h #domain – дана команда є безплатним аналізатором вразливості веб-ресурсів і також надає операційну систему або програму та їх версію в рамках #domain.

Після ідентифікації операційної системи та їх версії, як тестувальники на проникнення, потрібно перевірити чи існують якісь експреси для цієї версії системи. Для пошуку, існують величезна кількість ресурсів. Нижче є кілька найбільш популярних прикладів:

−exploit-db.com – сайт, який зберігає в собі величезну кількість експоїтів у відкритому доступі, які допомагають провести тестування на проникнення на різних ступенях зануреності;

−searchspoilts apache 1.3 – команда для Kali Linux, яка шукає можливі експлоїти для Apache сервера для версії 1.3.

На основі зібраної інформації, залежно від вже знайдених експлоїтів, хакер має можливість скористатися вразливістю сервера через несвоєчасне оновлення та отримати доступ до сервера, файлам конфігурації інших серверів, які знаходяться на даному сервері, отримання даних з інших сервісів, впроваджені зараженого програмного забезпечення. забезпечення та тд.

Список використаних джерел:

1. What is Patch Management and Why is it Important?. (2021, 1 вересня). https://jumpcloud.com/blog/what-is-patch-management.

2. Apache HTTP Server. (2010, вересень). https://en.wikipedia.org/wiki/Apache_HTTP_Server.

УДК 004.415.2

# ЕТАПИ СТВОРЕННЯ ДИЗАЙНУ МОБІЛЬНОГО ЗАСТОСУНКУ

Кабаченко В.О.
Науковий керівник – Золотарьов В.А.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
тел. +38(095) 570-31-70, e-mail: viacheslav.kabachenko@nure.ua

This paper is dedicated to the process of design development for mobile applications. The paper discusses the stages that a designer must go through to create an attractive and functional mobile application design. First of all, the process of identifying the target audience and its needs is studied. Next, the stages of prototype development and testing, including user interaction and solving identified problems, are considered. The paper also examines the issues of visual design, including the choice of colors, typography, and other elements that will help create a user-friendly and attractive design. As a result, the work allows you to understand what stages you need to go through to create a successful mobile application design.

Процес розробки мобільного застосунку, як і будь-якої розробки програмного забезпечення, включає: аналіз вимог до проекту, проектування, реалізацію, тестування продукту, впровадження та підтримку.

Для розробка ефективного мобільного застосунку можна поєднувати підходи User Experience (UX) та User Interface (UI). UX визначає як користувач сприймає і взаємодіє з продуктом, системою або послугою. UI фокусується на інтерфейсі, який полегшує комунікацію між користувачем і апаратними та програмними компонентами інфокомунікаційної системи. Моделюючи UX та UI, дизайнери можуть створити індивідуальний та ефективний мобільний застосунок [1].

На етапі проектування відбувається UX та UI моделювання для допомоги користувачу логічно досягти поставленої мети за допомогою інтерфейсу. Не слід плутати UI дизайн та UX моделювання, незважаючи на їхню схожість і той факт, що вони часто виконуються однією і тією ж людиною.

Для розробки мобільних застосунків процес UX/UI моделювання передбачає завершення етапу аналізу вимог перед етапом проектування. На цьому етапі визначають ідею, мету, завдання, джерела необхідної інформації, вказівки замовника та мобільну платформу для майбутнього застосунку.

Окреслимо ключові етапи моделювання UX.

- Аналіз переваг і недоліків існуючих застосунків;

- Визначення функціоналу мобільного застосунку , виходячи з вимог замовника та проведеного аналізу існуючих аналогів, UX-спеціаліст повинен розставити пріоритети і проранжувати важливість кожного функціонального компонента;
- Моделювання UX-дизайнером сценаріїв використання мобільного застосунку;
- Створення прототипу застосунку, зокрема розташування функціональних елементів на екранах мобільного застосунку.

При створенні дизайну мобільного застосунку UI-дизайнер за можливістю дотримується рекомендацій мобільної платформи та фірмового стилю замовника. Процес розробки дизайну складається з п'яти етапів: створення ескізу головного екрану, затвердження ескізу головного екрану замовником, створення ескізів усіх екранів та іконок у застосунку, затвердження дизайну замовником та написання довідкових рекомендацій для верстальника, який включає інформацію про розміщення об'єктів, кольори, шрифти та інші деталі[1].

Після передачі макету дизайну розробникам, активна частина UX/UI моделювання завершується і переходить у пасивне спостереження UX/UI фахівця, який стежить за тим, щоб макет відповідав реальному застосунку. Коли бета-версія мобільного застосунку буде випущена для обраної групи користувачів, UX/UI фахівець оцінює відгуки користувачів і вносить необхідні корективи. Використання технології UX/UI дизайну для мобільних застосунків підвищує якість дизайну і знижує витрати за рахунок зменшення та усунення помилок на ранніх стадіях розробки. Ці витрати іноді перевищують початкові витрати на розробку програми.

Якісний дизайн покращує користувацьку привабливість та якість програмування, оскільки не потребує зміни інформаційної структури застосунку при реалізації.

Список використаних джерел:

1. Кім В.Ю. Особливості розробки дизайну інтерфейсу користувача для мобільного застосунку // Нові інформаційні технології в автоматизованих системах. 2015. №18. [Електронний ресурс] – Режим доступу до ресурсу: http://cyberleninka.ru/article/n/osobennosti-razrabotki-dizayna-polzovatelskogo-interfeysa -dlya-mobilnogo-prilozheniya.

УДК 004.056.5:005.7

# ПРОЦЕСНІ ПІДХОДИ ДО АУДИТУ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Євсюкова О.О.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківський національний університет радіоелектроніки
каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
тел. +380 98 853 34 57 e-mail: olena.ievsiukova@nure.ua

Information security covers the tools and processes that organizations use to protect information. This includes policy settings that prevent unauthorized people from accessing business or personal information. Information system security services audit deal with the identification and analysis of potential risks, their mitigation or removal, with the aim of maintaining the functioning of the information system and the organization's overall business. While expanding online, cyber risks also increased with more targeted attacks against organizations ranging from small to large. Performing a security audit can help organizations by providing information related to the risks associated with their networks. It can also help in finding security loopholes and potential vulnerabilities in their system. Thereby patching them on time and keeping hackers at bay.

При створенні системи інформаційної безпеки важливим є процес перевірки та верифікації інформаційної безпеки, поряд з такими процесами, як впровадження захисних заходів, навчання персоналу та реалізація політики безпеки. Ці аудити дозволяють перевірити адекватність обраних захисних заходів та засобів та виявити існуючі вразливості в інформаційній системі. У процесі перевірки та верифікації інформаційної безпеки особливе місце займають аудити, основна мета яких – сформулювати незалежну оцінку інформаційної безпеки.

Процесний підхід – ефективний інструмент для аудиту систем менеджменту інформаційної безпеки, що ґрунтується на ідентифікації та оцінці процесів, що використовуються організацією для забезпечення безпеки інформації. Процесний підхід до аудиту фокусується на аналізі послідовності та взаємодії процесів, а також їх вхідних та вихідних даних. Він аналізує систему управління не як набір документованих процедур, а як активну систему процесів. Процесний підхід включає оцінку політики безпеки, процедур управління доступом, моніторингу та аналізу логів, управління ризиками та багато іншого.

Однією з переваг процесного підходу є його комплекність, адже такий підхід дає змогу оцінити ефективність системи інформаційної безпеки загалом, а не лише окремих її компонентів. Це дозволяє отримати повне уявлення про те, як організація забезпечує безпеку інформації. Аудитори,

які використовують процесний підхід, можуть виявити не тільки існуючі проблеми, а й потенційні ризики та вразливість системи безпеки.

Процесний підхід включає кілька етапів: ідентифікація та оцінка процесів, оцінка взаємозв'язків між процесами.

При ідентифікації процесів аудитор повинен визначити всі процеси, пов'язані із забезпеченням безпеки інформації в організації. Це можуть бути процеси управління доступом, резервного копіювання даних, моніторингу та аналізу логів, управління ризиками та інші процеси.

Наступним кроком аудитор повинен оцінити ефективність кожного процесу та виявити можливі вразливості та ризики у кожному з них. У цей момент може використовуватися стандарт ISO/IEC 27001, який містить рекомендації щодо оцінки процесів системи управління інформаційною безпекою.

При оцінюванні взаємозв'язків між процесами аудитор має визначити, як пов'язані між собою різні процеси та як вони впливають на безпеку інформації в організації. Аудитор повинен проаналізувати отримані результати та зробити висновки про те, наскільки ефективною є система менеджменту інформаційної безпеки в організації.

Серед недоліків процесного підходу аудиту систем менеджменту інформаційної безпеки виділяють його трудомісткість, високу складність та обмеженість. Такий підхід потребує великої кількості часу та ресурсів на ідентифікацію процесів, їх оцінку та аналіз взаємозв'язків між ними. Процесний підхід до аудиту інформаційної безпеки є складним методом, який потребує певних знань та навичок аудиторів. Процесний підхід може не враховувати деякі аспекти системи безпеки, які не є процесами, такими як фізична безпека та криптографічні методи захисту.

Проте, процесний підхід є одним із найефективніших методів оцінки системи менеджменту інформаційної безпеки. Результати аудиту, проведеного із застосуванням процесного підходу, можуть допомогти організації покращити свою систему менеджменту інформаційної безпеки та підвищити рівень захисту інформації.

Список використаних джерел:

1. ISO/IEC 27002:2022. http://www.itref.ir/uploads/editor/2ef522.pdf

УДК 004.056:355.451(477+73)

# ПОРІВНЯЛЬНИЙ АНАЛІЗ КІБЕРСТРАТЕГІЙ УКРАЇНИ ТА США

Шпількін А. Р.
Науковий керівник – ст. викл. Волотка В.С.
Харківський національний університет радіоелектроніки,
кафедра ІКІ ім. В.В. Поповського, м. Харків, Україна
тел. +38(063) 84-936-59, e-mail: andrii.shpilkin@nure.ua

This work is dedicated to the study of the existing national cybersecurity strategies, its best practices and comparing the relevant documents of United States of America and Ukraine. The rapid development of information and communications technology entails a certain list of challenges for all people. And some of them can be addressed by proper regulations and norms that provide guidance on a state or interstate basis.

Кібербезпека – відносно нове слово, вперше вживане у 1989 р. (згідно зі словником Merriam-Webster), та яке набуло популярності за останні 10-15 років. І зазвичай у цьому контексті оперують такими термінами, як злам, атака, хакер, засоби захисту. Але також є регуляторні норми, які впроваджуються на державному або міждержавному рівні та визначають подальший розвиток галузі в цілому.

Важливим документом такого роду на національному рівні є кіберстратегія. Як зазначено у «A GOVERNANCE FRAMEWORK FOR NATIONAL CYBERSECURITY STRATEGIES» – документі, що визначає кращі практики для підтримки застосування Національної стратегії кібербезхпеки (НСК) – від European Union Agency for Cybersecurity (ENISA), НСК необхідна для забезпечення безпеки мережевих та інформаційних систем. Мета НКС – викласти план дій для покращення безпеки та стійкості національних інфраструктурних систем і послуг. Вона спрямована на високорівневий підхід до кібербезпеки ("зверху-вниз") і встановлення низки національних цілей і пріоритетів.

Останнім часом, Україна стала потужним гравцем на кіберарені, адже доки інші держави мали змогу затверджувати теоретично, Україні довелося швидко пристосовуватися та бути готовою до викликів кібервійни.

Саме тому цікавим є порівняння кіберстратегій США та України. Як провідної держави у цій сфері та тої, якій довелося опановувати теоретичні сценарії на практиці.

Варто зазначити, що останній документ НКС США було видано 1 березня 2023, відповідний документ в Україні введено в дію указом Президента від 26 серпня 2021 року.

За результатами експертних оцінок, стан реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96, за визначеними показниками не перевищує 40 відсотків. Невирішеними залишилися питання оперативного обміну

інформацією про кіберзагрози, ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства. Недостатніми є організація і проведення наукових досліджень у сфері кібербезпеки .

Ключовими напрямками НКС України є:

– убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;

– захист прав, свобод і законних інтересів громадян України у кіберпросторі;

– європейська і євроатлантична інтеграція у сфері кібербезпеки.

Відповідний документ США містить ці положення у злегка зміненій формі (наприклад, безпосередньо визначає захист критичної інфраструктури), а також містить два додаткові напрями – формування ринкових сил (хто може, робить більше) та інвестиції у стійке майбутнє. Зробивши аналіз, можна виявити, що ці напрямки пов’язані, адже за рахунок збільшення відповідальності великих гравців приватного і державного секторів є прагнення зробити цифрову екосистему більш стійкою до кіберзагроз. Стосовно загального ландшафту кібербезпеки, НКС США визначає автократичні держави такими, що становлять небезпеку у цифровому середовищі та описує Китайську Народну Республіку як найбільш стійкого та активного зловмисника. Окрім цього, наголошено на успіху кампанії «Shields Up» від Агентства кібербезпеки та інфраструктурної безпеки, як вдалої взаємодії державного і приватного секторів для зменшення ризиків кібератаки та розуміння плану дій у такому випадку. У свою чергу, кіберстратегія України зазначає небезпеку від Російської Федерації, а рівень захищеності від таких загроз встановлено як метрику досягнення успіху реалізації заходів НКС.

Також цікавим пунктом є те, що як США, так і Україна визнають недостатню кількість наукових робіт, досліджень і розробок у галузі кібербезпеки та планують розвиток цього напряму шляхом забезпечення координації та стимулювання активності.

Загалом, НКС є необхідним державним документом для визначення подальшого розвитку у сфері кібербезпеки.

Список використаних джерел:

1. Про Стратегію кібербезпеки України, Указ Президента України №447/2021 (2021). https://www.president.gov.ua/documents/4472021-40013

2. A Governance Framework for National Cybersecurity Strategies (2023). https://www.enisa.europa.eu/publications/a-governance-framework-for-national-cybersecurity-strategies/@@download/fullReport

3. National Cybersecurity Strategy (2023) (United States). https://www.hsdl.org/c/view?docid=875831

УДК 004.056.5

# ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ НА БАЗІ СТАНДАРТУ WI-FI

Поповська Є.О.
Науковий керівник – доц. Куля Ю.Е.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Науки, 14,
кафедра Інфокомунікаційної інженерії імені В.В. Поповського,
тел. (067) 573-19-09, E-mail: yelyzaveta.popovska@nure.ua

The given work is devoted to the modern methods of protection surveillance systems established based on wireless systems. The subject of the study is the means of protecting the video surveillance system based on Wi-Fi wireless technology. Conducting a comparative analysis of Wi-Fi protocols. The main methods of wireless network encryption RC4, AES analyzed. Security protocols such as WEP, WPA, WPA2, and WPA3 reviewed and analyzed. The main methods of wireless network encryption RC4, AES analyzed.

Сучасні безпровідні локальні мережі (WLAN) є дуже корисними майже скрізь, як-от коледжі, кафе, метро, офісі тощо відповідно до потреб споживачів на прикладі послуг відеоспостереження. Тому, безпека та конфіденційність WLAN з послугами відеоспостереження є дуже важливим фактором. Безпровідні протоколи безпеки WEP, WPA, WPA2, WPA3 застосовуються для забезпечення автентифікації, конфіденційності та цілісності переданих даних [1].

Безпровідні протоколи працюють на канальному рівні та фізичному рівні стеку мережних протоколів. В свою чергу мережні протоколи використовуються для серії 802.11 протоколів безпровідних мереж і надають сучасні послуги, зокрема відеоспостереження.

1. Розповсюдження: передача кадру до певного або всіх місць призначення. 2. Комбінація: підключення від IEEE до інших мереж WLAN.

3. З’єднання: розпізнавання підключення клієнтів через точку доступу. 4. Повторне підключення: перехід між різними точками доступу, коли з’єднання втрачено. 5. Припинення: припинення існуючого зв’язку або підключення. 6. Перевірка: лише авторизовані користувачі отримують доступ до мереж. 7. Деавтентифікація: видалення дійсного користувача. 8. Секретність: ніхто не може бачити особисті дані іншого. 9. MSDU: Кадри даних служби MAC відповідальні за отримання даних від клієнта до кінцевого пункту призначення.

Звісно, що Wired Equivalent Privacy (WEP) є першим стандартом IEEE 802.11, який реалізує найпростіший механізм автентифікації. Шифрування WEP має багато вразливостей, через які атакуючий може повністю відновити ключ після захоплення мінімального мережного трафіку. Механізм автентифікації, розроблений із єдиним статичним ключем, застосовується всіма користувачами. Управляючий доступ до ключів, часта

їх зміна та виявлення порушень практично неможливі. В даний час на злом WEP витрачаються хвилини.

У 2005 році Федеральне бюро розслідувань США зламало WEP за 3 хвилини, використовуючи комбінацію статистичних методів, зосереджених на захоплених унікальних векторах ініціалізації, та атак методом грубої сили за словником для злому 128-бітних ключів WEP.

Протокол автентифікації для безпровідних локальних мереж забезпечує безпеку даних так само, як і в проводових локальних мережах. Він відповідає безпровідним стандартам 802.11. WEP використовує криптографічний алгоритм RC4 для кодування та декодування пакетів. WEP було розроблено для забезпечення конфіденційності, цілісності та автентифікації кадрів. Конфіденційність забезпечує кодування (алгоритм RC4) пакетів. Цілісність забезпечується циклічною перевіркою надмірності (CRC), а автентифікація здійснюється за допомогою спільного ключа, який відомий лише дійсним користувачам мережі.

Метою алгоритму WEP є забезпечення безпеки між кінцевими користувачами безпровідної локальної мережі через радіосигнали.

Слабкі сторони WEP: 1. Розмір IV є коротким і використовується повторно. 2. Уразливість шифрування RC4 через слабкі ключі. Кадри, які закодовані цими ключами, легко зламати. Оскільки перші три байти ключів беруться з IV, який надсилається незашифрованим у кожному пакеті, цією вразливістю можна легко зловживати шляхом пасивної атаки. Для захоплення 104-бітного ключа WEP потрібно прийняти від 2000 до 4000 реальних пакетів, які перехоплюються за дуже короткий проміжок часу. 3. WEP не зупиняє крадіжку фреймів.4. WEP не зупиняє атаки відтворення.

Щоб усунути вразливості WEP, не змінюючи мережних ресурсів, у 2003 році розроблено новий протокол під назвою Wi-Fi Protected Access. WPA використовує два методи, такі як: WPA Personal або WPA-PSK (Pre-Shared Key – спільний ключ) та WPA Enterprise або Commercial.

WPA Personal 1-3 поколінь використовується для невеликого діапазону мереж, наприклад у коледжах, готелях тощо. Ключ автентифікації може бути до 256 біт. На відміну від WEP, це може бути будь-який буквено-цифровий шаблон і використовується лише для узгодження першого сеансу разом із точкою доступу.

Висновки:

Порівняння безпровідних протоколів безпеки WEP та WPA 1-3 поколінь показало ефективність WPA3 покоління в режимах безпеки, алгоритмів шифрування, наявності прямої секретності та розширеної можливостей розмірах ключа.

Список використаних джерел:

1. Technologies Discussed [Електронний ресурс]. – Режим доступу до ресурсу: https://www.versitron.com/blog/hdcvi-vs-hdtvi-vs-hdahd-hdcctv-technologies-discussed.

УДК 004.056:[681.518.52:334.716]

# КІБЕРБЕЗПЕКА SCADA-СИСТЕМ ЕЛЕВАТОРНИХ КОМПЛЕКСІВ

Прийдак О.І.
Науковий керівник – к.т.н., доц. Піскарьов О.М.
Державний біотехнологічний університет, кафедра АКІТ, м. Харків, Україна
тел. +38(057) 712-35-37, e-mail: post@btu.kharkov.ua.

This article deals with the cyber security of SCADA systems in elevator complexes. The article discusses the main vulnerabilities of SCADA systems. It offers practical recommendations for securing SCADA systems, including regular system updates, the use of strong passwords and secure network connections, cyber security training for users, and data backups. It is noted that cyber security is critical for elevator complexes and should be a priority for all companies and organizations working with SCADA systems.

Кібербезпека стала однією з найактуальніших тем у світі технологій. Щодня нові пристрої та системи підключаються до Інтернету, що робить їх уразливими для кібератак. Однією з таких систем є SCADA система - система керування та автоматизації технологічних процесів в елеваторних комплексах. Такі системи керують роботою обладнання та виробничими процесами, контролюють параметри навколишнього середовища й оперативно реагують на неполадки. Крім того, збирають і передають цінні дані про виробничий процес, які можуть бути використані зловмисниками для кібератак [1]. Проблема кібербезпеки SCADA систем в елеваторних комплексах стала особливо актуальною у світлі дедалі поширеніших кібератак на промислові об'єкти [2]. Напади на SCADA системи можуть призвести до серйозних наслідків, як-от зупинка виробництва, втрата даних, витік конфіденційної інформації, а у випадку з елеваторними комплексами - до аварій, включно з різними видами вибухів.

Щоб убезпечити SCADA системи, необхідно застосовувати комплексний підхід, що включає в себе захист як програмного, так і апаратного забезпечення. Наприклад, важливо використовувати засоби аутентифікації та авторизації, паролі, біометричні дані або смарт-картки, а також зашифрувати трафік, що передається між пристроями. Крім того, необхідно регулярно оновлювати програмне забезпечення та перевіряти його на наявність вразливостей, а також встановлювати фізичні обмеження доступу до обладнання. Однак найефективнішим способом захисту SCADA систем є профілактика, яка охоплює навчання персоналу правилам кібербезпеки, регулярне аудиторське обстеження системи, створення резервних копій даних і створення плану дій у разі кібератаки.

Практичні рекомендації, які можуть допомогти захистити SCADA системи в елеваторних комплексах від кібератак, включають в себе наступне:

1. Регулярне оновлення та патчінг SCADA систем. Це дасть змогу виправити вразливості в безпеці та усунути помилки, які можуть бути використані зловмисниками для проведення кібератак.

2. Використання сильних паролів та їх регулярна зміна. Паролі мають містити щонайменше 8 символів і містити букви, цифри та спеціальні символи. Паролі також мають бути унікальними для кожного пристрою та запису.

3. Розмежування прав доступу користувачів. Кожен користувач повинен мати доступ тільки до необхідних функцій і даних, які необхідні для виконання його робочих обов'язків.

4. Встановлення антивірусного програмного забезпечення. Антивірусне ПЗ допоможе виявляти і блокувати шкідливі програми та файли, які можуть проникнути в SCADA систему.

5. Використання захищеного мережевого з'єднання. Мережеві з'єднання між пристроями і системами мають бути зашифровані, щоб запобігти перехопленню і підміні даних.

6. Навчання користувачів основам кібербезпеки. Усі користувачі SCADA системи повинні бути навчені основам безпеки, таким як розпізнавання фішингових листів, невідкриття шкідливих вкладень.

7. Резервне копіювання даних. Важливо регулярно створювати резервні копії даних, щоб у разі кібератаки була можливість швидко відновити роботу системи.

Застосування цих рекомендацій дасть змогу підвищити рівень безпеки SCADA систем в елеваторних комплексах і запобігти можливим кібератакам.

Таким чином, забезпечення кібербезпеки SCADA систем в елеваторних комплексах - це невід'ємна частина успішного функціонування виробництва. Відсутність ефективного захисту може призвести до серйозних наслідків, які можуть призвести до втрати матеріальних і фінансових ресурсів, а також загрожувати безпеці працівників і навколишнього середовища. Безпека SCADA систем в елеваторних комплексах - вимагає постійної уваги та зусиль з боку всіх учасників виробничого процесу. Захист має бути комплексним і включати в себе не тільки технічні, а й організаційні заходи. Тільки в цьому разі можна забезпечити надійну та безпечну роботу SCADA систем і запобігти можливим кібератакам.

Список використаних джерел:

1. Cyber Attacks On the Rise in the Agriculture Industry [Електронний ресурс] // EdgeLabs. – 2022. – Режим доступу до ресурсу: https://edgelabs.ai/blog/cyber-attacks-on-the-rise-in-the-agriculture-industry/.

2. Ransomware attacks on grain coops may just be the start of ag sector security woes [Електронний ресурс] // Andrea Peterson. – 2021. – Режим доступу до ресурсу: https://therecord.media/ransomware-attacks-on-grain-coops-may-just-be-the-start-of-ag-sector-security-woes.

УДК 004.056

# ДЕЯКІ ПОГЛЯДИ НА ПОБУДОВУ МОДЕЛІ ЗАГРОЗ В ІНТЕРЕСАХ ОЦІНКИ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ

Магдаліна М.І.
Науковий керівник – доцент Снігуров А.В.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
тел. +38(097) 933-78-40, e-mail: mariia.mahdalina@nure.ua.

In the report, an analysis of problems in building a model of threats and an intruder in the assessment of information security risks of companies is carried out. The report analyzes the content of the threat model, presents problems in solving the task of building a threat model. A classification and integral indicator of intentional threats is proposed.

При оцінці ризиків інформаційної безпеки одним з ключових завдань є побудова моделі загроз і її складової – моделі порушника. Оцінка ризиків інформаційної безпеки (ІБ) вимагає розуміння рівня загроз (можливості - Likelihood, ймовірності – Probability, або щорічної кількості - Annualized rate of occurrence). Ця оцінка є різною для різних компаній, різних ризикових ситуацій, різної безпекової ситуації.

Відомо, що усі загрози поділяються відповідно джерела загрози на загрози від антропогенних джерел, загрози від природних джерел та загрози від техногенних джерел. До перших відносяться загрози від людини. Такою людиною може бути зловмисник, який реалізує або таргетовану (цільову) атаку, або нетаргетовану атаку. Такою людиною може бути зловмисник, який по необережності або халатності порушує інформаційну безпеку компанії. Зловмисники можуть бути зовнішні та внутрішні (інсайдери). До типів зовнішніх зловмисників можуть відноситися представники спеціальних служб іншої держави, кримінальні структури, потенційні злочинці і хакери, несумлінні партнери, представники аварійних служб і наглядових організацій, технічний персонал телекомунікаційних послуг. До інсайдерів можуть відноситися основний персонал компанії (програмісти, розробники, користувачі), представники служби захисту інформації, допоміжний склад (охорона, прибиральники тощо), технічний персонал (експлуатація, життєзабезпечення).

Під природними загрозами розуміються пожежі, землетруси, повені, урагани, магнітні бурі, радіоактивне випромінювання, інші форс-мажорні обставини. Під техногенними загрозами розуміються технічні проблеми з засобами зв'язку, мережами інженерних комунікацій (каналізація, водопостачання), транспортом, неякісними технічними засобами обробки інформації, неякісними програмними засобами обробки інформації, проблеми з допоміжними засобами (охоронна сигналізація, телефони) тощо.

Модель загроз та модель порушника мають дати відповідь на одне з головних питань при оцінці ризиків ІБ – який порушник реальний для

конкретної компанії, яка природна або техногенна загроза реальна для компанії.

При аналізі поставленого питання необхідно зрозуміти, по – перше, що таке модель. Модель — це абстрактне представлення (опис) реальності в певній формі (наприклад, у математичній, фізичній, символічній або графічній), призначене для розвитку розуміння цієї реальності. В доповіді приводяться приклади моделі загроз ІБ, яка представлена в текстовій формі, та приклади математичної моделі таких загроз. В доповіді аналізуються проблеми адекватності та точності моделі загроз. Важливим поняттям при побудові моделі загроз є класифікація загроз. Класифікація — це система групування об'єктів дослідження або спостереження відповідно до їх загальних ознак. Класифікація загроз дозволяє їх поділити по певним класам, східним по значенням параметрів моделі. Це дає змогу виділити для кожного класу загроз східні механізми їх реалізації та побудувати механізми захисту від цих загроз.

При побудові моделі ненавмисних загроз – природних та техногенних в більшості випадків вистачає статистики реалізації цих загроз у світі, країні та регіоні компанії, історія реалізації цих загроз в самій компанії. Методи експертного аналізу загроз з використанням такої інформації дають можливість з певною якістю побудувати модель даних загроз. Складніше ситуація є з побудовою моделі зловмисника. Параметрами моделі мають бути: мотивація зловмисника та його потенціал. Під потенціалом зловмисника розуміється наявність у нього певної кваліфікації та обладнання для реалізації конкретної атаки.

Що ми маємо отримати після побудови моделі зловмисника для оцінки ризиків ІБ. По-перше інтегрований показник, який би об’єднував мотивацію та потенціал зловмисника. Необхідність такого показника обумовлена тим, що потенціал може у зловмисника і бути, але мотивації немає. І навпаки. Тому в доповіді пропонується ввести інтегральний показник зловмисника – рівень небезпечності зловмисника. По друге, класифікація типів зловмисників по інтегральному показнику. В доповіді пропонується класифікація на підставі 3-х рівнів по шкалі: високий, середній, низький.

Такий підхід дозволяє отримати інформацію про можливість реалізації тих чи інших каналів атаки на критичні активи організації з урахуванням того, хто може здійснити таку атаку.

Список використаних джерел:

1. ISO/IEC 27005:2022 Інформаційна безпека, кібербезпека та захист конфіденційності — Настанови щодо управління ризиками інформаційної безпеки [Електронний ресурс] / ISO. – 2022. – Режим доступу до ресурсу: https://www.iso.org/ru/standard/80585.html.

УДК 004.056

# ПІДХОДИ ДО БЕЗПЕРЕВНОГО УДОСКОНАЛЕННЯ МОДЕЛІ ЗАГРОЗ В ІНТЕРЕСАХ ОЦІНКИ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ

Магдаліна М.І.
Науковий керівник – доцент Снігуров А.В.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
тел. +38(097) 933-78-40, e-mail: mariia.mahdalina@nure.ua.

The report analyzes the problem of constantly updating the threat model while ensuring the functioning of the information security management system. It is proposed to draw up a threat model in a Google-sheet, and to calculate information security risk according to the SRAMM methodology.

Однією з системних вимог до системи управління інформаційною безпекою (СУІБ, Information Security Management System, ISMS) є вимога постійного покращення якості даної системи. Логіка реалізації даної вимоги ще в стандарті ISO/IEC 27001-2005 була представлена у вигляді моделі PDCA (або моделі Шухарта-Демінга) - моделі як основи для всіх процедур управління інформаційною безпекою. Сутність даної моделі полягає в реалізації взаємопов'язаних процесів на етапі планування СУІБ, впровадження та функціонуванні її, моніторингу та покращення. Такими процесами є оцінка та обробка ризиків інформаційної безпеки (ІБ), обробка інцидентів ІБ, аудит, аналіз системи з боку менеджменту компанії та інші. Необхідність реалізації даної моделі була пов'язана з тим, що після розробки та в процесі функціонування СУІБ в компанії, яка її експлуатувала, могли бути зміни в бізнес-процесах, а також з'являтися нові загрози та вразливості. В умовах значних змін в безпековій ситуації навколо компанії необхідна була переоцінка ризиків ІБ з удосконаленням заходів захисту критичних інформаційних активів.

Для необхідності якісної реалізації процесу переоцінки ризиків необхідна постійна оцінки загроз та вразливостей, тобто постійна переоцінка моделі загроз для компанії з урахуванням безпекової ситуації як з компанією, так і в регіоні, країні та світі [1].

Для постійного удосконалення моделі загроз необхідно використовувати ресурси, в які можна оперативно вносити зміни для тих загроз, які вже були проаналізовані, та вносити нові загрози, надавати допуск для експертів інформаційної безпеки, а також менеджменту компанії. На наш погляд, ефективною технологією для рішення цього завдання є Google Таблиці.

Google Таблиці – це онлайн-додаток, за допомогою якого можна створювати та форматувати таблиці, а також працювати над ними спільно з іншими користувачами [2]. При роботі з цими таблицями можна додавати

до таблиць текст, цифри та формули, а також редагувати та форматувати ці дані. Google Таблиці відповідають тим самим вимогам щодо забезпечення конфіденційності та захисту даних, які застосовуються до інших корпоративних сервісів Google Cloud. Корпорація Google використовує передові технології для захисту даних, у тому числі від шкідливого програмного забезпечення. Таблиці Google дозволяють зберігати файли в хмарі, а не локально, що знижує ризики для пристроїв компанії. Всі файли, завантажені на Google Диск або створені в Таблицях, шифруються не тільки під час передачі, але й при зберіганні.

Яка структура таблиці може бути та які сервіси в ній мають бути при побудові та корекції моделі загроз? Якщо аналізувати тільки модель навмисних загроз – модель порушника, то основними складовими даної таблиці мають бути: перелік критичних активів, перелік потенційних загроз для кожного з активів, опис загроз, опис вразливостей для даних активів, рівень загрози та рівень вразливості відповідно тієї методики, яка використовується. Дана таблиця може бути удосконалена розрахунком ризику ІБ. В доповіді приведений приклад Google-Таблиці загроз для навчальної ситуації, приведені приклади оцінки рівнів загроз та вразливостей для методики CRAMM, та приведений приклад оцінки ризику ІБ відповідно механізму розрахунку згідно даної методики.

Методика CRAMM спочатку був розроблена CCTA (Central Computer and Telecommunications Agency) у 1985 році у відповідь на зростаючу потребу в безпеці інформаційних систем. Дана методика на даний час є кращою методикою для використання в урядових департаментах Великобританії та прийнятий багатьма комерційними організаціями та іншими державними адміністраціями по всьому світу [3].

В доповіді запропоновані рішення дозволяють здійснювати постійне оновлення моделі загроз з урахуванням вразливостей, через які ці загрози здійснюють вплив з автоматизованим розрахунком ризику ІБ по методиці CRAMM.

Список використаних джерел:

1. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks [Електронний ресурс]. – Режим доступу до ресурсу: https://www.iso.org/standard/80585.html.

2. Приймайте обґрунтовані рішення, аналізуючи дані в Google Sheets [Електронний ресурс]. // Google – Режим доступу до ресурсу: https://www.google.com/intl/ru_ua/sheets/about/.

3. CRAMM (CCTA Risk Analysis and Management Method) [Електронний ресурс]. – Режим доступу до ресурсу: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html.

УДК 004.056

# ПІДХІД ДО КОМБІНАЦІЇ МЕТОДУ CRAMM З МЕТОДОМ CVSS ДЛЯ ПОКРАЩЕННЯ ОЦІНКИ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ

Магдаліна М.І.
Науковий керівник – доцент Снігуров А.В.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
тел. +38(097) 933-78-40, e-mail: mariia.mahdalina@nure.ua.

The report presents a proposal for improving the methodology CRAMM for assessing information security risks, taking into account the solutions presented in the methodology for assessing the vulnerabilities of the CVSS. The improvement consists in modernizing the procedure for calculating the level of vulnerability by adding the parameters of the basic metric of the CVSS methodology. This will significantly increase the accuracy of information security risk calculations when building the company's information security management system.

При оцінці ризиків інформаційної безпеки (ІБ) компанії виникає питання якості такої оцінки. Якість оцінки ризику ІБ, по-перше, залежить від точності вихідних даних, до яких відносяться точність описання бізнес процесів компанії, розуміння ТОП-менеджментом компанії того, які активи в компанії реально критичні, точності опису моделі загроз, розуміння своїх вразливостей. А, по друге, від точності опису параметрів ризику ІБ – рівня (частоти) загроз, рівня вразливості, вартості критичного інформаційного активу.

Одним з кращих методів оцінки ризику ІБ є метод CRAMM (CCTA Risk Analysis and Management Method). Даний метод на даний час використовується в урядових департаментах Великобританії та прийнятий багатьма комерційними організаціями та іншими державними адміністраціями по всьому світу [1].

Рівень загрози в методі CRAMM оцінюються за п’ятибальною шкалою: дуже низький, низький, середній, високий або дуже високий. Зміст даної оцінки має такі значення: дуже низька - очікується, що інцидент траплятиметься в середньому не частіше одного разу на 10 років; низька - очікується, що інцидент траплятиметься в середньому раз на 3 роки, середня - очікується, що інцидент траплятиметься в середньому раз на рік, висока - очікується, що інцидент траплятиметься в середньому раз на 4 місяці, дуже висока - очікується, що інцидент траплятиметься в середньому раз на місяць.

Рівні вразливості оцінюються за шкалою низький, середній або високий. Зміст даної оцінки має такі значення: низька - якщо інцидент трапиться, ймовірність реалізації найгіршого сценарію (оцінено під час

оцінки активів) буде не більше 33%, середня - якщо інцидент трапиться, існуватиме від 33% до 66% шансів реалізації найгіршого сценарію (оцінено під час оцінки активів), висока - якщо інцидент трапиться, ймовірність реалізації найгіршого сценарію (оціненого під час оцінки активів) буде вище 66%.

Оцінка рівня активу здійснюється по кільком категоріям, як то «Менеджмент і бізнес-операції», «Особиста безпека», «Персональна інформація», «Юридичні та нормативні зобов'язання», «Правозастосування», «Комерційно-економічні інтереси», «Фінансові втрати/переривання діяльності». Рівень активу для кожної з цих категорій визначається в шкалі від 1 (мінімальний вплив на бізнес-процеси компанії) до 10 ( максимальний вплив на бізнес-процеси компанії).

Результат оцінки ризику відповідно методу CRAMM розраховується в шкалі від 1 до 7. Можна побачити, що точність оцінки рівня загрози середня (п’ять рівнів), точність оцінки вартості активу висока (10 рівнів), але точність оцінки рівня вразливості нижче ніж середня (3 рівня). Зрозуміло, що цю методику розробляли фахові експерти, які вирішили визначити такі рівні показників ризику ІБ.

Виникає питання, як можна підвищити точність оцінки ризику ІБ? В доповіді пропонується рівень вразливості оцінювати відповідно методу CVSS. В стандарті NIST CVSS v3 критичність вразливостей оцінюється на основі декількох глобальних груп метрик: базові метрики, тимчасові метрики, метрики навколишнього середовища – дозволяють деталізувати базові та тимчасові метрики та врахувати особливості середовища в якому знаходиться вразливість, що підлягає оцінці.

Якщо використовувати як оцінку рівня вразливості для методу CRAMM базові метрики методу CVSS, то вже в дану метрику входять такі параметри, як Вектор доступу (Attack Vector), Складність атаки (Attack Complexity), Обов'язкові привілеї (Privileges Required), Взаємодія з користувачем (User Interaction), рівень збитків конфіденційності, цілісності та доступності інформації. Рівень вразливості згідно методу CVSS розраховується в шкалі від 1 до 10. В доповіді представлений механізм перерахунку рівня такої кількісної оцінки вразливості в якісну шкалу для використання в методі CRAMM, а також приклад оцінки ризиків ІБ для навчальної ситуації з використанням удосконаленого методу CRAMM.

Список використаних джерел:

1. CRAMM (CCTA Risk Analysis and Management Method) [Електронний ресурс]. – Режим доступу до ресурсу: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html.

2. Common Vulnerability Scoring System [Електронний ресурс]. – Режим доступу до ресурсу: https://www.first.org/cvss/.

УДК 004.056:316.42

# МЕТОДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ У ФУНКЦІОНУВАННІ СУЧАСНОГО СУСПІЛЬСТВА

Маньковський А.Г.
Науковий керівник – к.т.н., доцент Снігуров А.В.
Харківський національний університет радіоелектроніки,
каф. Інфокомунікаційної інженерії імені В.В. Поповського, м. Харків,
Україна
тел. +38(068) 755 13 21, andrii.mankovskyi@nure.ua.

The report provides an analysis of social engineering methods that can be used by an attacker to attack an enterprise. Weaknesses and strengths of methods of protection against attacks using social engineering are given, and mechanisms of protection against attacks using social engineering methods are analyzed in detail.

Ефективність підприємства пов'язана не лише з її технологічними можливостями, методами управління та реалізації продукції, а також можливістю протистояти тим зовнішнім впливам, які накладає конкурентна боротьба. Соціальна інженерія – метод отримання доступу до інформації, заснований на особливостях психології людей. Основною метою соціальної інженерії є отримання доступу до конфіденційної інформації, паролів, банківських даних та інших захищених систем.

В доповіді проведений аналіз методів соціальної інженерії при реалізації загроз інформаційної безпеки. Стисло наведемо дані методи.

Претекстинг - це метод соціальної інженерії, при якому зловмисник використовує неправдиві приводи та обман, щоб отримати доступ до конфіденційної інформації чи систем. Вони вигадують привід чи цілий сценарій, щоб вивідати дані чи спонукати жертву на дії. Вони часто просять жертву підтвердити свою особистість. А для цього нібито слід відповісти на серію питань. Наприклад, назвати дівоче ім'я матері, місце народження, дату народження, пароль, номер банківського рахунку, номер зі зворотного боку банківської картки. Отримані дані використовують у своїх цілях для подальшої атаки.

Фішинг – це техніка інтернет-шахрайства, спрямовану отримання конфіденційної інформації користувачів - авторизаційних даних різних систем. Основним видом фішингових атак є підроблений лист, відправлений жертві електронною поштою, який виглядає як офіційний лист від платіжної системи або банку.

Троянський кінь – це техніка ґрунтується на цікавості, страху чи інших емоціях користувачів. Зловмисник відправляє листа жертві за допомогою електронної пошти, у вкладенні якого знаходиться «оновлення» антивірусу, ключ до грошового виграшу або компромат на співробітника.

Quid pro quo (послуга за послугу) – дана техніка передбачає звернення зловмисника до користувача електронною поштою або корпоративним телефоном. Зловмисник може представитися, наприклад, співробітником технічної підтримки та інформувати про виникнення технічних проблем на робочому місці.

Дорожнє яблуко – цей метод є адаптацією троянського коня і полягає у використанні фізичних носіїв (CD, флеш-накопичувачів). Зловмисник зазвичай підкидає такий носій у загальнодоступних місцях на території компанії (парковки,мїдальня, робочі місця співробітників, туалети). Для того, щоб у співробітника виник інтерес до цього носія, зловмисник може нанести на носій логотип компанії та якийсь підпис. Наприклад, "дані про продаж", "зарплата співробітників", "звіт у податкову" та інше.

Зворотна соціальна інженерія - цей вид атаки спрямований на створення такої ситуації, за якої жертва змушена буде сама звернеться до зловмисника за «допомогою».

Tailgating (або piggybacking) - це метод маніпулювання людьми, який полягає в тому, щоб проникнути в обмежену зону, яка зазвичай охороняється, за рахунок використання чужих облікових записів або підробки легітимності.

Методи атаки.

1. Теорія десяти рукостискань. Головна мета зловмисника, який використовує телефон для соціальної інженерії, полягає в тому, щоб переконати свою жертву в одному з двох моментів:

а) Жертві дзвонить співробітник компанії;

б) Телефонує представник уповноваженого органу (наприклад, правоохоронець чи аудитор).

2. Вивчення корпоративної мови.

3. Запозичення музики очікування під час дзвінків.

4. Спуфінг (підміна) телефонного номера.

5. Використання новин проти вас.

6. Використання довіри до соціальних платформ.

7. Тайпсквоттінг.

В доповіді приводяться напрямки захисту підприємства від атак з використанням методів соціальної інженерії. Приводиться приклад процесів, які мають бути реалізовані при побудові систем управління інформаційною безпекою [1], надаються технічні механізми виявлення атак методами соціальної інженерії.

Список використаних джерел:

1. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks [Електронний ресурс]. – Режим доступу до ресурсу: https://www.iso.org/standard/80585.html.

УДК 004.056.53

# ВИКОРИСТАННЯ ПОВЕДІНКОВОЇ МОДЕЛІ ФОГГА ДЛЯ НАВЧАННЯ З ПИТАНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Божко О.В.
Науковий керівник – к.т.н., доцент Снігуров А.В.
Харківський національний університет радіоелектроніки,
каф. Інфокомунікаційної інженерії імені В.В. Поповського, м. Харків,
Україна
тел. +38 (068) 316-02-73, e-mail: oleh.bozhko@nure.ua.

This article explores the potential of using Dr. BJ Fogg's behavioral model to develop a training program for employees in the field of information security. The Fogg Behavior Model states that these three elements must be present for an action to occur: motivation, ability, and trigger. The Fogg Behavior Model provides a framework for understanding how to influence human behavior. The article discusses the rationale for using this model to increase employees' awareness in the field of information security

Підвищення обізнаності співробітників у сфері інформаційної безпеки (ІБ) є важливим завданням для багатьох організацій. Але як забезпечити ефективне навчання, щоб співробітники не тільки розуміли, що потрібно робити, а й дійсно почали застосовувати знання на практиці? Одним із рішень може стати використання поведінкової моделі доктора Брайана Фогга (Fogg Behavior Model), яка допомагає створювати ефективні програми навчання на основі розуміння принципів людської поведінки.

Основною ідеєю моделі Фогга є те, що поведінка людини визначається взаємодією трьох чинників: мотивації, здатності та спонукання [1]. Щоб людина почала виконувати певну дію, їй потрібно бути достатньо вмотивованою, мати достатню спроможність виконати цю дію та отримати спонукання, яке призведе до дії. На рис. 1 схематично представлено суть поведінкової моделі.

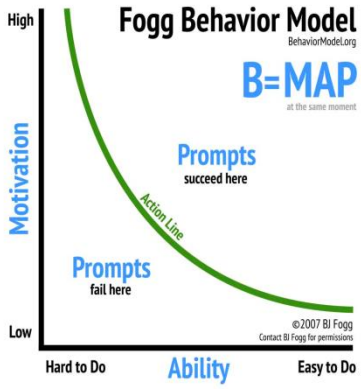



Рисунок 1 - Графічне представлення поведінкової моделі Фогга

Під час розроблення програми навчання для підвищення обізнаності в галузі ІБ на основі моделі Фогга можна використовувати три основні підходи: збільшення мотивації, спрощення завдання та використання спонукань. Збільшення мотивації може бути досягнуто шляхом демонстрації важливості теми і показу того, які наслідки можуть виникнути в разі недотримання правил. Спрощення завдання може бути досягнуто шляхом спрощення процесу виконання правильних дій і створення зрозумілих інструкцій, які легко запам'ятовуються. Використання спонукань являє собою створення ситуацій, коли співробітник отримує тригер для виконання дій, наприклад, отримання нагадування або повідомлення.

Одним із найважливіших аспектів під час використання моделі Фогга є врахування контексту. Так, залежно від контексту, може змінюватися підхід до впливу на мотивацію, здібності та спонукання людини, що, своєю чергою, може вплинути на підвищення обізнаності співробітників. Наприклад, у компанії з розвиненою корпоративною культурою співробітники можуть відчувати більшу мотивацію, якщо знають, що недотримання правил безпеки може призвести до інциденту, внаслідок якого компанія зазнає серйозних збитків.

Як варіант використання моделі Фогга для підвищення обізнаності співробітників у сфері ІБ, можна розглянути наступний приклад.

У результаті аудиту безпеки, в компанії Х було виявлено низький рівень обізнаності співробітників у питаннях інформаційної безпеки. Тоді, відповідно до моделі Фогга, було ухвалено рішення провести низку навчальних вебінарів для підвищення мотивації співробітників до дотримання правил інформаційної безпеки. На вебінарах було висвітлено те, як важлива безпечна поведінка працівників для загальної захищеності компанії від загроз ІБ. Так само було розроблено систему заохочень за безпечну поведінку співробітників.

Отже, поведінкова модель Брайана Фогга допомагає розв'язувати низку психологічних і соціальних проблем, включно з проблемою підвищення обізнаності співробітників у сфері інформаційної безпеки. Вона заснована на трьох ключових принципах: підвищення мотивації, спрощення завдання, спонукання до дії. Так само важливим аспектом використання цієї моделі є врахування контексту, від якого залежить, наскільки успішно будуть реалізовані ключові принципи.

Список використаних джерел:

1. Fogg B. Fogg Behavior Model [Електронний ресурс] / B. Fogg. – 2009. – Режим доступу до ресурсу: https://behaviormodel.org/.

**УДК 004.032.2:621.391**

# ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.77:355.01(477)

# ПОПИТ НА ТЕХНОЛОГІЮ VPN ПІД ЧАС ВОЄННОГО СТАНУ В УКРАЇНІ

Новіченко Є.О.
Науковий керівник – доц. Сабурова О.С.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
тел. +38(096) 552-30-10, e-mail: yelyzaveta.novichenko@nure.ua.

Citizens of Russia and Ukraine are trying to circumvent increasingly stringent internet laws by using VPNs in record numbers in both countries. The Russian invasion of Ukraine had a number of unexpected consequences. Dozens of technology companies have left the area to show solidarity with the Ukrainian people, resulting in the inability to access services such as Netflix, PayPal and more. Subsequently, citizens of both countries turned to virtual private network (VPN) services in the hope of circumventing government-imposed bans.

Загарбники всіляко намагаються ізолювати людей на окупованих територіях від цивілізованого світу. Один із способів – блокування зв'язку та інтернету.

Окупанти намагаються підключити українців до російських інтернет-мереж, де є обладнання для фільтрації інтернет-трафіку, що дозволило заблокувати багато українських та міжнародних веб-ресурсів. Щоб уникнути стеження та обійти обмеження, українські користувачі, підключені до російських мереж, повинні використовувати сервіси VPN.

VPN — це віртуальна приватна мережа, яка забезпечує шифрування трафіку між VPN-клієнтом і сервером, змінюючи IP-адресу. Сервіси VPN дозволяють використовувати ресурси, доступ до яких заборонено за географічним принципом або на підставі рішень влади. Завдяки VPN користувач вільно відвідувати заблоковані веб-сайти [1].

В Україні доступ до Інтернету був порушений через вторгнення російських військ, що також підштовхнуло все більше і більше українців використовувати VPN. Насправді ці дані показують подібне зростання, причому зростання попиту досягло піку на 609% вище, ніж середньодобовий показник на початку лютого (рис.1).

В цей час попит на послуги VPN в рф досяг піку в 2692% 14 березня порівняно із середньодобовим попитом за тиждень до вторгнення в Україну. Цей останній пік стався після трьох днів постійного зростання інтересу. Станом на 31 березня попит на VPN знизився, але залишався високим на 243% вище норми, тоді як середній щоденний попит на VPN у період з 15 по 31 березня був на 617% вищим за норму (рис.2).

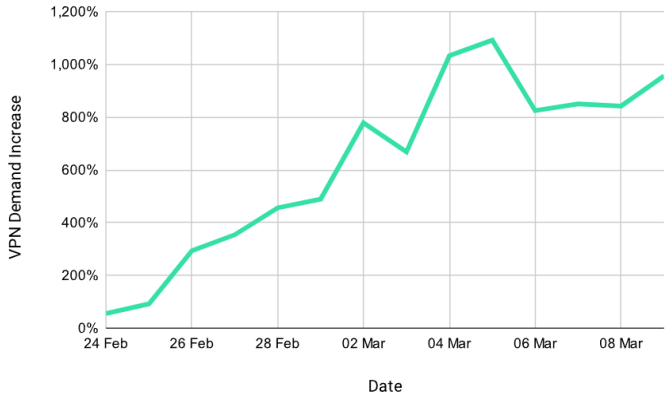



Рисунок 1 – Статистика зростання попиту VPN в Україні з початку війни

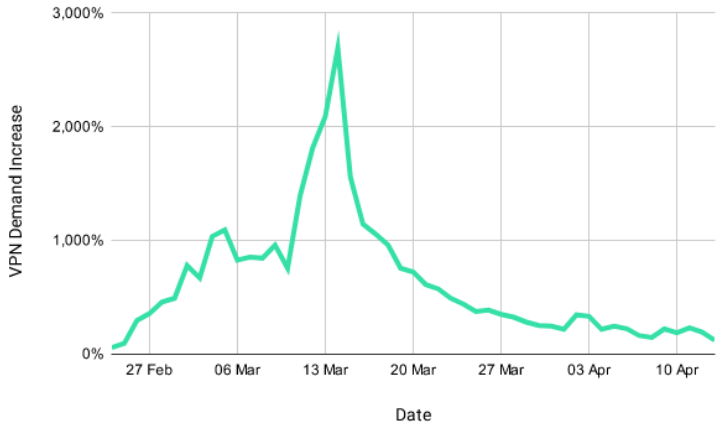



Рисунок 2 - Статистика зростання попиту VPN в рф

В умовах війни російські війська можуть блокувати доступ до українських державних сайтів та ЗМІ на тимчасово окупованих територіях України. Громадянам України важливо отримувати інформацію про евакуацію, рекомендації державних органів та роботу волонтерів. Якщо користувач знаходиться на території, де сили окупантів блокують доступ до життєво важливих джерел інформації, йому знадобляться засоби обходу блокування сайтів – технологія VPN.

Список використаних джерел:

1. Геническ City. Для тих, хто в окупації: підбірка безпечних VPN-сервісів для користування інтернетом (2022, 16 червня) https://henichesk.city/articles/219181/dlya-tih-hto-v-okupacii-pidbirka-bezpechnih-vpn-servisiv-dlya-koristuvannya-internetom

2. Top10VPN. VPN Demand Surges Around the World (2023, 5 січня) https://www.top10vpn.com/research/vpn-demand-statistics/

3. Techco. VPN Usage in Russia and Ukraine Has Skyrocketed (2022, 10 березня) https://tech.co/news/vpn-usage-russia-ukraine

УДК 004.75:37

# НАВЧАЛЬНА ПЛАТФОРМА ДЛЯ РОЗВИТКУ НАВИЧОК РОБОТИ ХМАРНИМИ СЕРВІСАМИ

Канівець В.І.
Науковий керівник – к.т.н., доц. Скорик Ю.В.
Харківський національний університет радіоелектроніки, кафедра ІМІ,
м. Харків, Україна
тел. +380975448660, email: vitalii.kanivets@nure.ua.

This publication states that cloud computing has become a fundamental aspect of our daily lives, increasing the demand for qualified professionals who are able to effectively use cloud services and ensure their security and stability. The work provides a scheme for the operation of the learning platform in conjunction with cloud providers such as GCP, AWS, Azure. To create such a platform, Terraform and Jenkins can be used to solve specific problems to provide automation of raising resources, checking completed tasks and destroying resources, which saves time and money during training.

У сучасному світі практично кожен аспект нашого життя залежить від хмарних технологій. У цьому контексті зростає потреба в кваліфікованих фахівцях, які можуть ефективно використовувати хмарні сервіси та забезпечувати їх безпеку та стабільність. Відповідно до цього, розробка та впровадження навчальної платформи для розвитку навичок роботи з хмарними сервісами стає все більш актуальною. [1]

Для розробки ефективної навчальної платформи для розвитку навичок роботи з хмарними сервісами, необхідно враховувати специфіку цієї технології. Зокрема, така платформа повинна містити матеріали та вправи, які дозволять користувачам не лише ознайомитися з теорією, а й отримати практичні навички використання різноманітних хмарних сервісів. Важливо також забезпечити користувачам можливість розвитку навичок у конкретних сферах, наприклад, управління базами даних, розробці програмного забезпечення або інтеграції хмарних сервісів з мережевими аплікаціями. [2] Крім того, платформа повинна бути постійно оновлювано. та вдосконалюванною, щоб відповідати сучасним тенденціям у розвитку хмарних сервісів. Навчальна платформа має бути мультихмарна, тому треба розробити підходящу схема проходження завдання. Враховуючі останні тенденції розвитку хмарних провайдерів, наразі можна виділити три основні провайдери: GCP, AWS, Azure. Для створення подібної платформи можна використати Terraform - це інструмент інфраструктури як коду, який дозволяє визначати як хмарні, так і локальні ресурси в зрозумілих для людини конфігураційних файлах. [3]

Для автоматизації всіх процесів використаємо Jenkins. Це провідний сервер автоматизації з відкритим кодом. Jenkins надає сотні плагінів для підтримки створення, розгортання та автоматизації будь-якого проекту. [4]

Користувач має підготувати свого хмарного провайдера для того, щоб платформа мала змогу піднімати на ньому ресурси для виконання завдання та перевірки. Після цього, використовуючі Jenkins, він може вибрати потрібне йому завдання та запустити його.

На його хмарі піднімуться відповідні ресурси з неправильному конфігурацією і користувачу потрібно буде вирішити всі недоліки шляхом виправлення тих ресурсів відповідно до завдання.

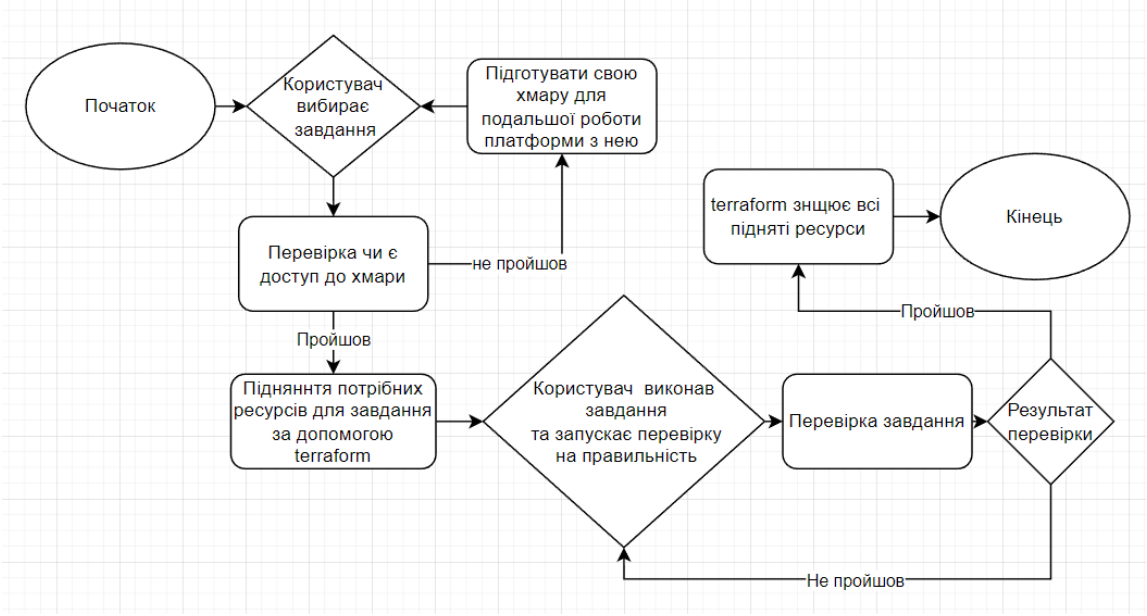



Рисунок 1 – Схема проходження завдання

Як тільки користувач буде впевнений, що його завдання виконане, він може запустити перевірку на тому Jenkins та переконатися вірно чи ні він виконав завдання. Якщо завдання виконано не вірно, Jenkins наддасть відповідний результат, що не так, та що потрібно виправляти і попросить виконати знову.

Користувач може продовжити і повторювати перевірку доки не виконає завдання. Коли все буде вірно всі ресурси автоматично будуть знищені з хмари, що буде гарантувати мінімальні грошові витрати. Кількість створених завдань може постійно поповнюватися для покриття знань по всіх сервісах хмарних провайдерів.

Список використаних джерел:

1. Білан М.О. ІТ-технології в навчанні. - К.: Видавництво "Інститут медіації", 2016. - 240 с.

2. Панікова О.В. Інформаційні технології в освіті. - К.: Академія, 2018. - 192 с.

3. Інтернет-ресурс "Terraform". - URL: https://developer.hashicorp.com/terraform/intro (дата звернення: 21.03.2023).

4.Інтернет-ресурс "Jenkins". - URL: https://www.jenkins.io/ (дата звернення: 21.03.2023)

УДК 004.75

# ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ПІДХОДУ INFRASTRUCTURE AS CODE ТА ОГЛЯД ПОПУЛЯРНИХ РІШЕНЬ

Степанов О.О.
Науковий керівник – к.т.н., доц. Скорик Ю.В.
Харківський національний університет радіоелектроніки, кафедра IMI,
м. Харків, Україна
тел. +380636161486, email: oleksandr.stepanov@nure.ua

This paper aims to define the concept of Infrastructure as Code (IaC), or IaC for short, explain its potential benefits, and provide a list of features that distinguish it from the traditional manual approach to cloud infrastructure setup. The paper also presents examples of tools designed to support IaC, such as CloudFormation from Amazon Web Services and Terraform from HashiCorp. Furthermore, the paper compares these tools based on their functionality, security, backup mechanisms, and compatibility. Finally, the paper concludes with a discussion of which tool is more suitable for specific use cases.

Створення та управління хмарною інфраструктурою вручну може бути досить складним завданням, особливо коли над проектом працює розподілена команда. Саме в таких ситуаціях стане в нагоді інфраструктура як код (Infrastructure as Code).

Infrastructure as Code (скорочено IaC) – це підхід, який дозволяє автоматизувати завдання, які виконуються під час підготовки, настроювання та розгортання IT-інфраструктури[1]. IaC дозволяє використовувати файли конфігурації, написані описовими мовами програмування високого рівня, для автоматизації управління інфраструктурою. Практичні результати впровадження IaC посприяли поширенню ринку хмарних послуг, а також створенню все більшої кількості рішень IaC. AWS CloudFormation та Terraform – два сервіси IaC, які зараз є найбільш популярними.

Один з них може бути кращим за інший залежно від того, наскільки вони відповідають потребам інфраструктури. Щоб виявити слабкі та сильні місця кожного, було проведено порівняння AWS CloudFormation та Terraform на основі їх особливостей, методами ведення логів, а також можливостей засобів безпеки та відкату до попереднього стану інфраструктури.

CloudFormation від Amazon Web Services – це веб-сервіс Amazon [2], який дозволяє створювати, надавати та керувати набором пов'язаних сервісів Amazon та сторонніх ресурсів. Вбудований дизайнер AWS Cloudformation спрощує додавання, налаштування та підключення різних ресурсів Amazon Web Services, тим самим спрощуючи управління інфраструктурою. Також до переваг можна донести візуалізацію інфраструктури, що полегшує проектування.

Terraform — це інструмент керування інфраструктурою з відкритим вихідним кодом, що не залежить від певного хмарного сервісу, розроблений HashiCorp, який забезпечує модульну конфігурацію інфраструктури, що дозволяє використовувати модулі будь-яких хмарних провайдерів в своїй інфраструктурі. Terraform відрізняється можливістю одночасного запуску кластерів, що складаються з модулів компонентів високого та низького рівня. Також можна створити налаштування Terraform, написавши файли конфігурації, які Terraform використовує для створення плану виконання для досягнення бажаного стану інфраструктури. І Terraform, і CloudFormation пропонують механізми захисту від ненавмисного видалення. Цей захист гарантує, що користувач не зможе видалити ресурси як залежність в інших додатках, тим самим значно знижуючи шанси на випадкове порушення інфраструктури. Робиться це за рахунок версіонування службового файлу, в який записується стан інфраструктури. Terraform виділяється своєю модульністю. Він включає вбудовану підтримку багатьох сторонніх модулів. Це досягається за допомогою провайдерів або плагінів, які реалізують свої типи ресурсів. Можна додати будь-який ресурс, будь-то від AWS, Google Cloud Platform, Microsoft Azure або інший, додавши провайдера до своєї конфігурації. CloudFormation використовує набори вкладених стеків або шаблонів як модулі. Ці вкладені стеки є будівельними блоками для інфраструктури і дозволяють імпортувати та експортувати стандартні параметри конфігурації. У цих випадках можемо створити спеціальний шаблон для таких ресурсів, який потім можна буде імпортувати в кожен стек, якому потрібний ресурс. Таким чином, у користувача може бути кілька конфігурацій ресурсів, які використовуються для різних інфраструктур. Запобігти виникненню помилок можна, використовуючи команду terraform plan, яка виводить список усіх майбутніх змін перед їх фактичним виконанням. Окрім цього, є можливість пробного прогону оновлення та перевірки вихідних даних, щоб переконатися, що всі зміни відповідають очікуванням, а потім зафіксувати зміни. Перш ніж ухвалити рішення про використання CloudFormation або Terraform, слід подумати про потреби команди та інфраструктури. Якщо в основному робота відбувається лише з ресурсами AWS, CloudFormation може краще підійти. Якщо інфраструктура залежить від багатьох сторонніх ресурсів, Terraform може підійти краще.

Список використаних джерел:

1. Брікман Є. Terraform: інфраструктура на рівні коду. – Себастополь .: O`REILLY. – 2020. – 368 с.

2. Лащевські Т., Арора К., Фарр Е. Хмарні Архітектури: розробка стійких хмарних додатків. – СПб .: Пітер. – 2021. - 320 с.

3. Таненбаум Е. Комп’ютерні мережі. – СПб .: Пітер. – 2002. – 848 с.

УДК 004.91

# ВИЛУЧЕННЯ ТЕКСТУ З ІНТЕРНЕТУ НА ОСНОВІ НАВЧАННЯ МАШИН

Шалатов В.О.
Науковий керівник – к.т.н., доц. Кривенко С.А.
Харківський національній університет радіоелектроніки, каф. ІМІ
м. Харків, Україна
тел. +38(012) 345-67-89, e-mail vasyl.shalatov@nure.ua,

In this work, Beautiful Soup is used to extract the titles, authors, summaries, published data, and hyperlinks from blog posts. The extracted text could then be used in a downstream NLP task, such as topic extraction, sentiment analysis, text-to-speech, or translation.

Першим етапом програми NLP є завантаження та обробка тексту. Цей етап можна розглядати як такий, що складається з трьох під етапів. По-перше, необхідно отримати дані з джерел даних. Наприклад, можна отримати текст із веб-сайтів або інших веб-ресурсів. Цей процес відомий як веб-збирання. Якщо виконується завантаження даних з документів, необхідно перетворити їх у форму, яку вимагає застосований компонент завантаження. Для більшості реальних програм є бажання автоматизувати процес вилучення. Витягнувши текст, його можна завантажити в конвеєр перетворення. Цей процес можна виконати за допомогою бібліотек Python, але також можна автоматизувати процес за допомогою Amazon Texttract. Нарешті, можна перетворити текст у числове представлення для використання обраної моделі навчання машин (ML). Метою даної роботи є розробка моделі використання Beautiful Soup [1], щоб видобувати заголовки, авторів, резюме, опубліковані дані та гіперпосилання з публікацій блогу. Щоб потім витягнутий текст можна було б використати в подальших завданнях NLP, таких як виділення теми, аналіз настроїв, перетворення тексту в мовлення або переклад. Повідомлення в блозі, яке аналізувалося, є блогом навчання машин AWS [2].

За допомогою веб-браузера була відкрита сторінка AWS Machine Learning. Використовувався режим інспектора браузера, щоб дізнатися структуру сторінки. У Mozilla FireFox і Google Chrome можна відкрити інспектор, натиснувши CTRL+SHIFT+C. Якщо використовується інший браузер, необхідно звертатися до документації браузера.

Були переглянуті різні елементи веб-сторінки, переміщаючи вказівник на сторінку. Переміщенням вказівника на наступні елементи було визначено, чи можна знайти теги, які використовуються для ідентифікації інформації: заголовок публікації в блозі; автор; дата публікації; короткий текст; гіперпосилання на публікацію в блозі.

Покрокова методика пошуку тегів наведена нижче.

Код статусу HTTP дорівнює 200, це передумова виконання наступних

кроків.

Вміст зі сторінки **content** був завантажений в об'єкт **soup**.

Всю сторінка доступна для перегляду за допомогою функції *soup.prettify()*.

Примітка. Вміст зі сторінки блогів AWS може бути довгим. Щоб перейти до наступного завдання, необхідно прокручувати блокнот **JupyterLab** вниз.

До всіх елементів сторінки можна отримати доступ за допомогою крапкової нотації (.). Таким чином, щоб переглянути заголовок, можна використовувати **soup.title**. Якщо потрібен лише текст, можна використовувати текстовий елемент **soup.h2.text**. **Best Egg** досяг утричі швидшого навчання моделі ML за допомогою автоматичного налаштування моделі **Amazon SageMaker.** Коли використовувався інспектор для пошуку тегів на сторінці блогів AWS, було виявлено, що вміст публікації в блозі впорядковано **organized/categorized/marked** позначено тегами <article>, які вказують на окрему одиницю вмісту.

Заголовок можна знайти на **soup.article.h2.span**. Щоб відобразити лише текст, використалась властивість *text*. Дата публікації статті знайдена за допомогою: *soup.article.time.text*. Далі короткий зміст статті витягнутий за допомогою: *soup.article.section.p.text*. Прізвище автора вказано у нижньому колонтитулі. Допис у блозі може мати кількох авторів. Однак спочатку було отримано лише першого автора: *soup.article.footer.span.prettify().*

Гіперпосилання на повний текст статті є останньою інформацією, яка була знайдена: *soup.article.a['href'].* Тепер коли були визначили всі відповідні елементи. Можна знайти всі статті за допомогою функції find_all(). Визначивши формат даних, можна додати результати до масиву. Далі був завантажений масив у фрейм даних **pandas**. Стовпець **published** тобто значення дати й часу були перетворені за допомогою метода *to_datetime().*

Ширину стовпця було налаштовано для **pandas** і відображені перші п'ять рядків фрейму даних.

Тепер, коли дані знаходяться у фреймі даних **pandas**, їх можна використовувати у наступних завданнях NLP.

Список використаних джерел

1. Beautiful Soup Documentation [Online]. Available: https://www.crummy.com/software/BeautifulSoup/bs4/doc/. [Accessed 24 03 2023].

2. AWS Machine Learning Blog [Online]. Available: https://aws.amazon.com/blogs/machine-learning/. [Accessed 24 03 2023].

УДК 004.75:621.391

# АНАЛІЗ ТА ОПТИМІЗАЦІЯ ВИТРАТ НА ХМАРНІ РЕСУРСИ В УМОВАХ НЕПЕРЕДБАЧУВАНОГО НАВАНТАЖЕННЯ В AWS

Кобзєв.В.Д
Науковий керівник – доц. Костромицький А.І
Харківський національний університет радіоелектроніки, кафедра ІМІ
м. Харків, Україна
тел. +38(050) 805 33 34, email: vadym.kobziev@nure.ua

In today's world, when more and more companies use cloud resources, the cost of maintaining these resources becomes a big problem. Unpredictable load on the infrastructure can lead to excessive use of resources and rising costs. This publication examines the analysis and optimization of cloud resource costs under unpredictable load conditions in Amazon Web Services (AWS).

У сучасному світі, коли все більше компаній використовують хмарні ресурси, витрати на підтримку цих ресурсів стають великою проблемою. Непередбачуване навантаження на інфраструктуру може призвести до надмірного використання ресурсів та зростання витрат. У даній публікації розглядається аналіз та оптимізація витрат на хмарні ресурси в умовах непередбачуваного навантаження в Amazon Web Services (AWS).

Розробка тестового стенду на основі AWS ElasticBeanstalk, AWS CloudWatch, Auto Scaling Group (ASG) та AWS Budget дозволяє розробити стратегію оптимізації витрат на основі дослідження.

Для порівняння ефективності систем без автоматичного масштабування та аналізу Budget та систем з їх використанням, будемо виконувати наступні кроки:

- Розгорнемо тестовий додаток на обох системах.
- Запустимо Apache JMeter для генерації навантаження на систему.
- Замінимо метрики використання ресурсів під час навантаження на систему, такі як використання процесора, пам'яті, мережі та інші.
- Порівняння результатів тестування та замірів метрик на обох системах.
- Візьмемо до уваги витрати на хмарні ресурси під час виконання тестів на обох системах.
- Порівняння результатів витрат на хмарні ресурси після використання AWS Budget.
- Розробимо автоматизацію за допомогою Terraform.
- Зробимо порівняння та відображення нашего плану оптимізації на схожі реальні проекти.

У отриманому результаті тестування додатку petclinic на більшу кількість запитів за допомогою Apache JMeter. за кількістю запитів, які були відправлені (10000), середній час відповіді на запит (105 мс), мінімальний

(51 мс) та максимальний (1024 мс) час відповіді на запит, кількість помилок (0) та відсоток помилок від загальної кількості запитів (0.00%) що занадто краще результату без використання автоматичного горизонтального масштабування.

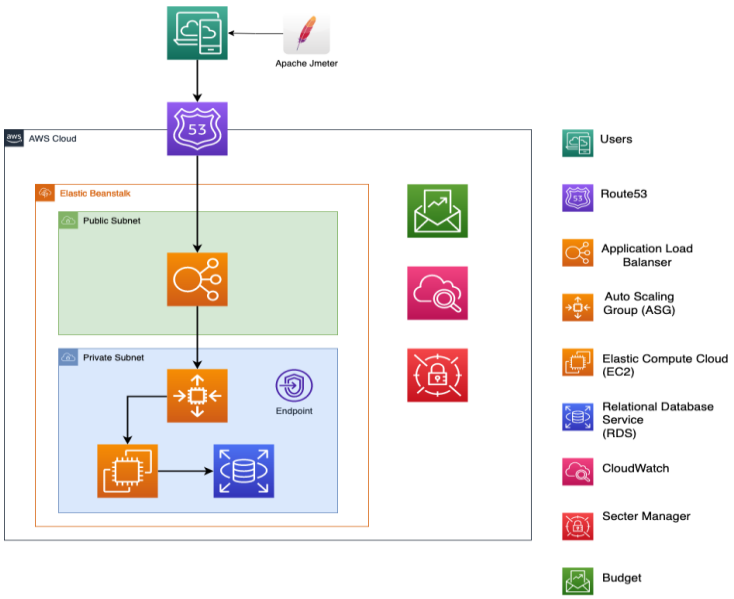



Рисунок 1 – Схема інфраструктури для тестування.

Отже, на основі проведених досліджень можна зробити висновок, що використання ASG та AWS Budget може значно зменшити витрати на хмарні ресурси в умовах непередбачуваного навантаження в AWS. Крім того, за допомогою Terraform була розроблена автоматизація, що дозволить легко застосовувати запропоновану стратегію оптимізації на реальних проектах в AWS та додає можливість швидкого встановлення інфраструктури в результаті аварії.

Список використаних джерел:

1. Amazon Web Services. (n.d.). AWS Elastic Beanstalk. [Електронний ресурс] / – 2021. – Режим доступу до ресурсу: https://aws.amazon.com/elasticbeanstalk/

2. Amazon Web Services. (n.d.). Amazon CloudWatch. [Електронний ресурс] / – 2022. – Режим доступу до ресурсу: https://aws.amazon.com/cloudwatch/

3. Amazon Web Services. (n.d.). Auto Scaling. [Електронний ресурс] / – 2021. – Режим доступу до ресурсу: https://aws.amazon.com/autoscaling/

4. Amazon Web Services. (n.d.). [Електронний ресурс] / – 2021. – Режим доступу до ресурсу: https://aws.amazon.com/budgets/

5. Apache JMeter. (n.d.). [Електронний ресурс] / – 2021. – Режим доступу до ресурсу: https://jmeter.apache.org

УДК 621.395

# МЕТОДИ ОЦІНКИ ЯКОСТІ МОВИ В IP-ТЕЛЕФОНІЇ

Кротінов А.П.
Науковий керівник – ас. Штих І.А.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. «Інформаційно-мережної інженерії»,
тел. (057) 702-14-29)
e-mail: inna.shtykh@nure.ua, тел. 0968264249

The work is devoted to the problems of IP telephony and factors that affect the quality of the IP network, including: delay, jitter, maximum bandwidth, packet loss, support for QoS mechanisms of channel-level technologies. Also, gateway quality factors: allowable bandwidth, delay, jitter buffer, packet loss, level control, echo cancellation. The main methods of assessing the quality of communication, which are currently used in IP telephony, are considered.

Для передачі сигналу використовують IP-шлюзи. Це пристрої за допомогою яких здійснюється трансляція даних з одного типа мережі в іншу. Їх ще називають IP-сервери. З одного боку до них можуть бути підключені телефонні лінії і можуть встановити зв'язок з яким завгодно телефоном в світі, а з другої – Інтернет – канали, які дозволяють з'єднатися з будь яким підключеним до Інтернет комп'ютера [1].

Якість мови як правило оцінюють через: розбірливість (виразність), натуральність, гучність.

Перша і основна вимога відображає виконання лінією зв'язку своєї головної функції – забезпечити, щоб той, хто слухає правильно зрозумів сенс того, що йому передається. Для цього мова має бути досить розбірлива.

Друга вимога – натуральність – оцінює здатність системи відтворювати не лише зміст передаваємої промови, але і її тембр, індивідуальні особливості голосів різних, що говорять.

Третя вимога – гучність – визначає бажаний рівень сигналів, що приймаються, який в оптимальному випадку має бути таким, щоб розбірливість мови досягалася без напруги слухового апарату з боку того, хто приймає.

Методи оцінки якості прийнято розділяти на суб'єктивні (якість передачі інформації не вимірюється якими-небудь числовими одиницями, а оцінюється умовним балом) і певної числової величини, не залежної від того, ким робляться виміри (об'єктивні) [1].

Основні методи оцінки якості зв'язку, які зараз використовуються в IP-телефонії [2]:

– найширше використовується підхід аналізу спотворень від компресії/декомпресії, який оперує оцінкою MOS (Mean Opinion Score), яка визначається для конкретного кодека як середня оцінка якості великою групою слухачів за п'ятибальною шкалою. Для прослуховування

пред'являються різні звукові фрагменти – мова, музика, мова на тлі різного шуму і інші варіанти. Недолік моделі MOS полягає в тому, що ця модель не може кількісно та окремо враховувати такі фактори: наскрізну затримку між абонентами; варіацію затримки (джиттер); втрати пакетів; відлуння (якщо в розмовному тракті є перехід з двопроводової схеми передачі до чотирипроводової чи навпаки).

– усунути недоліки MOS можна при використанні Е-моделі, яка дозволяє отримати оцінку якості на основі результатів вимірювання різних характеристик передачі пакетів та кінцевого обладнання. Ця модель дозволяє в комплексі врахувати практично всі несприятливі фактори. Е-модель – багатокритеріальна оцінка якості (R – фактор) в діапазоні від 1 до 120 балів, де 120 відповідає найвищому рівню якості.

– у системах цифрового зв'язку і IP–телефонії також може застосовуватися артикуляційний метод. Метод артикуляції оснований на забезпеченні розбірливої передачі мови. Мірою розбірливості служить розбірливість елементів мови – величина, визначувана як відношення числа правильно прийнятих елементів мови (звуків, складів, фраз, а стосовно IP - мовних пакетів) до досить великого загального числа переданих елементів. Розбірливість виражається у відсотках або в долях одиниці.

На відміну від перерахованих раніше заходів розбірливість безпосередньо не вимірюється (у рамках класичних підходів), проте являється єдиній з усіх перерахованих заходів розбірливості, яка може бути аналітично розрахована [2].

ITU -T в рекомендації G.114 визначив метод оцінки якості передачі мови через сумарну(наскрізну) затримку. Якість вважається хорошою, якщо наскрізна затримка при передачі сигналу в один бік не перевищує 150 мс Сучасне устаткування IP-телефонії при включенні "спина до спини" (два пристрої – шлюзи – з'єднуються безпосередньо) вносить затримку близько 60 –70 мс. Таким чином, залишається ще близько 90 мс на мережеву затримку при передачі IP- пакету від відправника до пункту призначення, що говорить про можливість забезпечити при сучасному рівні технології передачу мови з досить високою якістю [2].

Список використаних джерел:

1. Дэвидсон Д. Основы передачи голосовых данных по сетям IP, 2-е изд. / Дэвидсон Д., Питерс Д. и др.//: Пер. с англ. – М.: Издат. дом «Вильямс», 2007. – 400 с.

2. Вегенша Ш. Качество обслуживания в сетях IP: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 386 с.

УДК 621.396

# РОЗГОРТАННЯ СИСТЕМИ CORDECT У СІЛЬСЬКІЙ МІСЦЕВОСТІ

Славгородський Я.В.
Науковий керівник – ас. Штих І.А.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. «Інформаційно-мережної інженерії»,
тел. (057) 702-14-29)
e-mail: inna.shtykh@nure.ua, тел. 0968264249

The work is devoted to the corDECT subscriber radio access system, which is designed to provide simultaneous switching of language information channels and medium-speed Internet access in homes and offices; clearly demonstrates that a properly designed and deployed network enables cost-effective organization of telephone and Internet connections to rural subscribers in areas with extremely low subscriber density.

Забезпечення телефонним зв'язком та послугами Internet абонентів у сільських районах – основне завдання системи corDECT WLL. Система може забезпечити рентабельним зв'язком зони, де густина абонентів не нижче 0,2 абонентів на кв. км. Для більш низької щільності рентабельніше використовувати інші системи.

Для організації зв'язку в зонах з низькою абонентською щільністю необхідно наявність лінії прямої видимості між антеною абонента і CBS/RBS. У цьому випадку важливе ретельне планування розташування щогл та CBS/RBS для того, щоб забезпечити зв'язком усіх потенційних абонентів, розташованих у 10-кілометровому радіусі. Переважно так само, щоб антена абонента була розташована на височині або на щоглі з тим, щоб забезпечити лінію прямої видимості [1].

BSC і RAS можуть бути розташовані в будівлі обслуговуючої АТС або в будівлі лінійного віддаленого вузла, поруч із щоглою (зазвичай висотою від 15 до 35 метрів). CBS, встановлені на щоглі, можуть безпосередньо обслуговувати сільських абонентів у 10-кілометровому радіусі (іншими словами, покривати площу в 300 кв. км.) так, як показано на рис. 1. Цей сценарій розгортання системи використовується за абонентської щільності від 1 абонента на кв. км.

Для обслуговування анклаву абонентів у віддаленій зоні може застосовуватись BSD. BSD підтримує до чотирьох CBS, розташованих на віддаленій опорі та обслуговує абонентів у 10-кілометровому радіусі навколо неї, як показано на рис. 2. BSD вимагає організації резервного живлення у віддаленій точці. Подібна модель розгортання системи є рентабельною при абонентській щільності 0,2 абонента на кв. км, за умови наявності мікрохвильового релейного або оптоволоконного зв'язку [1].

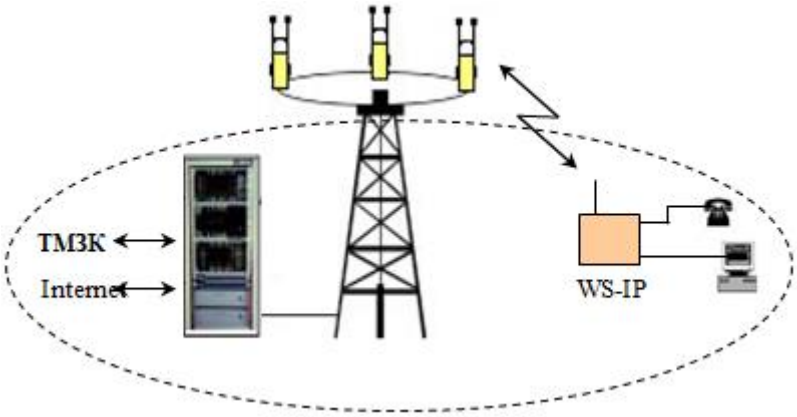



Рисунок 1 – Побудова мережі за абонентської щільності понад 1 аб./км$^2$

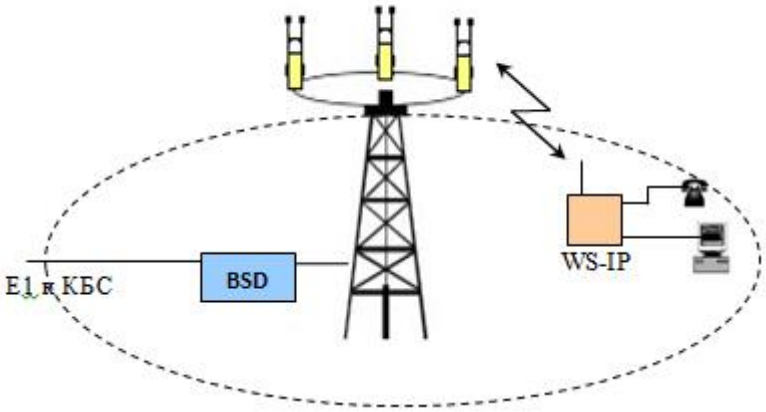



Рисунок 2 – «Сільське» рішення з використанням BSD

У разі, коли немає потоків E1, необхідне використання базових виносних станцій (RBS). RBS може бути встановлена на відстані до 25 км від розташування CBS, і забезпечити зв'язок між ними на лінії прямої видимості. Для подолання проблеми великої затримки передачі сигналу від RBS CBS, передача сигналу RBS сформована відповідним чином.

Кожна RBS обслуговує абонентів у 10-кілометровому радіусі. RBS підтримує 11 каналів та може встановити 11 одночасних з'єднань. Двопрогонова радіолінія забезпечує такі ж голосові та Internet послуги як однопрогонова. Для абонента підключення через RBS є прозорим. Для RBS потрібне власне джерело живлення з резервом, яке надходить від мережі або від батареї. RBS ефективна за абонентської щільності 0,2 абонента на кв. км [1].

Список використаних джерел:

1. Паван Джаноркар. Система абонентского радиодоступа «corDECT»// ООО «DECT Телеком», 2006. – 261 с.

УДК 681.516.73

# ВІДМОВОСТІЙКІСТЬ ПРОЦЕСІВ В РОЗПОДІЛЕНИХ СИСТЕМАХ

Копиця А.А.
Науковий керівник – ас. Штих І.А.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. «Інформаційно-мережної інженерії»,
тел. (057) 702-14-29)
e-mail: inna.shtykh@nure.ua, тел. 0968264249

The work is devoted to the methods of ensuring stability to the most divided system. Following a summary of the sing- ing basic statements about the stability to water, let's take a look at the nutritional stability of the processes and the supra-group strength. Under stiykistyu until vidmovi protsesiv my rozumiємo methods, for the help of such vidmova one or more processes to go through to solve the system may be unremarkable. Zim nutrition is associated with the problem of supergroup distribution, if the transfer of a set of processes is carried out with a guarantee of delivery.

Характерною рисою розподілених систем, що відрізняє їхню відмінність від одиничних машин, є можливість часткової відмови. Часткова відмова відбувається при збої в одному з компонентів розподіленої системи. Ця відмова може порушити нормальну роботу деяких компонентів, у той час як інших компонент це не торкнеться. На противагу відмові в розподіленій системі відмова в нерозподіленій системі завжди є глобальною, у тому сенсі, що вона зачіпає всі її компоненти і легко може призвести до непрацездатності всього додатку [1].

Кажуть, що система відмовляє, якщо вона не в змозі виконувати свою роботу. Зокрема, якщо розподілена система створювалася для надання користувачам деяких послуг, то система вважатиметься такою, що перебуває в стані відмови в тому випадку, якщо вона не зможе надавати всі або деякі послуги. Помилкою (error) називається такий стан системи, що може призвести до її непрацездатності. Так, наприклад, при передачі пакетів через мережу може статися, що деякі пакети, що прийшли до одержувача, виявляться пошкодженими. Ушкодження в даному випадку означатимуть, що одержувач може неправильно прочитати значення бітів (наприклад, 1 замість 0) або виявитися не в змозі визначити сам факт приходу пакета.

Причиною помилки є відмова (fault). Зрозуміло, що знайти причину помилки є дуже важливим. Так, наприклад, викликати пошкодження пакетів цілком може несправне або неякісне середовище передачі.

Основний підхід до захисту від наслідків відмови процесів – об'єднати кілька ідентичних процесів у групу. Основна властивість всіх подібних груп полягає в тому, що коли повідомлення надсилається групі, його отримують усі члени цієї групи. Таким чином, якщо один із процесів групи перестає працювати, можна сподіватися на те, що його місце займе інший [1].

Групи процесів можуть бути динамічними. Можуть створюватися нові групи та ліквідуватися старі. У ході системної операції процес може увійти до групи або залишити її. Процес може входити до кількох груп одночасно. Таким чином, нам необхідні механізми для управління групами та членством у них.

Групи віддалено нагадують громадські організації. Аліса може бути членом клубу книголюбів, тенісного клубу та товариства «зелених». У певні дні вона може отримувати листи (повідомлення), що повідомляють про нову книгу «Випічка для ювілеїв» з клубу книголюбів, про щорічний тенісний турнір, присвячений святу 8 Березня, з тенісного клубу та з товариства захисту природи про початок кампанії на захист південних бабаків. Будь-якої миті вона може залишити будь-який з них або всі ці клуби, або вступити до інших [1].

Мета групування полягає в тому, щоб перейти від розгляду окремих процесів до нової абстракції – групи процесів. Так, процес може посилати повідомлення групі серверів, не знаючи нічого про те, скільки їх там і де вони знаходяться, причому склад групи серверів при кожному виклику може бути різним.

Всі групи можна розділити відповідно до їх внутрішньої структури. У деяких групах усі процеси рівні між собою. Жодних начальників немає, і всі рішення ухвалюються колективно. В інших групах існує щось на кшталт ієрархії. Так, наприклад, один із процесів – координатор, а решта – прості виконавці. У такій моделі при появі запиту, створеного десь поза процесом або одним із внутрішніх робочих процесів, цей запит надсилається координатору. Координатор вирішує, який із виконавців найкраще впорається із запитом та передає йому цей запит [1].

Кожна з цих організацій має свої переваги та недоліки. Однорангова група симетрична і немає одиничної точки відмови. Якщо в одному з процесів виявляється помилка, група просто стає меншою, але продовжує існувати. Недолік однорангових груп у тому, що прийняття рішень більш складний. Так, наприклад, для того, щоб домовитися про щось, необхідно проводити голосування, що тягне за собою певну затримку та необхідність додаткових дій.

Ієрархічна група має протилежні властивості. Втрата координатора тягне у себе зупинку роботи всієї групи, але доки він у робочому стані, приймає рішення сам, нікого при цьому не турбуючи.

Список використаних джерел:

1. Таненбаум Э. Распределенные системы. Принципы и парадигмы / Э. Таненбаум, М. ван Стеен. – СПб.: Питер, 2003. – 877 с.

УДК 004:621.391]:004.6

# АНАЛІЗ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ SELENIUM ДЛЯ ВЕБ-СКРАПІНГУ ЗАДЛЯ ОТРИМАННЯ ДАНИХ З ОНЛАЙН РЕСУРСІВ ТА АВТОМАТИЗАЦІЇ ВЗАЄМОДІЇ ПРОГРАМНИМИ ЗАСОБАМИ

Мишко М.М
Науковий керівник – доц. Костромицький А.І
Харківський національний університет радіоелектроніки, кафедра ІМІ
м. Харків, Україна
тел. +38(099) 031 29 33, email: maksym.myshko@nure.ua

Web scraping is the process of extracting information from websites by collecting data through automated methods. This technique has become increasingly popular in recent years as the internet has become more central to our lives, and businesses have turned to the web to collect data and insights. Python is one of the most popular programming languages for web scraping. However, some websites use complex user interfaces or require authentication, which can make web scraping difficult.

Selenium is a popular tool for automating web browsers, which makes it easier to perform web scraping tasks that require interaction with the web page. In the study, we will explore the use of Selenium for web scraping, including its benefits and drawbacks, and discuss specific use cases where Selenium can be helpful.

Веб-скрапінг - це процес вилучення інформації з веб-сайтів шляхом автоматичної збирання даних. Ця техніка стала все більш популярною в останні роки, оскільки Інтернет став центральним елементом нашого життя, і бізнеси звертаються до Інтернету, щоб збирати дані та інсайти. Python є однією з найпопулярніших мов програмування для веб-скрапінгу.

Однак деякі веб-сайти використовують складні інтерфейси користувачів або потребують автентифікації, що може зробити веб-скрапінг складним. Selenium є популярним інструментом для автоматизації веб-браузерів, що полегшує виконання завдань веб-скрапінгу, які потребують взаємодії з веб-сторінкою.

Метою роботи є аналіз можливостей використання Selenium для веб-скрапінгу, включаючи його переваги та недоліки, і обговорити конкретні випадки, де Selenium може бути корисним.

Випадки використання:

- Одним з найбільш поширених випадків веб-скрапінгу з використанням Python і Selenium є збір даних з веб-сайтів для дослідження або бізнес-цілей.

Наприклад, бізнес може використовувати веб-скрапінг для збору інформації про конкурентів, тенденції на ринку або поведінку споживачів.

Дослідники можуть використовувати веб-скрапінг для збору даних для аналізу, таких як дані соціальних мереж або наукові дані. [1]

- Інший випадок використання Selenium - отримання авторизаційного токена, який може бути використаний для API-запитів. Багато веб-сайтів використовують API-запити для надання доступу до своїх даних, але вимагають авторизаційного токена, що має бути включений до кожного запиту.

За допомогою Selenium можна автоматизувати процес входу в систему та отримання авторизаційного токена, що дозволяє нам здійснювати API-запити.

Можливі проблеми та рішення:

- Однією з найбільших проблем веб-скрапінгу за допомогою Selenium є те, що він може бути повільнішим, ніж інші методи веб-скрапінгу. Оскільки Selenium потребує відкриття браузера та імітації взаємодії з веб-сторінкою, він може працювати повільніше, ніж використання запитів для отримання даних безпосередньо з сервера веб-сайту.

Однак, є декілька способів оптимізації продуктивності Selenium, таких як скорочення кількості взаємодій з веб-сторінкою або використання браузеру у «headless» режимі для уникнення рендерингу веб-сторінки на екрані. [2]

- Іншою проблемою веб-скрапінгу за допомогою Selenium є те, що він може бути менш надійним, ніж інші методи веб-скрапінгу. Оскільки Selenium ґрунтується на взаємодії з веб-сторінкою, будь-які зміни у макеті веб-сайту або структурі HTML можуть зламати скрипт скрапінгу.

Для зменшення ризику виникнення цієї проблеми важливо використовувати стабільні селектори, які менш схильні до змін, і моніторити веб-сайт на зміни, які можуть вплинути на працездатність скрипта.

Список використаних джерел:

1. Martin P. What is Web Scraping and What is it Used For? [Електронний ресурс] / Perez Martin. – 2021. – Режим доступу до ресурсу: https://www.parsehub.com/blog/what-is-web-scraping/.

2. Nadkarni S. Selenium Headless Browser Testing [Електронний ресурс] / Shilpa Nadkarni. – 2021. – Режим доступу до ресурсу: https://www.toolsqa.com/selenium-webdriver/selenium-headless-browser-testing/.

УДК 004:621.391]:004.056

# АНАЛІЗ АЛГОРИТМІВ ПОБУДОВИ ПРИХОВАНИХ КАНАЛІВ НА БАЗІ ТЕКСТОВОГО КОНТЕНТУ

Будянський В.С.
Науковий керівник – ст.викл. Твердохліб В.В.
Харківський національний університет радіоелектроніки, кафедра ІМІ
м. Харків, Україна
тел. +38(098) 92-98-128, e-mail: vadym.budianskyi@nure.ua

Today, algorithms for constructing hidden channels, which are based on the use of text-type media, can compete with algorithms that, in turn, focus on the use of video, graphic and audio containers.

Yes, today an extremely large number of, for example, web documents and accompanying files are transmitted over the network every second. These are, first of all, php, html, css, and external script files of various formats. Under such conditions, it makes sense to consider text steganography as one of the rather powerful tools for building hidden channels of data exchange.

Виконується аналіз методів стенографічного приховування на базі текстових носіїв з позицій забезпечення максимальної захищеності стеганограм, потенційно можливої емності носія та складності реалізації алгоритма

Серед стегонаграфічних алгоритмів орієнтованих на текстові дані поширення отримали: «хвостових пробілів», зміни порядку розміщення маркерів кінця рядку, використання візуально однакових символів, заміни коду символа пробіла.

Зазначимо що їх застосування буде найбільш ефективним в умовах використання веб-документів у якості носія, за цих умов методу хвостових пробілів як і методу заміни черговості символів кінця рядку теоретично доступна ємність контейнеру що дорівнює кількості рядків разом з тим враховуючи залежність між рівнем захищеності та ємністю стегосистеми, а саме $V\uparrow \rightarrow P\downarrow$, очевидно що використовуватися за цих умов може лише деяка частина доступної ємності. На користь цього свідчить також те, що виявлення стеганограм утворених подібним способом зводиться до зчитування даних у кінці рядку та пошуку закономірності у них, тобто ємність V необхідно мінімізувати. Разом з тим до переваг одного та іншого методу можна віднести простоту реалізації яка зводиться до:

- Позиціонування маркера у кінець рядку
- Зчитування символів кінця рядку
- Модифікація символів кінця рядку які необхідно вбудувати

У свою чергу метод заміни символу пробілу характеризується значно вищою ємністю порівняно до двох попередньо зазначених алгоритмів

оскільки вона визначається як V ~ S*k, де: S – кількість рядків у документі, k – середня кількість пробілів.

Як видно з виконаного аналізу методів добудовування прихованих каналів найвищою ємністю характеризується метод заміни символа пробіла, у той же час ємність методів хвостових пробілів та методу заміни черговості символів кінця рядку – найнижча, їхня ємність може бути у цілому прогнозованою, тоді як ємність методу заміни візуально однакових символів є апріорі невідомою та контентно залежною.

Алгоритм зміни порядку розміщення маркерів кінця рядку

В основі даного методу знаходиться несприйняття переважною більшістю засобів відображення текстових даних черговості розміщення символів переведення рядку CR та повернення каретки LF, які обмежують кожен рядок у текстовому масиві.

Алгоритм «хвостових пробілів»

При цьому, у кінці рядку файлу-носія вписується додатковий символ пробілу на той випадок, коли необхідно кодувати символ 1 повідомлення, яке вбудовується. При цьому, на випадок вбудовування нульового біту додатковий символ пробілу не вноситься.

Алгоритм на базі використання візуально однакових символів

В основі даного алгоритму знаходиться той факт, що ряд кириличних символів, а також символів латиниці є візуально аналогічними. При цьому, зрозуміло, що кожному з таких символів відповідають різні коди символьних таблиць.

Алгоритм заміни коду символа пробіла

Даний алгоритм базується на тому факті, що, зокрема, символ пробілу може бути представлено у межах текстового файлу з використанням різних числових кодів.

**Висновки:** Беручи до уваги виявлену специфіку реалізації методу заміни візуально схожих символів, у тому числі можливість вносити додаткові текстові наповнення даний метод може розглядатися як один з найбільш перспективних для подальшого вдосконалення одним з таких напрямків імовірно може бути розробка інформативних ознак, також залежних від контенту носія що вказуватимуть на ділянки тексту у межах яких буде виконуватися інкапсуляція прихованих даних.

Список використаних джерел:

1. Ватолин Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. – М. : ДИАЛОГ – МИФИ, 2003. – 384 с.

2. Чемпен Н., Чемпен Д. Цифровые технологии мультимедиа. – М.: Вильямс, 2006. – 624 с.

3. Мартинюк О.М., Попіна С.Ю., Елементи комбінаторики й класичне означення ймовірності. Тернопіль, 2003. – 40 с.

УДК 621.396:004.7

# АНАЛІЗ СТАНДАРТУ БЕЗДРОТОВИХ ЛОКАЛЬНИХ МЕРЕЖ IEEE 802.11AX

Фодченко А.В.
Науковий керівник – к.т.н., доц. Чеботарьова Д.В.
Харківський національний університет радіоелектроніки, каф. IMI,
м. Харків, Україна
тел. +38(097) 680-03-07, e-mail: anastasiia.fodchenko@nure.ua

This work is devoted to the analysis of the wireless LAN standard - 802.11ax. The paper analyzes the following advantages of IEEE 802.11ax: increased security, increased battery life, high speed even under load, increased access point bandwidth to support IoT and mobile devices, reliability-oriented speed and beams, 8X8 spatial streams for simultaneous use. To create a more secure, interconnected, secure and efficient environment, it is advisable to use IEEE 802.11ax.

Під час пандемії COVID-19 та війни в Україні багато процесів переведено в режим онлайн, що надзвичайно збільшило використання бездротового зв'язку для доступу до інтернету. Зростаюча кількість джерел Wi-Fi сигналу та обсягу трафіку, перевантаження мереж та проблеми з підключенням через кілька пристроїв стали для українців більш суттєвими, ніж раніше. Допомогти у вирішенні цих проблем може застосування нового стандарту Wi-Fi 6, що може забезпечити користувачам більш швидкий і стабільний бездротовий інтернет.

Нове покоління Wi-Fi 6 розроблене для задоволення зростаючої потреби в ємності та гарантує, що пристрої Wi-Fi можуть продовжувати надійно працювати в переповненому середовищі. Wi-Fi 6 базується на стандарті 802.11ax Інституту інженерів з електротехніки та електроніки (IEEE) [1]. Wi-Fi 6 пропонує кілька переваг, які дозволяють знайти нові рішення для таких завдань, як безпека та ефективність, покращений зв'язок між машинами через IoT та миттєвий доступ до потокового контента.

Бездротові мережі починають використовувати переваги нових функцій WPA3, що допомагає забезпечити безпеку бездротової мережі. Акредитація Wifi Alliance вимагає обов’язкове використання цієї функції у Wi-Fi 6, крім того в цій технології розширено можливості для запобігання хакерам і посилення шифрування.

Wi-Fi 6 має функції, що дозволяють ефективно переводити налаштування Wi-Fi певних пристроїв у «сплячий режим», коли вони не використовуються. Це вивільняє пропускну здатність за рахунок сплячих з'єднань, які не використовуються і відкривають їх для інших активних пристроїв.

Для створення більш захищеного, взаємопов'язаного, безпечного та ефективного середовища доцільно використовувати Wi-Fi 6, що має низьке

енергоспоживання та збільшує використання крихітних датчиків IoT. Оскільки цим пристроям не вистачає ємності батареї, вони покладаються на більш ефективні вимоги до живлення Wi-Fi 6, які використовують фіксований зв'язок за розкладом через цільовий час пробудження [2].

Підвищена щільність пристроїв часто призводить до зниження швидкості. Wi-Fi 6 використовує при надсиланні сигналу множинний доступ з ортогональним частотним поділом (OFDMA), що допомагає розділити навантаження. Таким чином одна точка доступу може обмінюватись даними з кількома пристроями одночасно. Це є істотною перевагою, коли необхідно підключити кілька пристроїв.

Wi-Fi 6 динамічно використовує блоки ресурсів, щоб точка доступу могла підтримувати кілька клієнтів одночасно, використовуючи менші канали всередині каналів для додатків з нижчою пропускною здатністю [2]. Продуктивність підвищується в областях з кількома підключеними пристроями, і споживачі будуть менше конкурувати за смугу пропускання. В стандарті Wi-Fi 6 суттєво збільшено пропускну здатність точки доступу, що зменшує затримки та повне зависання під час відео- і аудіо сеансів. Wi-Fi 6 підтримує конфігурації з антенами до 8×8:8, що забезпечує збільшення швидкості та дозволяє декільком користувачам «говорити» одночасно [2].

Формування променя фокусує сигнал на потрібному шляху замість рівномірного розподілення його по області. Це допомагає підвищити надійність та швидкість з'єднання.

Варто також звернути увагу на деякі недоліки Wi-Fi 6. Wi-Fi 6 має менший радіус дії порівняно з мережею 5 ГГц, і сигнали перериватимуться частіше, якщо між маршрутизатором і пристроєм буде перешкода [3]. Крім того, Wi-Fi 6 не забезпечує набагато більшої швидкості для пристроїв, які не підтримують її.

Таким чином, в роботі проаналізовано переваги та недоліки технології IEEE 802.11ax та запропоновано її використання для вирішення актуальних проблем в галузі надання швидкісного бездротового інтернету.

Список використаних джерел:

1. Wi-Fi 6E: Wi-Fi® in the 6 GHz band [Електронний ресурс] // Wi-Fi Alliance. – 2023. – Режим доступу до ресурсу: https://www.wi-fi.org/downloads-registered-guest/Wi-Fi_6E_paper_202112.pdf/37285.

2. Chiradeep BasuMallick. What Is Wifi 6? Meaning, Speed, Features, and Benefits [Електронний ресурс] / Chiradeep BasuMallick // Spiceworks. – 2022. – Режим доступу до ресурсу: https://www.spiceworks.com/tech/networking/articles/what-is-wifi-six/#_004.

3. Is Wi-Fi 6 Worth the Upgrade: Introduction to What's New in Wi-Fi 6 for Home Users [Електронний ресурс] // Speedefy. – 2023. – Режим доступу до ресурсу: https://www.speedefy.com/article/is-wifi-6-worth-upgrade-and-what-is-new-in-wifi-6/#:~:text=Cons%3A,that%20don't%20support%20it.

УДК 004.451:004.732

# АДМІНІСТРУВАННЯ ОПЕРАЦІЙНИХ СИСТЕМ ПРИ ПОБУДОВІ ЛОКАЛЬНОЇ МЕРЕЖІ

Соцька В.В.
Науковий керівник – ас. Штих І.А.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. «Інформаційно-мережної інженерії»,
тел. (057) 702-14-29)
e-mail: inna.shtykh@nure.ua, тел. 0968264249

This work is devoted to the construction of a local network followed by the administration of operating systems, since an important step is to specify the network settings correctly. For administration, it is necessary to specify all parameters on each network device for the correct and high-quality operation of the network, and for this there are two options, which are described in the work, Cisco hardware configuration is also demonstrated.

Для мережного адміністрування операційних систем важливо правильно вказати налаштування мережі. Під мережними налаштуваннями розуміють [1]:

- IP-адреса пристрою – унікальна в межах локальної мережі адреса, однозначно ідентифікуючий пристрій;
- маска підмережі – 32-бітове число, яке дозволяє визначити приналежність мережного пристрою до тієї чи іншої підмережі;
- стандартний шлюз – адреса мережного пристрою, на який буде відправлено пакет у тому випадку, якщо адресат не належить до підмережі відправника;
- сервер DNS – спеціалізований сервер, який перетворює мережеві імена, що легко запам'ятовуються в IP-адреси, і навпаки.

Отже, для адміністрування необхідно вказати ці параметри на кожному мережному пристрої. Для цього існують два шляхи [2]:

- вказати параметри мережі вручну для кожного пристрою. Це найпростіший шлях, але у разі великої локальної мережі – дуже складний варіант для адміністратора;
- використовувати динамічне налаштування параметрів мережі. В такому у разі мережний пристрій буде автоматично отримувати параметри із сервера. Такий варіант простіше для адміністрування, але вимагатиме налаштування сервера.

У локальній обчислювальній мережі, що створюється, було застосовано обидва варіанти налаштування. Серверне обладнання та мережні принтери було налаштовано з використанням статичної адресацію – оскільки багато програмного забезпечення звертається до серверів за IP-адресами, а можлива зміна адреси мережної принтера може внести сум'яття в роботу користувачів.

Робочі місця користувачів будуть отримувати налаштування мережі з сервера DHCP, що спростить їхнє адміністрування.

Також важливим аспектом адміністрування є контроль доступу до обладнання та контроль мережного доступу до ресурсів. Контроль доступу до обладнання в даній роботі буде продемонстровано шляхом налаштування прав доступу до комутаторів. Контроль мережного доступу в обладнання Cisco реалізується за допомогою списків контролю доступу, ACL [2].

Оскільки таке завдання в даній роботі не було поставлено, тому цього налаштовувати не було здійснено – але можливість виконання такого контролю є, для цього достатньо створити списки контролю доступу на кореневому комутаторі.

Реальне обладнання Cisco первинно налаштовується через консоль, а потім може бути налаштовано або через консоль, або через мережне підключення. При цьому, з метою збереження безпеки мережі, важливо не залишати можливості неконтрольованого підключення до обладнання. Для цього необхідно встановити пароль на доступ до консолі, а також встановити пароль на доступ до привілейованого режиму. Це робиться такими командами [2]:

```
line con 0
password cisco
login
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
service password-encryption
```

В результаті таких команд на устаткуванні буде встановлено пароль на підключення до нього – Cisco, аналогічний пароль буде встановлено на доступ до привілейованого режиму.

Список використаних джерел:

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010. – 944 с. – ISBN 978-5-49807-389-7.

2. Бен Пайпер. Администрирование сетей Cisco: освоение за месяц / пер. с анг. М. А. Райтман – Litres ,2022. – 317 с. – SBN 978-5-97060-519-6.

УДК 681.7:004.7

# ДОСЛІДЖЕННЯ ВПЛИВУ РІЗНИХ ФАКТОРІВ НА ОПТИЧНІ ВЛАСТИВОСТІ ОПТИЧНОГО КАБЕЛЮ

Козін А.О.
Науковий керівник – ас. Штих І.А.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. «Інформаційно-мережної інженерії»,
тел. (057) 702-14-29)
тел. +38(063) 542-66-76, email: artem.kozin@nure.ua.

This work is devoted to the influence of various factors on the optical properties of the optical cable, which include both internal and external losses. The optical properties of an optical cable, such as dispersion, signal loss, and others, play an important role in the efficiency and productivity of optical communication systems. Uncontrolled cable factors can cause signal degradation and reduced optical cable performance.

Оптичні системи являються основним засобом передачі даних по оптичним мережам зв’язку, забезпечуючи високошвидкісну та надійну передачу. Однак, ефективність його роботи може залежати від багатьох факторів, таких як довжина хвилі світла, типу оптичного кабелю, геометричні параметри кабелю, властивості навколишнього середовища та інші. Дослідження впливу цих факторів на оптичні властивості кабелю є важливою задачею, яка може оптимізувати проєктування й налаштування оптичних кабельних систем, а також підвищити їх продуктивність, надійність [1].

Було виявлено, що основними джерелами втрат в ОВ являються дисперсія, поглинання, Релеївське розсіювання, що призводять до послаблення світлового сигналу при його передачі вздовж волокна. Також було розроблено різні методи й технології для зниження втрат, такі як багатошарове покриття, покращення процесів виготовлення скляних волокон, оптимізація дизайну оптичного кабелю та інше.

Відкриття втрат в оптоволокні (рис. 1) мало велике значення для розвитку оптичної галузі зв’язку та телекомунікацій, оскільки дозволило вченим й інженерам розробити більш ефективні та надійні оптичні системи зв’язку, котрі сьогодні широко використовуються по всьому світові.

Оптичні властивості оптичного кабелю, такі як дисперсія, втрати сигналу та інші, грають важливу роль в ефективності й продуктивності оптичних комунікаційних систем.

Неконтрольовані кабельні фактори можуть викликати деградацію сигналу і зниження продуктивності оптичного кабелю. Деякі з цих факторів включають [1]:

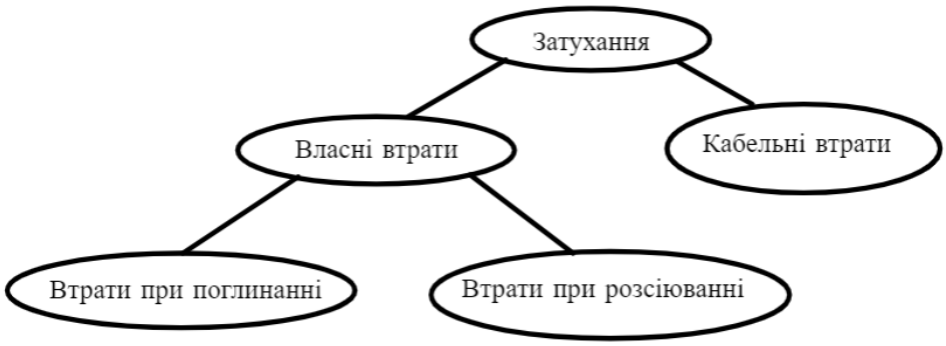



Рисунок 1 – Класифікація втрат в оптичному кабелю

– довжина кабелю: оптичний кабель може втрачати сигнал через великі відстані між проміжними системами. Чим довше кабель, тим більше загасання сигналу, що може обмежувати максимальну відстань передачі даних;

– вигини: вони можуть викликати додаткові втрати сигналу через розсіювання світла і порушення оптичної структури волокна. Правильний монтаж та обслуговування оптичного кабелю, що включає уникання гострих вигинів, є важливим фактором для підтримання високої продуктивності;

– температура: високі чи низькі температури можуть впливати на оптичні властивості, викликаючи теплове розширення чи стискання волокна, що може привести до механічного напруження. Це особливо важливо для систем, що працюють в екстремальних умовах, таких як підводні кабелі або кабелі в космічних умовах;

– забруднення: забруднення пилом, брудом чи іншими зовнішніми речовинами може викликати розсіювання світла та втрати сигналу. Регулярне очищення і захист оптичних конекторів від забруднення є важливим фактором для підтримки високої якості передачі;

– механічний вплив: фізичний вплив, такі як удари, вібрації, стискання та розтягування, викликають пошкодження оптичного кабелю та впливають на оптичні властивості.

Дослідження втрат в оптичному кабелі має важливе значення для розуміння та оптимізації процесів передачі оптичних сигналів в оптичних волокнах. Втрати в оптичних кабелях дозволяють інженерам розробляти більш ефективні методи зниження втрат й підвищення продуктивності оптичних систем.

Список використаних джерел:

1. Фокин В.Г. Оптические системы передачи и транспортные сети. Учебное пособие. – М.: Эко-Трендз, 2008. – 271 с.

УДК 621.391:004.773.7

# ПІДВИЩЕННЯ НАДІЙНОСТІ ТА ОПТИМІЗАЦІЇ ТРАФІКУ ВІДЕО КОНФЕРЕНЦ ЗВ'ЯЗКУ

Шрамко В.С.
Науковий керівник – проф. Шубін І.Ю.
Харківський національний університет радіоелектроніки,
каф. Програмної інженерії
м. Харків, Україна
тел. +38(099) 936-83-94, email: vitalii.shramko.cpe@nure.ua

This work is about increasing the reliability and traffic optimization of video conference communication. The author discussed the main challenges and solutions to improve the performance of video conferences, and presented a set of techniques to reduce the network bandwidth requirements and improve the video quality.

В останні роки відеоконференцзв'язок став невід'ємною частиною бізнесу, освіти, охорони здоров'я та інших сфер. З появою пандемії COVID-19 попит на надійний та оптимізований відеоконференцзв’язок значно зріс. Однак, незважаючи на наявність високошвидкісного Інтернету та передових технологій відеоконференцій, користувачі все ще стикаються з кількома проблемами, такими як проблеми з підключенням, низька якість відео та затримки в передачі. Тому існує нагальна потреба вирішити ці проблеми та підвищити надійність і оптимізацію трафіку відеоконференцзв’язку.

Основна мета цієї дисертації — дослідити та запропонувати вирішення проблем, пов’язаних із зв’язком у режимі відеоконференції, зокрема щодо надійності та оптимізації трафіку. Дисертація буде зосереджена на таких дослідницьких питаннях:

Які загальні виклики пов’язані з відеоконференцзв’язком?

Як вирішити ці проблеми, щоб підвищити надійність відеоконференцій?

Як можна застосувати методи оптимізації трафіку, щоб зменшити затримку та покращити якість відео під час відеоконференції?

Щоб відповісти на ці дослідницькі запитання, дисертація розпочнеться з надання вичерпного огляду існуючої літератури з відеоконференцзв’язку. У цьому огляді будуть визначені проблеми та обмеження, пов’язані з відеоконференціями, зокрема проблеми з підключенням до мережі, обмеження пропускної здатності та затримки в передачі. Він також вивчатиме різні технології та методи, які зараз доступні для вирішення цих проблем.

Далі в дисертації буде запропоновано декілька рішень для підвищення надійності відеоконференцзв’язку. Ці рішення включатимуть використання резервної передачі даних, адаптивного потокового відео та інструментів моніторингу мережі. У дисертації також розглядатиметься ефективність цих

рішень за допомогою моделювання та експериментів, порівнюючи продуктивність відеоконференцій до та після впровадження цих рішень.

Формула для розрахунку часу проходження відеоконференції (RTT) виглядає так:

$$RTT = t2 - t1$$

Де t1 — час, коли клієнт надсилає повідомлення, а t2 — час, коли клієнт отримує підтвердження від сервера.

У дисертації також будуть досліджуватися методи оптимізації трафіку, включаючи формування трафіку, стиснення та кешування. Ці методи можуть зменшити затримку та покращити якість відео під час відеоконференції. У дисертації буде запропоновано структуру оптимізації трафіку, яка об’єднує ці методи та оцінює їх ефективність за допомогою експериментів і моделювання.

На завершення ця дисертація спрямована на підвищення надійності та оптимізацію трафіку відеоконференцзв’язку. Визначаючи проблеми та обмеження, пов’язані з відеоконференціями, і пропонуючи ефективні рішення для їх усунення, ця теза може сприяти розвитку відеоконференцзв’язку та його застосування в різних сферах.

Список використаних джерел:

1. Литвин, В. В., & Лапік, О. В. (2017). Методи забезпечення якості відеоконференцій. Інформаційні технології та комп'ютерна інженерія, 2(40), 73-81.

2. Карпухін, М. Ю. (2017). Оптимізація мережі передачі даних для відеоконференцій. Проблеми телекомунікацій, 3(14), 26-36.

3. Тютюнник, О. В., Литвин, В. В., & Лапік, О. В. (2019). Аналіз методів забезпечення якості відеоконференцій в умовах розподілених мереж. Вісник Національного університету "Львівська політехніка". Комп'ютерні науки та інформаційні технології, 933, 153-160.

4. Грищук, Є. І., & Клименко, Н. В. (2018). Підвищення якості відеоконференцій з використанням технології адаптивної потокової передачі даних. Вісник Національного університету "Львівська політехніка". Комп'ютерні науки та інформаційні технології, 900, 79-86.

5. Mirkovic, J., Reiher, P., & Zhang, L. (2018). Analysis of Network Performance for Video Conferencing. IEEE/ACM Transactions on Networking, 26(3), 1188-1201.

УДК:681.7:004.7]:004.056

# ПОКРАЩЕННЯ ЗВ'ЯЗКУ ПРИ ЗАХИСТІ ІНФОРМАЦІЇ В ОПТОВОЛОКОННИХ ЛІНІЯХ

Ярова О. С.
Науковий керівник – доцент кафедри ІМІ, к.т.н., Харченко Н.А.
Харківський національний університет радіоелектроніки 61166, Харків, просп. Науки,14, каф. Радіотехніки, тел. (057) 702-00-00
gmail: oleksandra.iarova@nure.ua.
Контактний номер телефону: 380995024536.

With the development of technology and circuitry IC has emerged the creation of a single electronic devise, such as a radio receiver, meter or control unit, on one crystal.

In the 21st century, there is telecommunications equipment: antenna, switch, router, VoIP gateway, modem, secret connection technology... Each telecommunications equipment is connected with its own cable to work on the network: optical fiber, twisted pair, coaxial cable, telephone cable.

An important part in ensuring communication is to correctly configure all communication equipment in the network so that there are no errors in operation and a stable connection is established with the desired communication center.

Насамперед, висока якість зв'язку це головна мета кожного зв'язківця, в оптоволоконних лініях передачі даних особливо важливо цю якість підтримувати, бо надання інфокомунікаційних послуг на великі відстані значно підвищує вимоги до характеристик системи передачі. Тому на початку проектування мережі, визначаються головні параметри (наприклад, пропускна здатність, відстані між вузлами, підключення додаткового обладнання), від яких буде залежати технологія передачі, по якій вже буде підбиратися обладнання для функціонування мережі.

На якість зв'язку великий вплив мають саме параметри побудови оптичної мережі: правильність вибору прокладки оптоволоконного кабелю, вибір типу кабелю, рівень якості пайки кабелю, перевірка кожного оптичного волокна рефлектометром після прокладання і після пайки, правильне встановлення муфт на лінії, використання якісних конекторів і оптичних адаптерів.

Також особливу увагу необхідно приділяти параметрам встановлюваного обладнання: оптичних підсилювачів, компенсаторів дисперсії, транспондерів Можна використовувати моделі різних компаній, але так, щоб вони були сумісні в роботі, також є обов'язковою відповідність стандарту для забезпечення переходу з оптики на звиту пару.

Також, незважаючи на те, що оптичний зв'язок має досить високий рівень захисту інформації, у випадках передачі секретної інформації повинно застосовуватися додаткове обладнання. Встановлення ЗАЗ обладнання (криптографічні засоби захисту інформації) є одним з

найвідповідальніших етапів надання спецзв'язку, бо воно має відповідати закону України. Налаштування засекречувальної апаратури зв'язку виконують спеціально навчені спеціалісти з відповідним рівнем допуску. Звісно, що кожен вид обладнання буде мати свої особливості налаштування та програмного забезпечення. Прописування конфігурації допускається одним або двома спеціалістами, що залежить від необхідного рівня захисту інформації у обладнанні (1 або 2 КД). Підключається ЗАЗ апаратура одразу після приймача, і далі інформація подається на маршрутизатори і комутатори, які передають по системі вже захищену інформацію, такий вид зв'язку називають закритим, а у поєднанні з оптичною мережею передачі він буде мати високі показники якості. ЗСОІ (захищена система обміну інформації), за законом, кожне її обладнання і його ключі мають бути поставлені на облік. При наказі зміни ключів або обладнання, потрібно виконувати дії за законом і приписом: привозити обладнання можуть тільки спеціальні служби, встановлення обладнання виконується тільки фахівцями з потрібним допуском СІ, старі ключі та ЗАЗ обладнання зі старими журналами обслуговування передаються службам безпеки на перевірку, а потім знищуються.

Висновок

Для отримання якісної мережі зв'язку, треба чітко виконувати всі етапи починаючи з планування і закінчуючи побудовою та фінальним тестуванням базових характеристик спланованої мережі.

Закритий зв'язок представляє собою звичайну побудову оптичної мережі, але перед передавальним обладнанням одразу підключається ЗАЗ, що шифрує інформацію, що тим самим покращує якість зв'язку.

В побудові мережі зв'язку і її експлуатації беруть участь велика кількість спеціалістів, які роблять свою спаву (якусь окрему), бо кожен етап виконують кваліфіковані працівники і вони слідкують за своїм обладнанням, у випадках поломки чи помилки в мережі, швидко вирішують проблеми, це підвищує якість мережі, що дуже важливо.

Список використаних джерел

1. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. (2010). Телекомунікаційні та інформаційні мережі: Підручник для вищих навчальних закладів.

2. Шолудько В.Г., Єсаулов М.Ю., Вакуленко О.В., Гурський Т.Г., Фомін М.М. (2017). Організація військового зв'язку. Навчальний посібник.

3. Шифратор з інтегрованим модулем керування. Взято 10 квітня 2023 з http://www.tritel.ua/index.php/ru/produktsiya/sposobi-kzi/pelena-e2013-04-29-12-26-44/gnom-e2013-04-29-12-27-07/shifrator-s-integrirovannym-modulem-kommutatsii-detail.

УДК 004.032.2:621.391

# РОЗРОБКА WEB-ЗАСТОСУНКУ ДЛЯ СПІЛКУВАННЯ РОБІТНИКІВ ІТ-КОМПАНІЇ

Красніков В. О.
Науковий керівник – ас. каф. ІМІ, Ляшенко Г.Є.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м.Харків, Україна
E-mail: vsevolod.krasnikov@nure.ua

This work is devoted to the creation of a web application to improve the interaction of IT company employees. The web application will allow convenient communication between employees, exchange information and manage projects. In the report will cover the main stages of developing and testing a web application, including user interface design, technology selection, and functionality development and testing. In the report will also provide information about the benefits of using a web application in the work of an IT company and its impact on increasing the efficiency and productivity of the work process.

У сучасному світі ефективна комунікація між працівниками є однією з основних складових успішної роботи будь-якої організації, особливо в галузі ІТ. Однак відсутність стабільної та швидкої мережі Інтернет може значно ускладнити процес комунікації між колегами, а також з партнерами та клієнтами. Це особливо актуально на сьогоднішній день в Україні, де зникнення мережі Інтернет може не тільки призвести до затримки в роботі та уповільнити спілкування в компанії, а навіть відкинути розробку на початкові етапи.

Метою даної доповіді є опис розробки веб-додатку, який дозволяє працівникам ІТ-підприємства спілкуватися між собою незалежно від наявності мережі Інтернет. Перевагою розробки є ефективне та зручне використання застосунку, який дозволяє працівникам взаємодіяти між собою, вести трекінг роботи та вирішувати завдання в офлайн-режимах за умови що мережа працює не надійно з помилками та затримками, що призводить до уповільнення робочого процесу і зниження ефективності робітників[1].

У доповіді наводиться опис прототипу такого додатка у вигляді веб-додатка. Для розробки було використано мову програмування Java та фреймворк Spring Boot[2]. Для збереження даних та повідомлень було створено базу даних з використанням систем керування реляційними базами даних MySQL. Для оформлення зовнішнього вигляду застосунку використовувався додаток Bootstrap, який має відкритий доступ і код.

Розроблений веб-додаток має безліч переваг для комунікації між працівниками ІТ-підприємства, зокрема: він забезпечує зручний та ефективний інтерфейс для взаємодії між робітниками, дозволяє вести таск трекінг та вирішувати завдання незалежно від наявності мережі Інтернет[3], підвищує ефективність та швидкість роботи в цілому, забезпечує

збереження даних та повідомлень навіть при відсутності мережі Інтернет, дозволяє працювати в офлайн-режимі. Розроблений прототип додатку може бути допрацьований та удосконалений залежно від потреб конкретної IT-компанії. Крім того, розроблений додаток може бути корисним для будь-якої компанії, яка працює в умовах обмеженої доступності мережі Інтернет.

Таким чином, розроблений додаток може значно спростити та поліпшити комунікацію між працівниками IT-компанії, особливо в ситуації, коли мережа Інтернет недоступна або є ненадійною[4]. Крім того, з використанням додатку забезпечується можливість трекінгу роботи та вирішення завдань в офлайн режимі, що є важливим умовою продуктивної роботи в умовах недоступності Інтернету.

На основі результатів тестування, яке було проведено з ціллю дослідження повноцінної роботи застосунку в “реальних умовах”, можна зробити висновок, що розроблений застосунок є досить ефективним інструментом для покращення взаємодії та комунікації між робітниками IT-компанії. Розробка даного застосунку може бути корисною для будь-якої компанії, що працює у галузі IT, та забезпечить надійну та швидку комунікацію між працівниками в будь-яких умовах.

Крім того, важливо зазначити, що розроблений додаток має потенціал для подальшого розширення та вдосконалення. Наприклад, можна додати нові функції, які можуть поліпшити співпрацю між колегами: спільне редагування документів, обмін файлами або організацію віртуальних зборів. Застосунок також можна адаптувати для використання на мобільних пристроях, що дозволить працівникам зв'язуватися між собою незалежно від їх місцезнаходження.

Враховуючи стрімкий розвиток технологій, швидкий та стабільний доступ до Інтернету стає все більшою необхідністю для успішної роботи. Однак, в ситуаціях, коли підключення до мережі обмежене або відсутнє, розроблений додаток може стати незамінним інструментом для забезпечення безперебійного спілкування та продуктивної роботи команди. Інноваційні рішення, які дозволяють працювати в офлайн-режимі та забезпечують збереження даних, відкривають нові можливості для підприємств у будь-якій галузі. Розробка такого додатку є важливим кроком у напрямку покращення комунікації та роботи в умовах залежності від доступу до Інтернету.

Список використаних джерел

1) Schoeffner, A. (2018). Offline First Web Development: Design, develop, and deploy your first offline-ready web applications.

2) Mishra, S. (2017). Building Offline-First Mobile Apps.

3) Kapila, A. (2015). Developing Offline-First Web Applications.

4) Firtman, M. (2016). Offline First: Creating Mobile Web Applications.

УДК 004.032.2:621.391

# АНАЛІЗ МОЖЛИВИХ ЗАГРОЗ В КОРПОРАТИВНИХ МЕРЕЖАХ

Лінник М.В.
Науковий керівник – ас. каф. ІМІ Ляшенко Г.Є.
Харківський національний університет радіоелектроніки,
м. Харків, Україна
тел. +38(099) 422-25-62, e-mail: maksim.linnik@nure.ua

This work is devoted to the main vulnerabilities in the local networks or in the internet space and devoted to the ways to protect against these vulnerabilities. How to protect yourself from cyber-attacks, phishing, and other attacks. How to behave properly in the online space to avoid the risk of being attacked and avoid personal data leakage.

У сучасному світі корпоративні мережі стали необхідністю для більшості компаній. Вони дозволяють зберігати, обробляти та передавати важливу інформацію, тим самим створюючи великий потенціал для підвищення продуктивності та ефективності. Однак, кількість загроз, які можуть впливати на корпоративні мережі та цілі компанії, зростає з кожним днем.

Метою роботи є аналіз загроз які можуть впливати на роботу корпоративної мережі, а також дослідження технології захисту від мережних вразливостей.

Кібератаки є одними з розповсюджених загроз які спрямовані на викрадення конфіденційної інформації, розповсюдження вірусів, вимагання викупу, або навіть на знищення даних.

Для захисту від кібератак, компанії можуть використовувати різні технології, такі як брандмауери, антивірусні програми, системи виявлення вторгнень та інші. Також важливо вдосконалювати системи безпеки, періодично проводячи тестування на проникнення, що дозволяє виявляти слабкі місця та вносити необхідні зміни в систему. Необхідно також забезпечити надійну автентифікацію користувачів, щоб уникнути несанкціонованого доступу до мережі[1].

Відомий метод соціальної інженерії, який використовується для отримання конфіденційної інформації, такої як логіни та паролі, від користувачів - це фішинг. Зазвичай, цей метод реалізується шляхом надсилання повідомлення, яке здається легітимним, але фактично є спробою отримати доступ до даних користувача[2].

Щоб запобігти таким атакам, користувачам необхідно бути обережними та перевіряти, що електронні листи та повідомлення є від легітимних джерел.

DDoS-атаки (атаки на збої в роботі мережі) - це атаки, при яких велика кількість запитів з небезпечних джерел змушують мережу працювати

повільніше або зупинятися повністю. Це може викликати серйозні проблеми з доступом до даних та виконанням бізнес-процесів.

Фізичні загрози, такі як викрадення або пошкодження обладнання, можуть викликати зупинку мережі та втрату даних. Обладнання повинно бути фізично захищене, та необхідно робити резервні копії даних, щоб забезпечити їх відновлення в разі втрати.

Іншою можливою загрозою є внутрішні загрози. Вони можуть бути здійснені працівником, який має доступ до конфіденційної інформації та може використовувати її для власних цілей. Для того щоб ізолювати себе від внутрішніх загроз, потрібно встановлювати певні правила щодо доступу до конфіденційної інформації та моніторингу дій користувачів.

Крім того, необхідно проводити регулярну оцінку ризиків та надавати навчання працівникам щодо безпеки мережі та її складових. Працівники повинні знати про можливі загрози та знаходити шляхи їх запобігання.

К внутрішнім загрозам також відносяться ризики з боку партнерів та підрядників, такі як компанії технічної підтримки або зовнішні постачальники програмного забезпечення. Потрібно вимагати від своїх партнерів та підрядників дотримання високих стандартів безпеки та встановлювати строгі правила доступ у до своїх систем та даних[1].

Найбільш небезпечна загроза - це різноманітне зловмисне програмне забезпечення, таке як троянські програми, шпигунські програми, рекламне програмне забезпечення та інші. Це ПЗ може використовуватися для крадіжки конфіденційної інформації, перехоплення трафіку мережі, блокування доступу до даних та інших шкідливих дій.

В результаті роботи було проведено аналіз кіберзагроз а також технологій захисту корпоративної мережі. Для підвищення безпеки доцільно встановлювати комплексні заходи безпеки та регулярно їх оновлювати. Доцільно створювати політику безпеки, яка визначає правила та процедури для захисту мережі та даних, включаючи процедури для управління паролями, процедури резервного копіювання, заборону використання неофіційного програмного забезпечення та інші правила.

Список використаних джерел:

1. Тимофєєва, І. Б., (Уклад.). (2017). Збірник матеріалів наукового круглого столу. «Кібербезпека та системи захисту інформації: виклики сьогодення».

2. Мехед, Д. Б., Ткач, Ю. М., & Базилевич, В. М. (2019). Дослідження технологій впливу та методів протидії фішингу. Захист інформації, 21(4), 246–251. https://jrnl.nau.edu.ua/index.php/ZI/article/view/14338.

УДК 004.032.2:621.391

# ТЕХНОЛОГІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РОЗУМНОГО БУДИНКУ

Поддельський В.М.
Науковий керівник – ас. каф. ІМІ, Ляшенко Г.Є.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м.Харків, Україна
E-mail: vladyslav.poddelskyi@nure.ua

This report discusses the growing popularity of smart homes with the development of the Internet of Things (IoT), which offers a variety of solutions to help people in their daily lives. Smart homes are designed to perform functions such as security, privacy, energy management, and other functions based on the needs of the homeowner. The aim of this work is to study the issue of privacy and security in smart homes, as well as to identify potential types of attacks and countermeasures. It also discusses various types of attacks, including physical attacks, denial-of-service attacks, and man-in-the-middle attacks, and suggests defence methods such as cryptographic algorithms to protect the storage and transmission of information.

На сьогоднішній день, з розвитком інтернету речей (IoT), розумні будинки стали більш доступними та популярними серед споживачів. IoT пропонує безліч рішень, які можуть допомагати людям у повсякденному житті. Розумні будинки є одним із найкращих варіантів. Як правило, такі будинки проектуються для виконання певних функцій, таких як безпека, конфіденційність, управління енергоспоживанням, та інших функцій.

Метою цієї доповіді є дослідження питання конфіденційності та безпеки розумного будинку, а також виявлення можливих видів атак та способів протидії їм. В роботі було розглянуто наступні види атак, такі як фізичні атаки, атаки типу “відмова в обслуговуванні” (DoS), “людина посередині” та інші[1].

Бездротова сенсорна система може бути вразлива до атак типу “відмова в обслуговуванні”, яка відбувається коли зловмисник використовує ПК для передачі повідомлення задля втручання в радіочастотний канал. Ця атака здійснюється шляхом безперервної передачі повідомлень з метою перевантаження каналу, що призводить до некоректної роботи датчика, так як він не може передати інформацію на сервер[2].

Атаки типу “людина посередині” також впливають на роботу всієї системи. В залежності від того, для чого зловмисник проводить атаку, ціль може різнитися. Наприклад, якщо атака направлена на порушення роботи, це може здійснюватися шляхом відправки хибних даних.

Фізичні атаки стосуються можливості зловмисника отримати фізичний доступ до сенсорів та пристроїв. Цей доступ дає змогу ряду атак бути спрямованими на знищення або викрадення пристроїв, незаконну модифікацію коду і отримання конфіденційної інформації, такої як дані авторизації, криптографічні ключі тощо.

В роботі було розглянуто методи захисту від більшості видів атак. Ключовим методом для забезпечення безпеки від кібератак є криптографічний метод. Криптографічні алгоритми використовуються для безпечного зберігання та передачі інформації. Існує два методи криптографічного шифрування – це симетричне та асиметричне. Симетричний алгоритм шифрування використовує один ключ, а асиметричний алгоритм використовує два різні[3].

Криптографічні алгоритми з асиметричним ключем потребують більше обчислювальної потужності та пам’яті, ніж симетричні алгоритми. Симетричний метод шифрування більш підходить для системи розумного будинку, оскільки датчики не мають достатньо ресурсів для виконання складної та ресурсоємної криптографії з відкритим ключем.

Таким чином, можна зробити висновок, що завдяки розвитку Інтернету речей (IoT) розумні будинки стали дуже популярними серед споживачів. Вони можуть значно полегшити повсякденне життя, забезпечуючи безпеку, конфіденційність, управління енергоспоживанням та інші функції. Однак, вони можуть бути вразливими до різних видів кібератак, таких як фізичні атаки, атаки типу DoS та атаки типу «людина посередині». Для того, щоб захистити систему від цих атак, необхідно використовувати криптографічні методи та інші методи захисту. Крім того, слід дотримуватися заходів безпеки, таких як контроль доступу та захист мережі від зловмисників.

Список використаних джерел

1. Fei Hu. (2016). Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations. CRC Press.

2. Young, C. (2019). Smart Home: Digital Assistants, Home Automation, and the Internet of Things.

3. Buchanan, M. (2020). The Smart Home Manual: How to Automate Your Home to Keep Your Family Entertained, Comfortable, and Safe. HomeTechHacker.

УДК 621.391:004

# ОСОБЛИВОСТІ ВИБОРУ РЕЖИМУ РОБОТИ МОДУЛІВ LORA EBYTE E32-433T20DT ПРИ ПОБУДОВІ МЕРЕЖІ ОПТИКО-ЕЛЕКТРОННИХ СТАНЦІЇ

Шлома О.К.
Науковий керівник – професор Шостко І.С.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Науки, 14,
кафедра Інфокомунікаційної інженерії ім. В.В. Поповського,
тел. (057) 702-13-20) e-mail: Oleksandr.shloma@nure.ua.

To configure the network of optical-electronic stations, it is necessary to take into account the features of wireless communication modules. EBYTE E32-433T20DT modules have 2 communication modes (data transmission with a fixed address and destination channel, or broadcast data transmission) and 4 operation modes (normal operation mode, wake-up mode, sleep mode with hibernation, and sleep mode with reduced power consumption). The operating modes are set using variable parameters M0 and M1. In normal mode, the module receives data from the UART or wireless interface, it is possible to transmit data in packet mode up to 58 bytes in size. The wake-up mode allows you to automatically add a preamble to the transmitted packet.

Модулі EBYTE E32-433T20DT за замовчуванням мають 2 режиму комунікації і 4 режими роботи. Режим роботи може бути оновлений лише коли закінчить черга на передачу даних. Режими роботи задаються зміною параметрів M0 та M1 мережевого девайса [1].

Перша форма комунікації - це передача даних в режимі з фіксованою адресою та каналом призначення. Значення для керування передаються у 16-річному форматі. Наприклад, у пакеті вказана адреса 0x0002 та канал 0x04, що означає, що пакет буде прийнятий лише модулем з адресою 0002, який слухає 4 канал, інші модулі відкинуть цей пакет. На рис. 1.1 зображена фіксована передача даних.

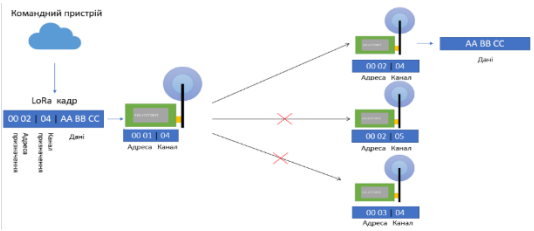



Рисунок 1.1 – Фіксована передача даних

Другий режим комунікації передбачає широкомовну розсилку даних. В пакеті встановлюється адреса у вигляді 0x00 0x00 або 0xFF 0xFF, а також канал, наприклад 0x04. Усі модулі, що слухають 4 канал, отримають цей пакет. Важливо зазначити, що відправник не обов'язково має слухати саме той канал, на який він розсилає пакети. На рис. 1.2 показано приклад широкомовної розсилки даних.

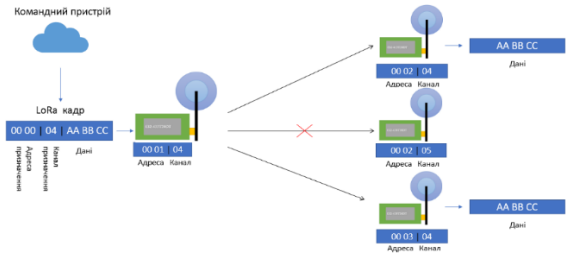



Рисунок 1.2 – Широкомовна передача даних

Модулі зв'язку мають чотири режими роботи. Ці режими задаються параметрами M1 та M0. Режими рахуються з 0 до 3.

Нормальний режим роботи має номер 0. В цьому режимі модуль приймає сигнали від UART або бездротового інтерфейсу. Параметри M0 та M1 мають значення 0. Максимальний розмір пакета - 58 байт. Як тільки з контролера приходять дані і пакет набуває свого максимального розміру - відразу починається процес передачі даних. Пакети формуються і передаються послідовно, якщо розмір введених даних менший за 58 – програма буде очікувати декілька секунд і почне передавати дані. Інший модуль може отримати ці дані якщо він має режим 1 або 0.

Режим пробудження має номер 1, де Модуль продовжує приймати сигнали від UART або бездротового інтерфейсу, M0 приймає значення 1, M1 має значення 0. Особливість цього режиму полягає в автоматичному додаванні преамбули до кожного пакету, що дозволяє пробудити модуль-отримувач з режиму збереження енергії (режим 2). Цим самим інший модуль може отримувати пакети, якщо він працює у режимі 0, 1 або 2.

Режим збереження енергії має номер 2, де значення M1 дорівнює 1, M0 має значення 0. В цьому режимі UART закривається для прийому, а бездротовий інтерфейс очікує на пакет зі спеціальною преамбулою від іншого модуля, який працює в режимі 1.

Режим сну, або режим 3, має значення M1 та M0, рівне 1. Цей режим використовується для коригування внутрішніх налаштувань модулів E32.

Висновки:

Таким чином для повсякденних задач буде використовуватись режим номер 0, тобто звичайний режим роботи, а параметри M1 та M0 модулю EBYTE E32 будуть дорівнювати 0. Це забезпечить повноцінне функціонування безпроводової мережі. Для збереження енергії може використовуватись режим номер 2, при якому параметри M1 та M0 приймають значення 1.

Список використаних джерел

1. Шлома О. К. Алгоритм дистанційного керування приводами лазерної оптико-електронної станції по can-шині / О. К. Шлома, І. С. Шостко. // ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОКОМУНІКАЦІЙ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ ТЕХНОЛОГІЙ. – 2020. – №4. – С. 36–37.

**УДК 004:621.317**

# ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТЕХНОЛОГІЇ, МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ, СТАНДАРТИЗАЦІЯ І СЕРТИФІКАЦІЯ

УДК 627.71:656.614.3

# ПРАКТИЧНЕ ЗАСТОСУВАННЯ КООРДИНАТНОГО КУРСОРУ ECDIS В ЯКОСТІ КУТОМІРНО-ДАЛЕКОМІРНОГО ПРИСТРОЮ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ПЛАВАННЯ ВЕЛИКОГАБАРИТНИХ СУДЕН КОНТЕЙНЕРОВОЗІВ

Любарець І.О.
Науковий керівник – к.т.н., доц. Давидов Володимир Семенович
Державний університет інфраструктури та технологій, каф. навігації та управління суднами, м. Київ, Україна
Тел.: +380953685289, e-mail: Ilyubarec@gmail.com

In this work, the practical use of the coordinate cursor of the electronic chart display information system (ECDIS) as an angle-range measuring device for increasing the safety of navigation of large container ships is proposed. Installation of additional antennas of the Global Positioning System (GPS) on the bow and stern of the vessel and using the coordinate cursor of ECDIS as an angle-range-measuring device - will provide possibility to measure the distance from the bow and stern extremities of the vessel to the nearest dangers with extreme accuracy.

Однією з важливих проблем сучасного судноплавства є забезпечення безпеки плавання великогабаритних суден контейнеровозів в прибережних водах і стиснених умовах, на які, як показує статистика, припадає близько 30% аварійних морських пригод [1]. Справа в тому, що розміри найбільших контейнеровозів сьогодні сягають 400 та 60 м. в довжину та ширину, відповідно. Це не могло не вплинути на керованість таких суден, яка суттєво погіршилася зі збільшенням розмірів. Іншим негативним наслідком збільшення габаритів суден контейнеровозів стала неможливість визначення точного положення носової та кормової кінцівок, що є дуже важливо при маневруванні суден в стиснених умовах. Отже, зважаючи на статистичні дані, загальноприйняті сьогодні засоби навігації та управління, виявилися нездатні в повній мірі забезпечити безпеку експлуатації великогабаритних суден контейнеровозів.

Однією з основних проблем є те, що на таких суднах відсутні технічні засоби, які б дозволили точно спрогнозувати місцезнаходження основних точок корпусу судна (носу та корми) на траєкторії руху. Немає ефективного засобу, який би вимірював відстань від носової та кормової кінцівок судна до навігаційної небезпеки з точністю до кількох метрів. Ті засоби, які використовують сьогодні, мають надзвичайну низьку ефективність при застосуванні в умовах обмеженої видимості. Вимірювання відстані за допомогою інфрачервоних далекомірів, встановлених на носовій та кормовій кінцівках судна стає практично неможливим в умовах обмеженої видимості, адже промінь лазера не здатний проникати крізь стінку дощу чи туману. Таким чином, судноводії великогабаритних суден не мають змоги

визначити ризик аварії на самій ранній стадії. Якщо, скажімо, підхід до причалу відбувається в умовах сильно обмеженої видимості (туман, злива, снігопад, і т.д.), контроль дистанції від носової та кормової кінцівки до причальної стінки стає критично важливим. Коли судно маневрує безпосередньо біля причалу на дуже малій швидкості (1-2 вузли), або ж на місці, за допомогою буксирів - його полюс повороту практично залишається в одній точці, в той час, як носова та кормова кінцівки суттєво приближуються чи віддаляються від причалу [2]. Величину зміни відстаней від кінцівок до причалу судноводій може знати лише приблизно. Основну небезпеку таїть динаміка їх зміни. Чим швидше зменшується відстань – тим менше часу для прийняття рішення залишається у судноводія.

Проте можливо, на носовій та кормовій кінцівках судна встановити додаткові до основної антени GPS. Необхідно автоматизувати в електронній картографічній навігаційній системі процес автоматичної координатної прив'язки, захоплення і супроводу кінцями рухливих координатних курсорів, що виходять з високоточних позицій носа і корми судна на електронній карті навігаційних орієнтирів, що мають високоточну геодезичну основу і координати яких внесені в електронну базу ECDIS. При точному збігу координат навігаційних орієнтирів з координатами кінців координатних курсорів судноводій отримує з точністю до 3,5 м., положення носа і корми свого судна на траєкторії руху і буде в змозі контролювати їх положення по напрямкам і дистанціям відносно орієнтирів або навігаційних небезпек [3]. Завдяки цьому можна було б миттєво передбачити розвиток небезпечної ситуації та прийняти необхідні міри. Комплексне використання таких можливостей ECDIS та системи рознесених на край судна приймачів GPS для контролю розташування носа та корми великогабаритних контейнеровозів, щодо навігаційних небезпек за допомогою координатного курсору, значною мірою доповнить можливості радіолокаційних станцій та засобів автоматичної радіолокаційної прокладки з контролю дистанції, збільшить точність її визначення за рахунок більш точного знання поточних географічних координат носа та корми судна з GPS, що працюють у спеціальних режимах.

Список використаних джерел:

1. Jasna Prpić-Oršić , Joško Parunov & Igor Šikić (2014) Operation of ULCS - real life, Int. J. Nav. Archit. Ocean Eng. (2014) 6:1014~1023, http://dx.doi.org/10.2478/IJNAOE-2013-0228;

2. Вульфович Б.А. Основи судноводіння. Мурманськ, МГТУ, 174 с., 2008.

3. Seaspirit (травень 2012) Точность спутниковых навигационных систем https://seaspirit.ru/navigator/navigation/tochnost-sputnikovsystem.html.

УДК 53.08:620.178.5

# РЕЗОНАНСНІ ЯВИЩА ПРИ ДОСЛІДЖЕННІ ВІБРАЦІЇ МЕХАНІЗМІВ

Стахова А.П.
Науковий керівник – д.т.н., проф. Квасніков В.П.
Національний авіаційний університет, каф. КЕСТ
м. Київ, Україна
тел. +380679131272, e-mail: sap@nau.edu.ua

The paper provides a theoretical consideration of resonance. The reasons for the occurrence of resonance of oscillatory motions are considered. The effect of resonance in an oscillatory system is considered.

Визначення динамічних характеристик окремих агрегатів, вузлів та механізмів необхідно виконувати на стадіях проектування, модернізації, зміни конструкції деталей та способів кріплення під час експлуатації. Це викликано тим, що динамічні характеристики механізмів визначають здебільшого надійність та ресурс самих механізмів.

У багатьох випадках окремі вузли та агрегати мають хороші технічні та вібраційні характеристики, надійність та ресурс, а в зборі механізми мають резонансні явища, які вимагають суттєвого доведення механізму чи агрегату. Причиною такого стану механізмів є невдалий розподіл власних частот, згинальних коливань по довжині зібраних агрегатів, рухливості у поєднаннях деталей та місцях монтажу агрегатів.

Визначення динамічних характеристик макетних та дослідних зразків вузлів механізмів дозволяє виключити вимушені та власні коливання елементів машин, які можуть спричинити резонансні вібрації при дії на конструкцію заданих внутрішніх та зовнішніх сил. При доведенні машин необхідно враховувати фактичні структурні та функціональні стани об'єктів випробувань, підвищення при експлуатації збурювальних сил, які збуджуються несправностями, що погіршують робочі процеси, зазорами, ослабленням посадок і механічних зв'язків. Оскільки функціональні характеристики багато в чому залежать від пружних властивостей елементів змінної жорсткості [1], що демпфують, таким чином облік коливань у сполученнях елементів вузлів механізмів і нестабільності робочих процесів має важливе значення.

Проаналізуємо залежність повного механічного опору від частоти змушувальної сили

$$z = \sqrt{r^2 + \left( m\omega - \frac{k}{\omega} \right)^2} = \frac{m}{\omega} \sqrt{4\delta^2\omega^2 + \left( \omega^2 - \omega_0^2 \right)^2}$$

При близькості своєї частоти системи $\omega_0 = \sqrt{k/m}$ реактивний опір $m\omega - k/\omega$ стає малим, а при $\omega = \omega_0$ перетворюється в нуль; при цьому повний опір $z = r$. На великій відстані від $\omega_0$ абсолютна величина

реактивного опору, а значить і $z$ сильно зростає як при дуже малих, так і при дуже великих частотах.

Простежимо, як змінюється амплітуда (рис. 1) швидкості вимушених коливань за зміни частоти зовнішньої сили. При дуже малих частотах $z$, великий член $k/\omega$ і тому амплітуда швидкості близька до нуля.

Збільшуючи частоту пружний опір $k/\omega$ зменшується, а інерціальний опір $m\omega$ збільшується; повний опір зменшується, і амплітуда швидкості зростає.

При $\omega = \omega_0 = \sqrt{k/m}$ маємо $m\omega = k/\omega$, і реактивний опір стає рівним нулю, амплітуда швидкості сягає найбільшого значення $v_0 = F_0/r$, а різниця фаз $\varphi_0$ між силою і швидкістю зникає.

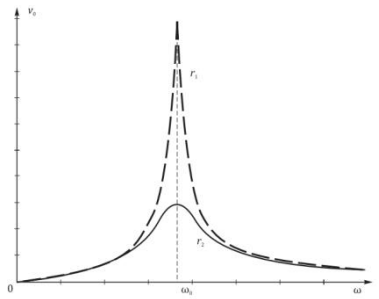


Рис. 1. Резонансна крива для швидкості

З подальшим підвищенням частоти інерційний опір стає більшим за пружний, повний опір зростає, і амплітуда швидкості зменшується. При збільшенні частоти значно більше резонансної ($\omega \to \infty$) повний опір $z \to \infty$, тобто коливальна система залишається майже нерухомою, не встигаючи слідувати за силою.

Гострота максимумів істотно залежить від $r$. Великому тертю $r_2$ відповідає полога крива зі слабко вираженим максимумом, а при малому терті $r_1$ - гостра крива із високим максимумом. При $r = 0$ максимум кривої прямує до безкінечності.

Система з дуже великим тертям або система поблизу резонансу, в якій $m\omega - k/\omega << r$, матиме імпеданс, близький до величини $r$. Її коливання будуть визначатися тільки тертям, тому в цьому випадку говорять про систему, керовану тертям.

Вібрація, створювана ударним рухом деталей, повинна модулюватись (одним дефектом) один раз за оборот валу, створюючи амплітудно-модуляційні бічні смуги. У кожному спектрі можна чітко бачити характерну частоту прояву несправності (дефекту) з бічними смугами модуляції розподіленими через інтервали, кратні частоті обертання валу, і навпаки, комбінаційних частот, що містять частоту обертання вала та деякі її гармоніки, які відсутні при справній роботі вузла.

Кількість та амплітуди бічних смуг використовуються для діагностики причин та розмірів дефекту. Вихід за межі допустимих значень амплітуд бічних смуг, отриманих на етапі діагностики, є аварійним сигналом розвитку несправності вузла.

Список використаних джерел:

1. Мигаль В.Д. Вибродиагностика машин при эксплуатации / В.Д. Мигаль. - Х.: ХГПУ, 1997. - 293 с.

УДК 004:621.391]:658.8

# VALUE STREAM MAPPING ЯК ІНСТРУМЕНТ ВІЗУАЛІЗАЦІЇ ТА ОПТИМІЗАЦІЇ ВИРОБНИЧОГО ПРОЦЕСУ

Довгополий С.О.
Науковий керівник – к.т.н., ст. викл. Мощенко І.О.
Харківський національний університет радіоелектроніки, каф. ІВТ,
м. Харків, Україна
тел. +38(095) 857-96-02, e-mail: serhii.dovhopolyi@nure.ua

This paper is devoted to the consideration of value stream mapping (VSM) - a visual representation of the production process that helps to identify waste and improve efficiency. It also highlights the importance of lean manufacturing and VSM as essential tools to enable businesses to remain competitive and produce high quality products with minimal waste By implementing lean manufacturing principles and utilizing VSM, businesses can optimize their operations, reduce costs, and increase customer satisfaction. This paper emphasizes the significance of VSM in today's competitive business environment.

Сьогодні перед будь-яким підприємством, що намагається підвищити свою конкурентоздатність, постають питання: Як покращити якість продукту? Чи є виробництво конкурентоспроможним? Які мінімізувати втрати? Для вирішення питань зменшення непродуктивних втрат при виробництві провідні світові компанії використовують модель управління якістю Lean Production. Бережливе виробництво (Lean Production) – це комплексна система організації підприємства та управління ним, за якої продукція виготовляється згідно із запитами споживачів з мінімальною кількістю витрат ресурсів. Бізнес України починаючи з 2018 року поступово впроваджує цю систему. Але більшість стартапів ще не знають про цю модель, що призводить до недоцільних втрат. Тому аналіз та рекомендації щодо застосування інструментів управління якістю, які пропонує модель Lean Production, є актуальною задачею.

Основою управління якістю виробництва продуктів та послуг, згідно ДСТУ EN ISO 9001:2018, є процесний підхід, який рекомендує розглядати організацію, як мережу взаємодіючих процесів [1]. Для візуалізації і оптимізації виробничих процесів в моделі Lean Production застосовується інструмент «Карта потоку створення цінності (VSM – Value Stream Mapping)». VSM — це візуальне подання виробничого процесу, яке розробляється у вигляді блок-схеми, що відображає всі етапи виробничого процесу, від постачання сировини до доставки готового продукту до споживача [2]. Метою VSM є позбутися усіх видів марнотратства, і досягти максимальної ефективності використання ресурсів. VSM також допомагає визначити можливості для оптимізації процесів, покращення якості та скорочення витрат.

Результати, яких можна досягти за допомогою VSM: Підвищення ефективності процесів: Скорочений час виконання: Покращена якість: Підвищення прибутковості: Покращена комунікація та співпраця: Підвищення рівня задоволеності клієнтів:

Практичне застосування аналізу VSM було змодельоване на прикладі підприємства ПАТ «Чернігівський завод радіоприладів» Завданням було візуалізувати всі процеси, пов'язані з виробництвом та життєвим циклом продукту з метою подальшого аналізу VSM. Використовуючи метод VSM, було проведено картографування потоку створення цінності на підприємстві ПАТ «Чернігівський завод радіоприладів». За результатами картографування був розрахований коефіцієнт часу додавання вартості, який дорівнює загальному часу додавання вартості поділеному на загальний час циклу, і в ідеальному випадку наближається до одиниці (21 год/352 год). Коефіцієнт дорівнює приблизно 0,06 (підприємства намагаються досягти значення 0,2, як досить високого рівня якості потоку створення цінності). Тому зроблено висновок щодо необхідності провести аналіз і оптимізацію потоків створення цінності з метою максимізації коефіцієнту часу додавання вартості.

Аналізуючи VSM ПАТ «Чернігівський завод радіоприладів», можна зробити наступні висновки: 1) Перший блок VSM «Прийом комплектуючих» виконує функцію тимчасового зберігання прийнятого товару, це марна витрата як ресурсу на оренду, так і людино-годин. Підприємство може відмовитися від цього вузла, транспортуючи прийнятий товар одразу до відділів. 2) Третій блок «Калібрування та налаштування конвеєра виробництва». Підприємство випускає товар як під конкретне замовлення покупця, так і для заповнення полиць складів відділів, що приводить до надлишку товару який не реалізується. Це також є недоцільною розтратою людино-годин. 3) Четвертий і п'ятий блок у часі розкидані на два повні робочі дні. Процеси, які виконує підприємство за два дні, правильно буде реалізувати в один день. Це допоможе підприємству швидше отримувати готовий продукт.

Подальше проведення дослідження в даному напрямку передбачає розробку VSM майбутнього стану та ідеального стану для використання інформації для максимального усунення непродуктивних витрат та оптимізації процесів ПАТ «Чернігівський завод радіоприладів».

Список використаних джерел:

1. Мощенко, І.О., Нікітенко, О.М., Козлов, Ю.В. (2022). Візуалізація інструментів контролю якості циклу PDCA засобами інформаційно-комунікаційних технологій. Збірник наукових праць ОДАТРЯ, 1(20), 6-15.

2. Семенычев, Ф.А. (2013). Стоимость ≠ ценность. Современные методики картирования потоков создания ценности с применением правила 80/20. Animedia Company.

УДК 658.56

# ТЕХНІЧНА ЕКСПЕРТИЗА ЕЛЕКТРОДВИГУНІВ

Сошенко Д.Д.
Науковий керівник – к.т.н., доц. Дегтярьов О.В.
Харківський національний університет радіоелектроніки, каф. ІВТ
м. Харків, Україна
тел. +38(097) 111-58-87, e-mail: denys.soshenko@nure.ua

The purpose of the work is to provide technical expertise of electric motors by developing metrological support for testing electric motors. Research methods – a comparative analysis of the existing regulatory framework for the safety of electric motors, measurement methods of controlled parameters, test methods. The essence, purpose, tasks and content of tests of safety parameters of electric motors are considered. The normative documents are proposed in accordance with which tests of safety parameters of electric motors are carried out. The program of tests of parameters of safety of electric motors is offered. Proposed test methods and control, measuring and testing equipment.

Якість - сукупність властивостей і характеристик продукції або послуг, що надаються продукції або послуг здатність задовольняти обумовлені або передбачені потреби людства.

Технічна експертиза - процес доказу того, що певні вимоги, що стосуються якості продукції, були виконані. Об'єктами технічної експертизи є конкретні матеріали, продукція, установки, на які поширюється *оцінка відповідності*. Відповідно до Закону України «Про технічні регламенти та оцінку відповідності» *оцінка відповідності* – процес доказу того, що певні вимоги щодо продукції, процесу, послуги, системи, особи або органу були виконані. Відповідно до Технічного регламенту низьковольтного електрообладнання [1] нормативним забезпеченням технічної експертизи електродвигунів в Україні є такий стандарт: ДСТУ 2331-93 Машини електричні асинхронні потужністю до 400 кВт включно. Двигуни. Вимоги безпеки та методи випробовувань.

Згідно діючих національних стандартів при технічній експертизі з метою оцінки безпеки електродвигунів необхідно виконати наступні випробування:

1. Зовнішній огляд та перевірка інструкції.
2. Випробування відповідність ступеня захисту.
3. Вимірювання опору ізоляції.
4. Випробування електричної міцності ізоляції.
5. Температурні випробування.
6. Перевірка рівня звуку.
7. Вимірювання вібрації.

На основі [2, 3] запропоновано програму технічної експертизи та випробувань параметрів безпеки двигунів електричних [табл.1].

Таблиця 1. Види випробувань при технічні експертизі двигунів електричних ассинхронних обертових

| Вид випрбування | Стандарт на метод випробування |
|---|---|
| 1. Зовнішній огляд та перевірка інструкції | ДСТУ 2331-93 |
| 2. Випробування відповідність ступеня захисту | ДСТУ IEC 60034-5:2005 |
| 3. Вимірювання опору ізоляції | ДСТУ 2331-93 |
| 4. Випробування електричної міцності ізоляції | ДСТУ 2331-93 |
| 5. Температурні випробування | ДСТУ 2331-93 |
| 6. Перевірка рівня звуку | ДСТУ IEC 60034-9:2003 |
| 7. Вимірювання вібрації | ДСТУ IEC 60034-14:2003 |

Запропоновано методи випробувань та контрольно-вимірювальне та випробувальне обладнання.

Випробування ступеня захисту IPX_ проводилися з використанням випробувального обладнання - стандартні щупи, камера пилу. Випробування ступеня захисту IP_X проводилися з використанням камери штучного дощу. Встановлено, що оболонка електродвигунів забезпечує захист від проникнення сторонніх предметів менше 1 мм і частковий захист від проникнення пилу, захист від водних бризок, що падають під будь-яким кутом - що відповідає ступеню захисту IP55.

Опір ізоляції електродвигунів вимірювався мегомметром на напругу 500 В щодо корпусу і між обмотками. Всі вимірювання опорів ізоляції обмоток електродвигунів проводилися практично в холодному стані обмоток, а також у стані близької до робочої температури обмоток. В результаті встановлено, що опір ізоляції струмопровідних частин не менше: у холодному стані за нормальних кліматичних умов – 30 МОм; при робочій температурі – 16 МОм; при верхньому значенні вологості повітря – 5 МОм.

Також проводилися температурні випробування. Ізоляція за нагрівостійкістю відповідає класу «F» витримує максимальну температуру 155 °С в термокамері типу КТХВ. Температура поверхні трохи більше 60 °С. Температура підшипника трохи більше 70 °С.

Список використаних джерел:

1. Технічний регламент безпеки низьковольтного електричного обладнання, затверджено постановою Кабінету Міністрів України від 16.12.15 № 1067 [Текст] // Офіційний вісник України. – 2016 – № 41. 45 с.

2. ДСТУ 2331-93 Машини електричні асинхронні потужністю до 400 кВт включно. Двигуни. Вимоги безпеки та методи випробовувань.

3. ДСТУ ISO/IEC Guide 60:2007 Оцінювання відповідності. Кодекс усталеної практики [Текст] – Введ. 01.01.08. – Київ: Держспоживстандарт України, 2008. – 6 с.

УДК 621.317:53.08

# РОЗРОБКА МЕТОДИКИ ОЦІНКИ НЕВИЗНАЧЕНОСТІ ВИМІРЮВАНЬ ПІД ЧАС КАЛІБРУВАННЯ АНЕМОМЕТРУ

Твердохліб Лілія
Науковий керівник – к.т.н., доц. Дегтярьов О.В.
Харківський національний університет радіоелектроніки, каф. ІВТ
м. Харків, Україна
тел. +38(099) 729-72-19, e-mail: liliia.tverdokhlib@nure.ua

The purpose of the work is to improve the metrological support for measuring speed of gas flow by developing a method of calibrating a digital anemometer. Research methods – methods of statistical analysis of measurement information, methods of uncertainty theory. The object of research is the uncertainty of digital anemometer verification. The results of repeated observations were processed. The standard uncertainty according to type A, B and the general standard uncertainty were determined. Budget the measurement uncertainty.

Анемометри – це засоби вимірювальної техніки, які використовуються для отримання оперативної інформації з прогнозування аварійних ситуацій, особливо в районах із критичним рівнем виникнення надзвичайних ситуацій техногенного та природного походження, при контролі за виконанням вимог технологій виробництва і безпеки праці на підприємствах із шкідливими умовами (вентиляція гірничих виробок, гальванічних, лакофарбових цехів та ін.) та як засіб контролю забезпечення під час роботи будівельних і козлових кранів, контролю тяги в димових та вентиляційних каналах житлових будинків, під час експлуатації вітряних енергетичних установок та для створення комфортних умов на робочих місцях тощо.

Калібрування засобів вимірювальної техніки здійснюють з метою встановлення придатності засобів вимірювальної техніки (ЗВТ) до застосування. Калібрування ЗВТ виконують метрологічні служби організацій. Калібрування проводиться метрологічними службами юридичних осіб з використанням еталонів, супідрядних державним еталонам одиниць величин. Результати калібрування ЗВТ засвідчуються каліброваним знаком, сертифікатом, записом в експлуатаційних документах. Розробка програми калібрування анемометру здійснюється згідно нормативного документу ДСТУ OIMLD 20:2008.

Для розробки методики розрахунку невизначеності під час калібрування анемометру та встановлення придатності приладу виконано багаторазові спостереження n=100 швидкості вітру. Виконано обробку результатів багаторазових спостережень. Визначено стандартну невизначеність за типом А, В та сумарну стандартну невизначеність.

Складно бюджет невизначеності вимірювань швидкості вітру на основі рекомендацій [1-3] (таблиця 1).

Таблиця 1 - Бюджет невизначеності вимірювання швидкості вітру під час калібрування анемометру

| Вхідна величина, $a_m$ | Оцінка вхідної величини, $a_m$ | Тип невизначеності | Число ступеней свободи | Коефіцієнт чутливості $ci=dy/dxi$ | Розподілення ймовірностей | Вклад в сумарну невизначеність, $ui(a_m)$ |
|---|---|---|---|---|---|---|
| Випадкова складова $a_m$ | 0,45 | A | n- 1 | 1 | Нормальний закон, $u_A$ | 0,0004 |
| Невизначеність вимірювання еталонної міри швидкісної характеристики при калібруванні,$\Delta_s$ | 0,003 | B | ∞ | 1 | Рівномірний закон, $u(\Delta_{s1})$ | 0,001 |
| Відхилення розміру еталонної міри швидкісної характеристики від номінального значення, $\Delta_n$ | 0,020 | B | ∞ | 1 | Рівномірний закон, $u(\Delta_n)$ | 0,012 |
| Різниця температури навколишнього повітря від нормальної, $\Delta_t$ | 0,6 | B | ∞ | 1 | Рівномірний закон, $u(\Delta_t)$ | 0,346 |
| Ціна поділки або дискретність відліку анемометру, $\Delta^*$ | 0,01 | B | ∞ | 1 | Рівномірний закон, $u(\Delta^*)$ | 0,003 |
| Y | 0,2-1,0 | | - | 2 | P=0,95 | 0,69 |

Список використаних джерел:

1. Zakharov, I. and Botsyura, O., “Estimation of expanded uncertainty in measurement when implementing a Bayesian approach” // Measurement Techniques, 2018, Volume: 61, Issue: 4, pp. 342-346.

2. SO/IEC Guide 98-3:2008 «Uncertainty of measurement – Guide to the expression of uncertainty in measurement (GUM:1995)».

3. ДСТУ-Н РМГ 43-2006. Метрологія. Застосування «Настанови з оцінювання невизначеності у вимірюваннях».

УДК 005.342

# ОЦІНЮВАННЯ ЯКОСТІ ІННОВАЦІЙНОГО ПРОДУКТУ

Русанова Є.В.
Науковий керівник – к.т.н., доц. Запорожець О. В.
Харківський національний університет радіоелектроніки, каф. ІВТ,
м. Харків, Україна,
тел. +38(057) 702-13-31, e-mail: yelyzaveta.rusanova@nure.ua

The problem of evaluating the level of quality of an innovative product is considered. Based on the goal, the nomenclature of quality indicators is selected and the basic values of the indicators are determined, which usually take the values of the indicators of the closest analogue product in terms of functional characteristics. The evaluation of the quality level is carried out by comparing the actual values of the product's quality indicators with the basic ones. Each indicator is assigned a weighting factor, which is taken into account in relation to the generalized indicator of the quality of the innovative product.

У сучасних умовах загострення конкуренції, перетворення її на глобальну основу виживання та успіху, основою сталого становища організації на ринку є своєчасна пропозиція продукції, що відповідає світовому рівню якості. При цьому конкурентоспроможність будь-якої організації, незалежно від розмірів, форми власності та інших особливостей, залежить насамперед від якості продукту та порівнянності його ціни з якістю, що пропонується.

Ці обставини призводять до закономірного зростання ролі системи якості підприємства як універсального інструменту підвищення конкурентоспроможності проектної організації, що дозволяє досягти мети зниження собівартості інноваційного продукту, що виробляється, при абсолютному задоволенні вимог споживача.

Як базове ми будемо використовувати таке визначення: інновація (нововведення) – комплексний процес створення, розповсюдження та використання нового практичного засобу (нововведення) для задоволення людських потреб, що змінюються під впливом закономірного розвитку суспільства, а також пов'язані з цим нововведенням зміни у соціальній та речовій середовищі; впровадження нових ідей, технологій, видів продукції тощо. у галузі праці, виробництва, управління на підприємстві, у галузі.

У системному плані інноваційний проект може бути представлений «чорною скринькою», входом якої є технічні вимоги та умови фінансування, а результатом роботи є досягнення необхідного результату. Виконання робіт забезпечується наявністю необхідних ресурсів: матеріалів, устаткування, людських ресурсів. Ефективність робіт досягається за рахунок управління процесом реалізації проекту, який забезпечує розподіл ресурсів, координацію виконуваної послідовності робіт і компенсацію внутрішніх і зовнішніх впливів.

Забезпечення та оцінка якості інноваційного продукту – одне з першочергових завдань. Оскільки якість визначає ефективність товару і рівень ринкової ціни на нього, то великого значення набуває комплексний підхід до забезпечення якості. Показники якості інноваційного виробу групуються за видами та групами. Основними групами показників є функціональні, ресурсозберігаючі та охоронні.

Загальну схему оцінки рівня якості інноваційного продукту можна описати таким чином. Виходячи з мети вибирається номенклатура показників якості та визначаються базові значення показників, якими зазвичай беруть значення показників найближчого за функціональними характеристиками виробу-аналогу. Оцінка рівня якості здійснюється шляхом порівняння фактичних значень показників якості виробу із базовими. Кожному показнику призначається коефіцієнт вагомості, що враховується щодо комплексного (узагальненого) показника якості інноваційного продукту.

Для оцінки економічної ефективності інноваційного продукту пропонується використати оцінку річного економічного ефекту. Одним із альтернативних способів оцінки ефективності інноваційного продукту є використання методу функціонально-вартісного аналізу. Функціонально-вартісний аналіз є методом комплексного техніко-економічного дослідження об'єкта з метою розвитку його корисних функцій при оптимальному співвідношенні між їх значимістю для споживача і витратами на їх здійснення.

Важливим етапом функціонально-вартісного аналізу є порівняння коефіцієнтів значимості окремих функцій виробу та коефіцієнтів витрат на реалізацію цих функцій. Відношення частки функції за витратами до значущості або важливості функції називається коефіцієнтом витрат за окремими функціями. Виправдане співвідношення цього коефіцієнта має бути рівним чи близьким до одиниці. Якщо коефіцієнт витрат менше одиниці, співвідношення вважають сприятливішим. При коефіцієнті, що перевищує одиницю, рекомендується вживати заходів щодо зниження витрат отримання функції.

Найбільш доцільним є функціонально-вартісний аналіз з продукції, що розробляється, ще не запущеної у виробництво. Тут є час для внесення змін в конструкцію виробу чи технологію виробництва.

Список використаних джерел:

1. Зянько, В. (2008). *Інноваційне підприємництво: сутність, механізми і форми розвитку*. УНІВЕРСУМ – Вінниця.

2. Михайлова, Л., Гуторов, О., Турчіна, С., & Шарко, І. (2015). *Інноваційний менеджмент*. Центр учбової літератури.

3. Микитюк, П. (2019). *Інноваційний менеджмент*. Екон. думка ТНЕУ.

УДК 621.317:53.08

# РОЗРОБКА МЕТОДИКИ ОЦІНКИ НЕВИЗНАЧЕНОСТІ ВИМІРЮВАНЬ ПІД ЧАС КАЛІБРУВАННЯ ТАХОМЕТРУ

Меюс Ю.О.
Науковий керівник – к.т.н., доц. Дегтярьов О.В.
Харківський національний університет радіоелектроніки, каф. ІВТ
м. Харків, Україна
тел. +38(096) 960-87-03, e-mail: yuliia.meius@nure.ua

The purpose of the work is to improve the metrological support of the measurement of the rotation frequency by developing a method of calibrating an electronic tachometer. Research methods – methods of statistical analysis of measurement information, methods of uncertainty theory. The object of the study is the uncertainty of household water meter calibrations. The processing of the results of repeated observations was carried out. The standard uncertainty according to type A, B and the total standard uncertainty are determined. Compile the measurement uncertainty budget.

Тахометр електронний ЭП 5.1 призначений для безконтактного та контактного вимірювання лінійної швидкості, а також частоти обертання вала турбіни з хромонікелевих феромагнітних сталей, частоти обертання вала роторів механізмів та машин в задачах контролю технічного стану обладнання з індикацією в цифрової формі, перетворення частоти обертання в уніфікований сигнал постійного струму та сигналізації при досягненні заданого значення.

Галузь застосування тахометра електронного ЭП 5.1: газова, нафтова, нафтохімічна, харчова промисловості, машинобудування, металургія, енергетика, залізничний транспорт, комунальне господарство.

Калібрування засобів вимірювальної техніки здійснюють з метою встановлення придатності засобів вимірювальної техніки (ЗВТ) до застосування. Калібрування ЗВТ виконують метрологічні служби організацій. Калібрування проводиться метрологічними службами юридичних осіб з використанням еталонів, супідрядних державним еталонам одиниць величин. Результати калібрування ЗВТ засвідчуються каліброваним знаком, сертифікатом, записом в експлуатаційних документах. Розробка програми калібрування тахометра здійснюється згідно нормативного документу ДСТУ OIMLD 20:2008.

Для розробки методики розрахунку невизначеності під час калібрування тахометра та встановлення придатності приладу виконано багаторазові спостереження n=60 кутової швидкості. Виконано обробку результатів багаторазових спостережень. Визначено стандартну невизначеність за типом А, В та сумарну стандартну невизначеність.

Складно бюджет невизначеності вимірювань на основі рекомендацій [1-4] (таблиця 1).

Таблиця 1 - Бюджет невизначеності вимірювання частоти обертання.

| Вхідна величина, $X_i$ | Оцінка вхідної величини $x_i$ | Тип невизначеності | Число ступенів свободи | Коэф. чутл. $c_i=dy/dx_i$ | Розподілення ймовірностей | Сумарна невизначеність, $u_i(y)$ |
|---|---|---|---|---|---|---|
| Випадкова складова | $\omega_1$=851,2 | A | n-1 | 1 | Норм. закон | $u_A$ = 0,663 |
| Невизначеність вимірювання еталонних мір частоти обертання при калібруванні | $\Delta_s$=0,025 | B | ∞ | 1 | Рівномірний закон | $u(\Delta_s)$= 0,025 |
| Відхилення розміру еталонних мір частоти обертання від номінального значення | $\Delta_n$=0,4 | B | ∞ | 1 | Рівномірний закон | $u(\Delta_n)$= 0,289 |
| Різниця температури навколишнього повітря від нормальної | $\Delta_t$=0231 | B | ∞ | 1 | Рівномірний закон | $u(\Delta_t)$= 0,231 |
| Ціна поділки або дискретність відліку тахометра | 0,1 | B | ∞ | 1 | Рівномірний закон | $u(\Delta^*)$= 0,029 |
| ω | 850 | 0,760 | - | 2 | P=0,95 | 1,52 |

Список використаних джерел:

1. Zakharov, I. and Botsyura, O., “Estimation of expanded uncertainty in measurement when implementing a Bayesian approach” // Measurement Techniques, 2018, Volume: 61, Issue: 4, pp. 342-346.

2. SO/IEC Guide 98-3:2008 «Uncertainty of measurement – Guide to the expression of uncertainty in measurement (GUM:1995)».

3. ДСТУ-Н РМГ 43-2006. Метрологія. Застосування «Настанови з оцінювання невизначеності у вимірюваннях».

4. Захаров І.П., Кукуш В.Д. Теорія невизначеності у вимірюваннях. Навчальний посібник. - Харків: Консум, 2002. – 256 с.

УДК 621.317:006.91

# РОЗРОБКА ВИТРАТОМІРА ТА ЙОГО МЕТРОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ

Пономаренко І.О.
Науковий керівник – к.т.н., доц. Дегтярьов О.В.
Харківський національний університет радіоелектроніки, каф. ІВТ
м. Харків, Україна
e-mail: illia.ponomarenko1@nure.ua

The purpose of the work is to improve the metrological support for measuring the flow of substances by creating an acoustic flowmeter with improved metrological and operational characteristics that meet the requirements of the technical task and the basic standards for flowmetry. The structural and principle diagrams of the acoustic flow meter have been developed. The method of metrological certification of the acoustic flow meter has been developed. Algorithms and schemes have been developed to implement the proposed methods of improving metrological characteristics. The metrological characteristics of the developed flow meter were evaluated, taking into account the influence of non-informative parameters of the analyzed environment.

Засоби вимірювання витрати та кількості рідин та газів застосовуються практично у всіх галузях сучасної промисловості. Широкого поширення набули акустичні витратоміри, що дозволяють вимірювати об'ємну витрату та об'єм рідини і насиченої водяної пари, що протікають у напірних трубопроводах, також об'ємну витрату та об'єм рідини, що протікає в безнапірних трубопроводах і колекторах. Вимірювання об'ємної витрати проводиться шляхом множення виміряного значення середньої швидкості рідини, що протікає (пара) на значення площі поперечного перерізу потоку.

В даний час перевагу отримали витратоміри, засновані на ультразвуковому методі вимірювання витрат. Акустичними витратомірами називають прилади, принцип дії яких полягає у вимірюванні будь-якого ефекту (залежно від витрати), що створює при проходженні акустичних коливань крізь потік рідини або газу. Більшість акустичних витратомірів працюють у ультразвуковому діапазоні. Акустичні витратоміри відрізняються за влаштуванням первинних перетворювачів і за використовуваними вимірювальними схемами. Високі частоти акустичних коливань (0,1-10 МГц) застосовуються для вимірювання витрати чистих рідин. Для вимірювання забруднених середовищ частоти коливань значно зменшують до кількох десятків КГц, щоб запобігти поглинанню та розсіюванню акустичних коливань. Довжина хвилі повинна бути в рази більша за діаметр повітряних бульбашок або твердих частинок. Для виміру витрати газів використовують низькі частоти [1-3].

В рамках даної роботи розроблено акустичний витратомір, що має переваги за техніко-метрологічними характеристиками у порівнянні з аналогами. Структурна схема акустичного витратоміра наведена на рис.1

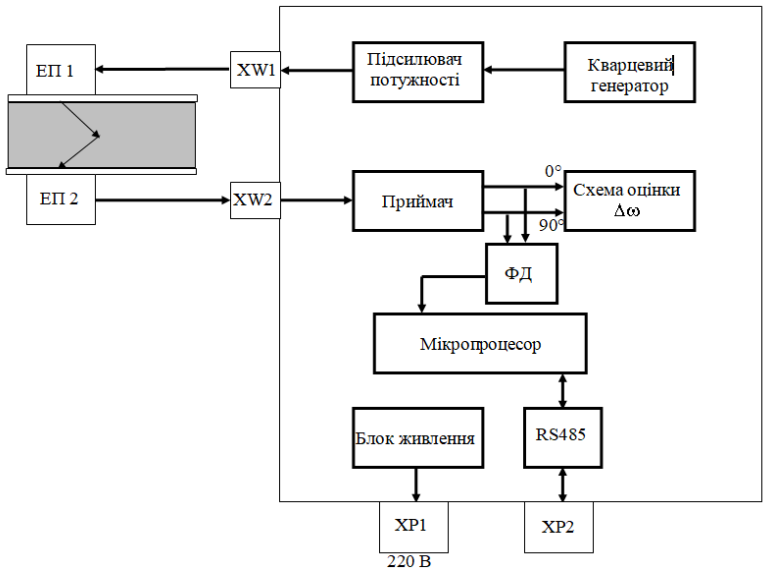



Рисунок 1 - Структурна схема акустичного витратоміра

Прилад (рис.1) містить два електронних перетворювачі (ЕП) ЕП1 та ЕП2, розміщених із зовнішнього боку трубопроводу та електронний блок, утворений кварцовим генератором, підсилювачем потужності, квадратурним приймачем, фазовим детектором (ФД), схемою оцінки центру тяжкості спектра прийнятого сигналу, а також мікропроцесор.

У цій схемі реалізований принцип квадратурної демодуляції прийнятого сигналу, що дозволяє визначати напрямок руху рідини.

Випромінювач ЕП1, збуджений безперервними коливаннями з частою $\omega_0$, що надходять з виходу підсилювача потужності створює ультразвукову хвилю, що випромінюється в контрольоване середовище під кутом до осі трубопроводу. На вхід приймального перетворювача ЕП2 надходить сигнал, відбитий від неоднорідностей потоку. Прийняті коливання подаються до приймача, на виході якого виділяється квадратурний сигнал доплерівської частоти, що надходить з одного боку на ФД, а з іншого - на вхід схеми оцінки центру тяжкості спектра. Чисельне значення ω надходить у мікропроцесор, де здійснюється розрахунок значення витрати Q. Для передачі даних служить вихід RS, або GSM модем, для передачі даних про стан приладу як по sms повідомленню, так і через інтернет.

Список використаних джерел:

1. Бірюков Б.В., Данилов М.А., Кривіліс С.С. Випробування витратомірів. Вид-во стандартів. - 240 с.

2. Гриньова, Л. Д. та ін. Матеріали та датчики для ультразвукових витратних засобів [Текст] // Вимірювальна техніка, № 7, с.12-19.

3. Малов, В. В. П'єзорезонансні датчики [Текст] / В. В. Малов - 2-ге вид., Перераб. та дод. : Вища школа, 271 с.

УДК 658.562:006.015.5

# ДОСЛІДЖЕННЯ ТА РОЗРОБКА ОЦІНКИ ЯКОСТІ ПОСЛУГ

Кулічко-Павленко І.С.
Науковий керівник – к.т.н., доц. Дегтярьов О.В.
Харківський національний університет радіоелектроніки, каф. ІВТ
м. Харків, Україна
тел. +38(066) 587-73-71, e-mail: ivan.kulichko.pavlenko@nure.ua

The purpose of the work is to improve of the fitness center service level by developing elements of the company's quality system. The object of the study is the elements of the quality management system of an enterprise serving the population - a fitness center. A system of objects is proposed for quality management at the enterprise. Methods for assessing the quality of fitness center services have been developed. The characteristic of research solutions is given. The object of the study is the elements of the quality management system of an enterprise serving the population - a fitness center.

Відповідно до визначення стандартів ISO *послуга* – це результат взаємодії постачальника та замовника та внутрішньої діяльності постачальника щодо задоволення потреб замовника. Вимоги до послуги повинні бути чітко виражені характеристиками, що піддаються визначення та оцінки замовником. *Петля якості послуги* – концептуальна модель взаємозалежних видів діяльності, які впливають якість різних стадіях (від визначення потреб до оцінки задоволення). В організації необхідно створити методики *системи якості*, щоб конкретизувати експлуатаційні вимоги для процесів, що стосуються послуг, включаючи маркетинг, проектування та надання послуги, які функціонують у петлі якості послуги.

Аналіз якісних показників послуг передбачає створення системи їх оцінки. Для цього запропоновано для оцінки якості послуг, що надає організація (фітнес-центра) сумісно використовувати дві розроблені методики:

1. методика "Expectation minus Perception"
2. методика, що базується на розрахунку індекса задоволення споживачів.

Для оцінки якості послуг підприємства запропоновано метод на основі концепції очікування мінус сприйняття. Сприйняття у методиці сприймається як виміряне споживче ставлення до реально створеної і сприймається послуги. Базовий алгоритм виявляє якості послуги може бути відображений наступним рівнянням:

$$SQ_i = \sum_{i=1}^{k} W_j (P_{ij} - E_{ij}),$$

де $SQ_i$ - якість стимулу $i$, що сприймається;

$k$ - кількість проаналізованих атрибутів;

$W_j$ - ваговий фактор атрибуту;

$P_{ij}$ - створене сприйняття стимулу *i* по відношенню до атрибуту $j$;

$E_{ij}$ - очікуваний рівень для атрибуту $j$, що є нормативом стимулу $i$.

На початковому етапі ми визначали, які з цих критеріїв найбільш важливі для респондентів щодо абстрактної компанії, що працює на досліджуваному ринку. Для цього кожен із опитаних мав оцінити зазначені критерії за п'ятибальною шкалою: «5» - дуже важливо, «4» - скоріше важливий, ніж ні, «3» - ні "так", ні "ні", «2» - швидше не важливо, «1» - не важливо. Даний етап необхідний для того, щоб скласти узагальнений портрет досліджуваного об'єкта ринку (компанії), що пропонує ту чи іншу послугу. На підставі такого портрета можна скласти уявлення про ідеального учасника ринку.

Для оцінки якості послуг організації запропоновано анкету, яка базується на методиці «Очікування мінус сприйняття». Розроблена анкета для вимірювання якості послуг складається із трьох блоків: «1-й блок тверджень» для визначення очікувань споживачів щодо якості послуг; «2-й блок тверджень» для визначення ступеня важливості критеріїв якості послуг для споживачів; «3-й блок тверджень» для визначення сприйняття споживачами якості послуг, наданих компанією.

На другому етапі респондентів просять висловити свою оцінку, за тими ж критеріями, якістю роботи досліджуваної компанії та трьох найближчих конкурентів. Потім результати оцінок порівнюються зі значеннями очікувань, і різниця показує, наскільки хороший результат (алгоритм "Expectation minus Perception").

За підсумками двох етапів можна провести порівняння ідеальної (за результатами Етапу 1) та реальної компанії за результатами Етапу 2. У результаті порівняння ми дізнаємося, наскільки успішна робота компанії з надання послуг:

- якщо очікувані (ідеальні) оцінки перевищують реальні, то якість на високому рівні.
- якщо очікувані оцінки нижче реальних, то компанії необхідно приймати заходи щодо підвищення показників за тими чи іншими критеріями.
- якщо очікувані оцінки збігаються з реальними, то компанія досить успішна, але їй є до чого прагнути.

Список використаних джерел:

1. ДСТУ 2375 Побутове обслуговування населення. Терміни та визначення [Текст] – Введ. 01.01.08. – Київ: Держспоживстандарт України, 2008. – 53 с.

2. ДСТУ 3279-95 Стандартизація послуг. Основні положення [Текст] – Введ. 01.01.08. – Київ: Держспоживстандарт України, 2008. – 29 с.

3. Буличова З.Ю., Караваєва О.А., Севастьянов В.С, Руденко Б.А. Оцінка якості послуг // Методи оцінки відповідності. - 2007. - № 9, с.26-31.

## АЛФАВІТНИЙ ПЕРЕЛІК

**ЗМІСТ**

**ДЛЯ НОТАТОК**

«РАДІОЕЛЕТРОНІКА І МОЛОДЬ У XXI СТОЛІТТІ»

МАТЕРІАЛИ 27-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

Відповідальний за випуск: А.В. Снігуров
Комп'ютерна верстка Г.Є. Ляшенко

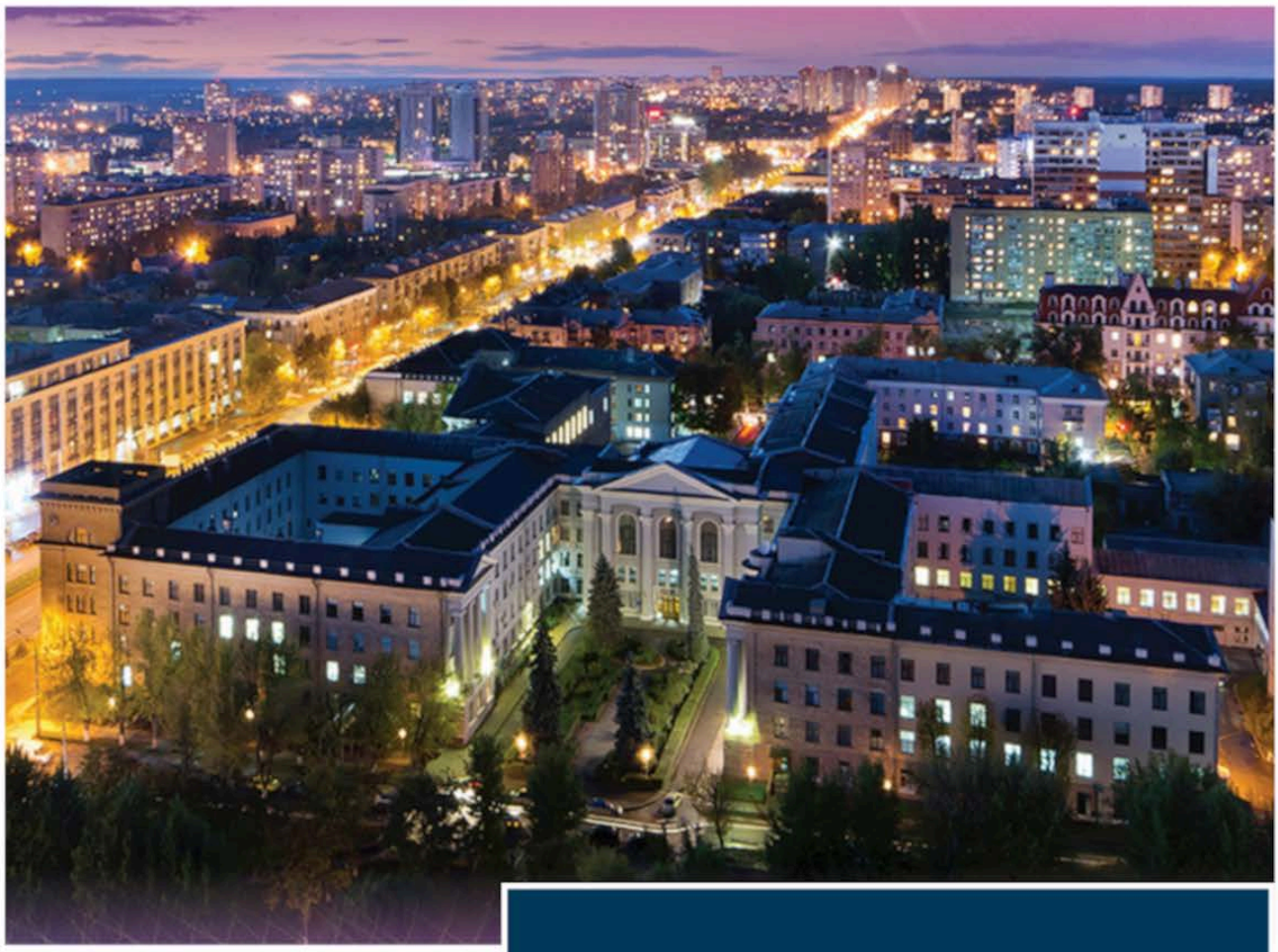
Матеріали збірника публікуються в авторському варіанті без редагування

Підп. до друку 09.04.2023 Формат 60x84 1/16 Спосіб друку - ризографія Тираж 99 прим.
Умов. друк. арк. 10,23
Зам. № __-____. Ціна договірна

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

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

NURE
Харківський національний
університет радіоелектроніки



# XXVII Міжнародний молодіжний форум

# "Радіоелектроніка та молодь у XXI столітті"