МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Матеріали XXVIII Міжнародного молодіжного форуму

«Радіоелектроніка та молодь у XXI столітті»

ТОМ 5 «Проблеми комп'ютерної інженерії та захисту інформації»

Харків 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

МАТЕРІАЛИ 28-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

«РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ У XXI СТОЛІТТІ»

16 – 18 квітня 2024 р.

Том 5

КОНФЕРЕНЦІЯ

«ПРОБЛЕМИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ЗАХИСТУ ІНФОРМАЦІЇ»

Харків 2024

УДК 004.032.2+004.7.032.2

28-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. матеріалів форуму. Т. 5. – Харків: ХНУРЕ. 2024. – 173 с.

У збірнику представлені матеріали доповідей учасників 28-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті».

Для науковців, викладачів, практичних працівників, студентів, а також широкого кола читачів, які цікавляться цією проблематикою.

Відповідальність за зміст поданого матеріалу несе його автор.

Видання підготовлено факультетом комп'ютерної інженерії та управління Харківського національного університету радіоелектроніки

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

E-mail: mref21@nure.ua

ISBN 978-966-659-395-8
DOI 10.30837/IYF.PCEIP.2024

Програмний комітет конференції

Волк М.О.	доктор технічних наук, професор, професор кафедри електронних обчислювальних машин (ЕОМ)
Коваленко А.А.	доктор технічних наук, професор, завідувач кафедри електронних обчислювальних машин (ЕОМ)
Литвинова Є.І.	доктор технічних наук, професор, професор кафедри автоматизації проектування обчислювальної техніки (АПОТ)
Ляшенко О.С.	кандидат технічних наук, доцент, декан факультету Комп'ютерної інженерії та управляння (КІУ)
Руденко О.Г.	доктор технічних наук, професор, завідувач кафедри комп'ютерних інтелектуальних технологій та систем (КІТС)
Сєвєрінов О.В.	кандидат технічних наук, доцент, професор кафедри безпеки інформаційних технологій (БІТ)
Халімов Г.З.	доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій (БІТ)
Чумаченко С.В.	доктор технічних наук, професор, завідувач кафедри автоматизації проектування обчислювальної техніки (АПОТ)

УДК 004.3+004.4:519.713:007.52

КОМП’ЮТЕРНА ІНЖЕНЕРІЯ: СУЧАСНІ ТЕХНОЛОГІЇ РОЗРОБКИ ТА ПРОГРАМУВАННЯ КОМП’ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

УДК 004.8:519.816

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МОНІТОРИНГУ ТА АНАЛІЗУ ЕФЕКТИВНОСТІ АКЦІЙНИХ ПРОПОЗИЦІЙ

Боровик П.К.
Науковий керівник – к.т.н., доц. Сердюк Н.М.
Харківський національний університет радіоелектроніки, каф. КІТС,
м. Харків, Україна
e-mail: polina.borovyk@nure.ua

This work explores the role of AI in improving the effectiveness of promotional offers in both retail and online marketing in the face of growing competition and consumer expectations. Traditional methods of analysis lack accuracy and efficiency, while AI's ability to process large amounts of data allows us to predict the results of promotional campaigns. Today, AI tools play an important role in planning marketing strategies, helping to adapt to consumer preferences and changes in strategy. AI analytical capabilities allow companies to increase the effectiveness of promotional campaigns, introduce product innovations, and attract customers.

У сучасному світі роздрібної торгівлі та онлайн-маркетингу акційні пропозиції є важливим інструментом для збільшення продажів, залучення клієнтів та підвищення їхньої лояльності до бренду. Однак ефективність цих акцій часто залежить від здатності точно відстежувати, аналізувати та ітеративно змінювати стратегії на основі поведінки та реакції споживачів. Традиційні методи оцінки ефективності акційних кампаній, такі як опитування, відстеження продажів та відгуки клієнтів часто не дають можливості аналізу та прогнозування в режимі реального часу. Саме тут інтеграція штучного інтелекту представляє собою трансформаційне рішення, пропонуючи потенціал не лише для моніторингу та аналізу ефективності акційних пропозицій у режимі реального часу, але й для прогнозування майбутніх тенденцій та реакції споживачів [1].

Суть використання штучного інтелекту в цьому контексті полягає в його здатності обробляти величезні масиви даних, виявляючи закономірності, тенденції та аномалії, які може не помітити людина, проводячи аналіз. Методи збору даних для цих цілей розвивалися від прямих спостережень та опитувань до більш складного аналізу цифрових потоків, таких як дослідження настроїв у соціальних мережах, відвідуваності веб-сайтів та історії покупок. Порівняльна перевага нейронних мереж над класичними методами є значною. Нейронні мережі, з їхньою здатністю навчатися та адаптуватися до нових даних, можуть забезпечити розуміння поведінки споживачів з надзвичайною глибиною та точністю [1]. Наприклад, якщо класичні методи можуть покладатися на лінійні регресійні моделі для прогнозування зростання продажів після акційної пропозиції, то нейронні мережі можуть враховувати ширший

спектр змінних, включаючи сезонність, демографічні дані споживачів і навіть зовнішні фактори, такі як економічні показники, щоб забезпечити більш детальний аналіз.

Розробка інструментів на основі штучного інтелекту для оцінки ефективності акційних пропозицій – це багатогранний процес, який включає збір даних, навчання моделі та розгортання системи для аналізу та зворотного зв'язку в режимі реального часу. Ці інструменти можуть мати різні форми: від інформаційних панелей, що надають оперативні дані про ефективність кампанії, до прогностичних моделей, які передбачають потенційний вплив майбутніх акцій. Інтеграція штучного інтелекту в цей процес не тільки підвищує точність оцінювання ефективності, але й значно скорочує час, необхідний для збору корисної інформації [2].

Використання штучного інтелекту для аналізу та моніторингу ефективності акційних пропозицій також відкриває шлях до більш гнучкого та динамічного підходу до промо-стратегії. Постійно використовуючи результати аналізу, отримані за допомогою штучного інтелекту, у процесі планування, компанії можуть створити безперервний цикл вдосконалення. Така адаптивна стратегія гарантує, що акційні пропозиції не лише відповідають поточним моделям поведінки споживачів, але й є достатньо адаптивними, щоб підлаштовуватися під нові тенденції та вподобання [3].

Підсумовуючи, можна сказати, що інтеграція штучного інтелекту в моніторинг та аналіз ефективності акційних пропозицій є значним кроком вперед у сфері маркетингу та аналізу споживчої поведінки. Використовуючи можливості технологій штучного інтелекту, компанії можуть отримати більш глибоке розуміння, прогнозувати майбутні тенденції та адаптувати свої стратегії до мінливих потреб і вподобань своїх клієнтів. Такий підхід не лише підвищує ефективність акційних кампаній, а й стимулює інновації в продуктових пропозиціях і маркетингових стратегіях [4].

Список використаних джерел

1. Prabin S. M., Thanabal M. S. A repairing artificial neural network model-based stock price prediction. International journal of computational intelligence systems. 2021. Т. 14, № 1. С. 1337. URL: https://doi.org/10.2991/ijcis.d.210409.002 (дата звернення: 24.02.2024).

2. Ramnani S. Revolutionising conventional marketing with AI: leveraging machine learning for marketing. Interantional journal of scientific research in engineering and management. 2024. Т. 08, № 01. С. 1–13. URL: https://doi.org/10.55041/ijsrem28481 (дата звернення: 24.02.2024).

3. The impact of artificial intelligence on consumer behaviour and changes in business activity due to pandemic effects / T. Dias та ін. Human technology. 2023. Т. 19, № 1. С. 121–148. URL: https://doi.org/10.14254/1795-6889.2023.19-1.8 (дата звернення: 25.02.2024).

4. Ziakis C., Vlachopoulou M. Artificial intelligence in digital marketing: insights from a comprehensive review. Information. 2023. Т. 14, № 12. С. 664. URL: https://doi.org/10.3390/info14120664 (дата звернення: 25.02.2024).

УДК 004.9:57.087 **DOI: https://doi.org/10.30837/IYF.PCEIP.2024.007**

МОДЕЛЮВАННЯ ІНТЕР'ЄРА РОЗУМНОГО БУДИНКУ З ВИКОРИСТАННЯМ ІНСТРУМЕНТАЛЬНИХ ЗАСОБІВ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

Воронін Р.А.
Науковий керівник – доц. Ларченко Л.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. АПОТ, тел. (057) 702-13-26)
e-mail: roman.voronin@nure.ua, (097)823-84-84

This study explores the use of augmented reality (AR) tools in designing smart home interiors, emphasizing enhanced visualization and interaction. By integrating AR, designers and homeowners can more effectively conceptualize and modify living spaces in real-time. This approach not only streamlines the design process but also allows for a personalized experience by accommodating user preferences in furniture arrangement and décor choices. Furthermore, AR's capacity for immersive visualization aids in better decision-making, ensuring that the final design aligns closely with the occupants' desires and lifestyle needs.

Розвиток концепції розумних будинків, інтегрованих з передовими технологіями, ставить перед дизайнерами та архітекторами завдання реалізації інноваційних підходів у моделюванні інтер'єрів. Зокрема, використання інструментальних засобів доповненої реальності (ДР) набуває вирішального значення у контексті оптимізації просторового розподілу та персоналізації домашнього середовища [1].

ДР-технологія відкриває новітні можливості для візуалізації і моделювання майбутнього простору, дозволяючи ефективно інтегрувати елементи інтер'єру в реальному часі [2]. Такий підхід сприяє глибшому розумінню взаємозв'язків між функціональністю, естетикою та комфортом, що є ключовим для створення індивідуалізованого та гармонійного житлового простору.

Метою дослідження є аналіз методів моделювання інтер'єра розумного будинку з використанням доповненої реальності, спрямованих на підвищення інтерактивності та персоналізації дизайну, що включає в себе створення алгоритмів для візуалізації та адаптації дизайнерських рішень у віртуальному просторі, а також аналіз впливу використання ДР на зручність користування і загальну задоволеність від використання житлових просторів.

У роботі розглядається технологія в області моделювання інтер'єра розумного будинку з використанням інструментальних засобів доповненої реальності, що охоплює аналіз потенціалу ДР-технологій у створенні гнучких і персоналізованих рішень для дизайну інтер'єру.

Розумні будинки становлять передовий напрямок у розвитку житлової інфраструктури, орієнтований на підвищення комфорту, безпеки, та енергоефективності. Ці системи інтегруються з широким спектром

інтелектуальних пристроїв та сенсорів, що дозволяє автоматизувати багато аспектів повсякденного життя. Від регулювання температури та освітлення до керування безпековими системами та побутовою технікою, розумні будинки забезпечують зручність та адаптованість до потреб мешканців.

Створення інтерактивних моделей дозволяють візуалізувати та модифікувати просторові рішення в реальному часі. Здійснюється аналіз методів інтеграції ДР з іншими інтелектуальними системами розумного будинку для створення гармонійного та функціонального простору, а також оцінюється вплив даних технологій на ефективність використання простору.

Система розумного будинку, об'єднана з технологіями доповненої реальності, розширює можливості інтерактивної взаємодії користувача з домашнім середовищем, перетворюючи завдання моделювання на інноваційний досвід. Дана система дозволяє не лише візуалізувати потенційні зміни в інтер'єрі, але й миттєво аналізувати різні сценарії освітлення, розміщення меблів та вибору кольорів стін.

Завдяки інтеграції системи моделювання інтер’єра з інтелектуальними датчиками та елементами керування, система може адаптуватись до змін у середовищі та потребах користувача, надаючи рекомендації для підвищення енергоефективності та комфорту.

Використання ДР у проектуванні розумного будинку відіграє ключову роль у створенні багатофункціонального та естетично привабливого житлового простору, що відповідає сучасним вимогам до індивідуального та екологічно чистого житла.

Розглянуто систему моделювання інтер'єра розумного будинку з використанням інструментальних засобів доповненої реальності, досліджено можливості візуалізації та інтерактивної модифікації дизайну в реальному часі. Проаналізована взаємодія між системами управління розумного будинку та ДР-технологіями, виявлено ключові переваги застосування ДР у створенні функціонального та естетично привабливого житлового простору.

Список використаних джерел:

1. Nasir S., Zahid M., Khan T., Kadir K., Khan S. Augmented Reality Application for Architects and interior designers: Interno A cost effective solution [Текст] / S. Nasir, M. Zahid, T. Khan, K. Kadir, S. Khan // 2018 IEEE 5th International Conference on Smart Instrumentation, Measurement and Application (ICSIMA). – 2018. – С. 1–6.

2. Dong S, Kamat V. SMART: scalable and modular augmented reality template for rapid development of engineering visualization applications / S. Dong, V. Kamat // Visualization in Engineering. – 2013. – № 1. – С. 1–17.

3. Dünser A., Walker L., Horner H., Bentall D. Creating interactive physics education books with augmented reality [Текст] / A. Dünser, L. Walker, H. Horner, D. Bentall // Proceedings of the 24th Australian Computer-Human Interaction Conference. – 2012. – С. 107–114.

4. Kiran A., Chowdary M. K. (2022). Home Automation using Augmented Reality [Текст] // 2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC). – С. 1-6.

УДК 004.7

МЕХАНІЗМИ ПРІОРИТЕЗАЦІЇ ПОТОКІВ МУЛЬТИМЕДІЙНИХ ДАНИХ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Герасимчук Д.В.
Науковий керівник – ас. Чепурна І.С.
Харківський національний університет радіоелектроніки, каф. ЕОМ,
м.Харків, Україна
e-mail: dmytro.herasymchuk@nure.ua

This paper provides an overview of the mechanisms and ways to implement the transmission of multimedia content in global computer networks. The use of combined solutions based on the use of routing, resource reservation, marking and classification of data packets in the QoS architecture helps improve methods for prioritizing inelastic data flows in computer networks.

Передача мультимедійного контенту є однією з найбільш поширених різновидів трафіку у глобальних комп'ютерних мережах. Наприклад, високороздільний відеоконтент реального часу потребує ефективного управління ресурсами мережі, забезпечення мінімальної затримки передачі таких даних, резильєнтності вузлів передачі даних. Це можливо досягти завдяки вдосконаленню методів пріоритезації потоків нееластичних даних у комп'ютерних мережах.

Існує ряд рішень, які дозволяють забезпечити зазначені вище вимоги до передачі трафіку в мережах, однак більшість із них мають вузьку спеціалізацію та ефективно працюють лише у комбінаторних схемах [3]. Кожна з таких схем може вимагати індивідуальних налаштувань взаємодії окремо взятих підходів

Метою даної роботи є огляд механізмів та шляхів їх реалізації щодо використання маршрутизації, резервування ресурсів, маркування і класифікацію пакетів даних в архітектурі QoS.

У якості першого прикладу варто розглянути QoS, який є класичним методом побудови систем забезпечення якості передачі даних. Іншими словами – цей метод забезпечує функціональність мережі щодо пріоритезації мультимедійного трафіку над іншими видами трафіків в залежності від встановлених правил його проходження через пристрої комутації та маршрутизації.

Іншим підходом є використання проміжних серверів для зберігання даних, що сприяє мінімізації затримок при передачі еластичних обсягів даних в комп'ютерних мережах, надаючи перевагу нееластичним даним. Проміжне зберігання зменшує кількість повторних запитів, а відповідно, і службового трафіку, який має місце при розрахунку бюджету пропускної здатності мережі. В даному випадку забезпечується вирішення подвійної задачі: гарантована доставка великих даних та даних реального часу.

В разі побудови гетерогенної корпоративної комп’ютерної мережі [1] має місце рішення, коли значення обсягу пропускної спроможності трафіку визначається на основі принципу кінцевої черги. Це рішення показує, яким чином відбувається асинхронне заповнення проміжних носіїв даних із заданими швидкостями в каналах зазначеної ємності. З іншої сторони це можна використати як підставу до побудови політики агрегації каналів визначеного розміру для видачі трафіку кінцевому користувачеві в залежності від його типу, обсягу та встановленого пріоритету.

У разі застосування механізмів визначеної пріоритезації трафіку у віртуалізованих середовищах [2], як правило, використовується спеціальні застосунки на базі віртуалізаторів мережних рішень, які можуть встановлювати більш високий рівень пріоритету трафіку користувачів з більш низькими часовими затримками на точці входу до даного середовища. Наприклад, при побудові систем доставки контенту з використанням WAN-оптимізаторів, користувачі, які будуть мати мінімальні значення входу на інтерфейси даної розподіленої системи, будуть отримувати мультимедійний контент першочергово, навіть, якщо вони будуть мати більш низький рівень обслуговування. З однієї сторони, це вирішить питання завантаженості каналів доставки контенту, з іншої сторони – дозволить вивільнити цей ресурс для користувачів, які мають значні часові затримки У деяких випадках постачальники хмарних рішень, які спеціалізуються на доставці зазначеного виду контенту можуть застосовувати спеціальні алгоритми кешування та буферизації даних за рахунок технології обчислень «на межі».

Список використаних джерел

1. V. Tkachov, M. Hunko and V. Volotka, "Scenarios for Implementation of Nested Virtualization Technology in Task of Improving Cloud Firewall Fault Tolerance," 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 2019, pp. 759-763, doi: 10.1109/PICST47496.2019.9061473.

2. Kuchuk, N. et al. Predicting traffic anomalies in container virtualization / Kuchuk, N., Kovalenko, A., Tkachov, V., Rosinskiy, D., Kuchuk, H. // Fifth International Scientific and Technical Conference "COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES". -2021. -С. 25-26

3. T. Vitalii, B. Anna, H. Kateryna and D. Hrebeniuk, "Method of Building Dynamic Multi-Hop VPN Chains for Ensuring Security of Terminal Access Systems," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2020, pp. 613-618, doi: 10.1109/PICST51311.2020.9467953.

УДК 004.27 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.011

ОСОБЛИВОСТІ ОБЧИСЛЕННЯ У ТУМАНИХ ОБЧИСЛЕНЬ У СУЧАСНИХ IOT СИСТЕМАХ

Гунько М.А., Фролов Д.Є.
Науковий керівник – к.т.н., доц. Ткачов В.М.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. ЕОМ, тел. (057) 702-13-54)
e-mail: d_ec@nure.ua

In this article will be explored the evolution of computational models. Despite the success of cloud computing, challenges such as high latency and lack of location information persist, leading to a push for a new decentralized approach. This next paradigm, termed fog computing, extends the cloud model by bringing computing and storage capabilities closer to data-generating IoT devices at the edge of the network. While fog computing holds promise for various industries, including healthcare and augmented reality, it also poses challenges such as resource provisioning, security, energy minimization, and standardization, necessitating further research and development efforts.

В останні кілька десятиліть обчислювальні моделі змінювали централізований і децентралізований підходи до обчислень. Починаючи з мейнфреймів у 70-х і 80-х роках, за еволюцією моделі послідувала хвиля децентралізації клієнт-серверної моделі в 90-х роках. Ця перша хвиля була спровокована падінням цін на персональні комп'ютери та зростанням інтересу до володіння власною обчислювальною потужністю. На початку 2000-х років обчислювальна модель знову перейшла від децентралізованого до централізованого підходу, а саме до парадигми хмарних обчислень. Незважаючи на те, що хмарні обчислення процвітають і не будуть замінені в найближчому майбутньому, існує сила, яка просуває новий децентралізований підхід до вирішення постійних проблем централізованих систем, наприклад, висока затримка, відсутність інформації про місцезнаходження. Різниця порівняно з попередньою парадигмою полягає в тому, що ця наступна парадигма не замінить попередню, а розширить її, щоб покращити певні можливості (рис. 1). Цей поточний перехід від парадигми централізованих хмарних обчислень до парадигми децентралізованих обчислень ознаменував народження туманних обчислень.

Ця нова парадигма розподілених обчислень містить ідею надання обчислювальних можливостей і можливостей зберігання ближче до пристроїв IoT, що створюють дані, на межі мережі. З метою зменшення відстані між кінцевими пристроями та найближчим блоком обробки ця парадигма вводить додатковий рівень багатих ресурсами пристроїв IoT,

тобто туманних осередків. Ці туманні комірки мають власні обчислювальні можливості та можливості зберігання для обробки запитів завдань, фільтрації та попередньої обробки даних. Це створює відстань в один стрибок до кінцевих пристроїв і, отже, зменшує затримку та час виконання завдання. Іншим важливим розширенням обчислень у тумані є широке географічне поширення цих додаткових пристроїв, спрямованих на безперебійне та надійне виконання послуг навіть при підключенні до рухомих пристроїв, наприклад, інтелектуальних автомобілів, мобільних телефонів.

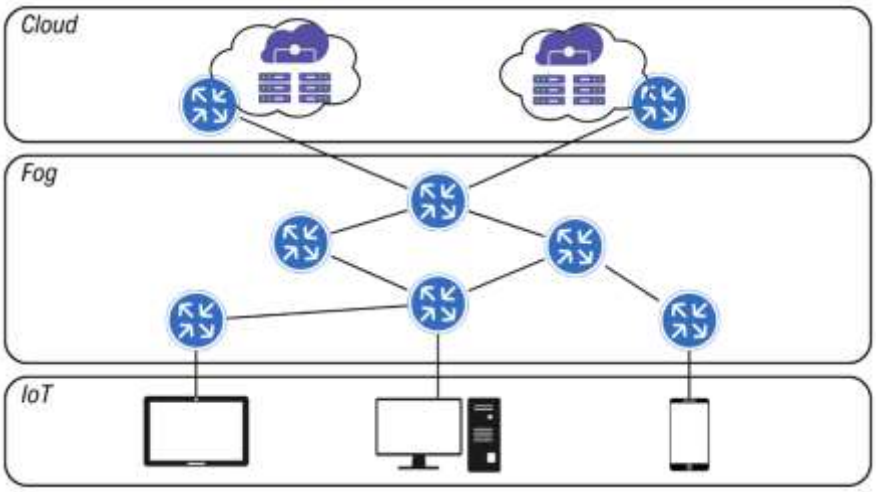


Рис. 1 – Ландшафт туманих вичеслень

Fog computing часто згадується як технологія забезпечення для різних застосувань у різноманітних галузях, наприклад, охорона здоров’я, доповнена реальність, кешування та попередня обробка. Будучи в змозі забезпечити багатообіцяючі вдосконалення, які виникають завдяки цій парадигмі, ще потрібно вирішити багато проблем. Вирішальні проблеми в дослідженнях включають забезпечення ресурсами, розміщення послуг, безпеку та надійність, мінімізацію енергії, стандартизацію та моделі програмування.

Список використаних джерел

1. Tkachov, V., Bondarenko, M., Ulyanov, O., & Reznichenko, O. (2019, December). Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory. In 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT) (pp. 161-165).

2. Tkachov, V., Hunko, M., Volotka, V.: Scenarios for Implementation of Nested Virtualization Technology in Task of Improving Cloud Firewall Fault Tolerance. In 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), pp. 759-763. IEEE (2019).

УДК 004.85 **DOI: https://doi.org/10.30837/IYF.PCEIP.2024.013**

ПАРАЛЕЛЬНІ ІМУННІ СИСТЕМИ ДЛЯ РОЗПІЗНАВАННЯ ОБРАЗІВ

Дараган Д. М.
Науковий керівник – доц. Сердюк Н.М.
Харківський національний університет радіоелектроніки, каф. КІТС,
м. Харків, Україна
e-mail: dmytro.darahan@nure.ua

The subject of the proposed paper is the use of parallel distributed computing on GPUs to solve the problem of pattern recognition by means of artificial immune systems. The purpose of this work is to review the prospects for the use of modern hardware for the study of areas of artificial intelligence, inhibited by the level of technical development. The relevance of the work lies in the constant growth of data volumes and the need for their processing using advanced methods. The theoretical foundations of the subject were considered, assumptions were made regarding the effectiveness of an approach, and prospects for future research were outlined.

Розпізнавання образів - це процес автоматичного визначення та інтерпретації об'єктів, патернів чи характеристик на цифрових зображеннях або відео. Ця задача може здійснюватись за допомогою класичних алгоритмів комп’ютерного зору. Серед алгоритмів машинного навчання особливо цікавим є застосування теорії штучних імунних систем для розпізнавання образів.

На поточному етапі розвитку апаратного забезпечення дослідникам і практикам штучного інтелекту доступні загальні обчислення на графічних відеокартах, що дозволяє повернутись до теоретичних досліджень 1970-1980 рр і знайти практичне застосування алгоритмам та моделям, потенціал яких було складно розкрити в ті часи.

Актуальним є питання застосування паралельних обчисленнь на GPU для задачі розпізнавання образів засобами штучних нейронних мереж.

Нашою метою є огляд можливості практичної реалізації описаного підходу та перспектив його подальшого розвитку.

Штучні імунні системи — це адаптивні системи, натхненні теоретичною імунологією, які застосовуються для вирішення проблем штучного інтелекту.[1] Критичним фактором, що стримував дослідження і практичне застосування ШІС виступав недостатній розвиток апаратного забезпечення, яке не могло надати потрібної обчислювальної потужності для виконання значної кількості адаптивних обчисленнь в часи зародження теорії штучних імунних систем.

У зв’язку з постійним зростанням обсягів данних, особливо цікавим є поєднання переваг штучних імунних систем з перевагами моделей паралельної розподіленої обробки (англ. - parallel distributed processing, PDP), дослідження яких також було загальмовано рівнем розвитку апаратного забезпечення. Паралельна розподілена обробка (PDP) — це тип обчислень, у якому кілька процесорів працюють разом, щоб виконати завдання. Кожен процесор має власну локальну пам'ять і виконує частину

завдання. Системи PDP часто використовуються для завдань, які можна розділити на менші частини[2].

Мережа PDP, характеризується чотирма ключовими аспектами: шаблоном зв’язку між блоками, ваговою матрицею зв’язності, що визначає відносну силу та знаки зв’язків, правилом активації та правилом навчання[2].

Як і нервова система, імунна система повинна вивчати нові данні, згадувати раніше вивчену інформацію та приймати рішення на основі попереднього досвіду. Імунна PDP описує мережу процесорів-лімфоцитів, що працюють паралельно.

Модель імунної мережі PDP можна підсумувати таким чином[3]:

1. Імунна мережа демонструє архітектуру PDP з окремими лімфоцитами, які виконують функції процесингових одиниць.
2. Сила зв'язку ідіотип-антиідіотип еквівалентна спорідненості антиідіотипу з ідіотипом.
3. Одиниці лімфоцитів демонструють сигмоподібне правило активації.
4. Мережа використовує правило навчання Гебба.
5. Складні шаблони антигенів можна вивчати та зберігати на рівні мережі.

Для практичної реалізації розглянутих концепцій є можливим застосовувати загальні обчислення на графічних відеокартах. Очевидним є застосування технології CUDA для цієї задачі. CUDA - програмно-апаратна архітектура паралельних обчислень, яка дозволяє суттєво збільшити обчислювальну продуктивність завдяки використанню графічних процесорів. Програмно-апаратна архітектура CUDA значною мірою відповідає еталонній моделі PDP, тому припускаємо, що імунна система отримає найвищу продуктивність за такої реалізації. Спростити та оптимізувати імплементацію паралельних імунних систем для розпізнавання образів дозволяє cuBLAS. бібліотека що підтримує змішане та низькоточне виконання з додатковим налаштуванням для найкращої продуктивності.

Як висновок, нами було розглянуто можливість паралельної розподіленої реалізації штучних імунних мереж на GPU для вирішення задачі розпізнавання образів та зроблено припущення щодо ефективності таких систем. Експериментальна перевірка наведених тверджень спонукає до подальших досліджень в галузі як штучних імунних систем, так і моделей паралельної розподіленої обробки та дає перспективи заново поглянути на наукові напрямки, загальмовані недостатнім рівнем апаратного забезпечення.

Список використаних джерел

1. D. Dasgupta (1999), Artificial Immune Systems and Their Applications, Germany: Springer,

2.Vertosick, F. T., & Kelly, R. H. (1989). Immune network theory: a role for parallel distributed processing?. *Immunology*, *66*(1), 1–7.

3. Rumelhart, D. & Hinton, G. & Williams, R.. (1986). PDP: Computational models of cognition and perception. I, MIT Press.

УДК 004.7

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В БАНКІВСЬКІЙ СФЕРІ

Єрьомін Д.А.
Науковий керівник – Радченко О.П.
Харківський радіотехнічний фаховий коледж,
м. Харків, Україна
e-mail: dimerbol@gmail.com

This article is aimed at the use of information technology in the banking sector. It describes modern technologies used in the field of finance. The advantages of modern solutions and developed technologies are determined. Conclusions about the work of information systems are made. The prospect of development in this direction is determined.

У наш час використання інформаційних технологій стало повсякденністю, розвиток яких не зупиняється. Технології впроваджуються у всі сфери нашого життя, особливо це помітно у сфері фінансів. Так, наприклад, за останні роки більшість з нас перейшла зі сплати готівкою до безготівкової оплати, до цього відносяться, як шопінг, так і сплата житлово комунальних послуг.

Використання інформаційних технологій значно спрощує наше життя, завдяки зручності у використанні та спроможності сплатити за будь-який товар чи послугу через мережу Інтернет.

Так банківські інформаційні технології розділяють на:

- документообіг та управління ризиками;
- банківські карти та платіжні системи;
- стратегічне та оперативне управління банком;
- дистанційне банківське обслуговування та кредитування. [1]

Сучасний банк – це централізована система, яка працює завдяки потужним IT-рішенням. Однією з ключових інновацій, яка лежить в основі сучасного банку, є автоматизована банківська система (АБС). [2]

АБС дозволяє:

- оцифрувати основні операційні процеси банків, підтримувати їх безперервну роботу;
- забезпечувати безпеку та надійність високого рівня;
- управляти великими обсягами інформації.

Прикладом такої системи є ABS Bars, що є автоматизованою банківською системою від UNITY-BARS та являє по собі програму – ядро, воно є основою будь-якої системи.

По суті це – інтерфейс, котрий має можливості зареєструвати співробітників, а також створити організацію структури банку. Потім до готового рішення підбираються модулі, для роботи з конкретними задачами, а саме:

– кредитування;
– проведення транзакцій;
– робота кас;
– облік клієнтів, особистих рахунків та операцій.

Тобто, АБС – це пов’язаний набір засобів і методів роботи з інформацією для управління банком.

Ще з початку 70-х років стало очевидним, що потужність систем обробки банківської інформації недостатньо надійна і швидка. Ручна обробка документів не дозволяла швидко обмінюватися інформацією між більшістю банків, їх філіалами по всьому світу. Крім того, ручна обробка приводила до помилок, збоїв у роботі. Різні банки застосовували різні системи розрахунків, що приводило до їх практичної несумісності. Це підштовхнуло фахівців європейських і північноамериканських банків до необхідності розробки і створення єдиної «мови» фінансових повідомлень, єдиної системи передачі банківської інформації. [3]

Рішенням проблеми стало створення товариства міжнародних міжбанківських телекомунікацій, яке отримало назву «SWIFT». Метою товариства є створення та використання засобів, для швидкої та безпечної обробки й передачі інформації

До переваг SWIFT відноситься:
– підвищення ефективності роботи банків;
– забезпечення надійності та безпеки при передачі даних;
– використання стандарту повідомлень.

Отже, автоматизація дозволяє банкам стати більш ефективними та конкурентоспроможними на ринку. Завдяки ній вдається оптимізувати операційні процеси, зменшити витрати та покращити якість обслуговування клієнтів. Розробка інформаційних систем для сфери банкінгу дозволила трансформувати індустрію фінансів. Настільки звичні нам банківські мобільні додатки не мали б змоги працювати, якби діяльність банку не була автоматизована.

Проте індустрія не стоїть на одному місці, сучасні реалії спрямовані на конкурентність, банки намагаються знайти нові шляхи прискорення та забезпечення безпеки транзакцій, в свою чергу розробники програмного забезпечення пропонують все більше рішень.

Список використаних джерел

1. Сучасні інформаційні технології в банківській сфері.
URL: http://dspace.oneu.edu.ua/jspui/bitstream/123456789/8638/1/Сучасні%20інформаційні%20технології%20в%20банківський%20сфері.pdf
2. Що таке ABS та як вона зробила банки швидшими та ефективнішими. URL: https://www.zhitomir.info/news_218198.html
3. Сучасні можливості використання інформаційних технологій у банківській справі URL: https://forinsurer.com/public/03/02/06/265

УДК: 004.7.032.2:004.056

РОЗУМНА ТРОСТИНА ДЛЯ СЛАБОЗОРИХ НА БАЗІ ARDUINO NANO

Жигалкін Є. В.
Науковий керівник – к.т.н., доцент Рахліс Д. Ю.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. АПОТ, тел. (057) 702-13-26
e-mail: yehor.zhyhalkin@nure.ua.

Computers are ubiquitous in our lives, but microcontrollers, often overlooked, are essential in powering many devices beyond smartphones. This document presents the development of a Smart Cane system utilizing Arduino technology to assist blind individuals in navigating their surroundings safely. The system integrates ultrasonic distance sensors and light sensors to detect obstacles and be visible in the dark. Controlled by an Arduino microcontroller, the Smart Cane provides real-time feedback through haptic alerts. This innovative solution enhances the mobility and safety of visually impaired individuals, offering potential for further refinement and expansion in future versions.

Вступ.

У сучасному світі виробництво доступних засобів адаптації для людей з обмеженими можливостями стає надзвичайно важливою проблемою. Розробка «розумної» тростини для слабозорих на базі Arduino Nano є актуальним відгуком на цю потребу. Ця робота націлена на вирішення проблеми недостатньої доступності засобів навігації для людей зі зниженим зором. Використання Arduino Nano дозволяє створити засіб, який надає інформацію про навколишнє середовище, що є критичним для безпеки та комфорту слабозорих. Це дослідження не лише технічно вдосконалює існуючі рішення, але й сприяє розвитку інклюзивного суспільства, де кожна людина має можливість вільно пересуватися та відчувати себе безпечно.

Метою роботи є створення моделі «розумної» тростини та програми прошивки для плати Arduino.

Для досягнення поставленої мети потрібно вирішити наступні *завдання*.

1. Дослідити основні функції тростини, розробити модель на базі Arduino Nano.
2. Обрати компоненти для створення прототипу, перевірити їх працездатність та зібрати схему на їх базі.
3. Створити програму-прошивку та протестувати її.

Об'єктом дослідження є застосування мікроконтролерів для допомоги людям з обмеженими можливостями, а *предмет дослідження* – створення прототипу на базі плати Arduino Nano та додаткових модулів.

Зміст дослідження. Для базової роботи “розумної” тростини потрібна плата Arduino Nano з чіпом Atmega 328p [1], ультразвуковий датчик наближення HC-SR04, датчик рівня освітленості на базі LM393, світлодіоди, модуль вібромотору, DC-DC підвищувальний модуль CKCS BS01, модуль зарядки та захисту TP4056, акумулятор формату 18650, макетна плата та проводи до неї [2].

Алгоритм функціонування можна представити наступним чином: Arduino за допомогою датчику наближення сканує простір попереду, при виявленні перешкоди на відстані 2 метри починає періодично подавати імпульси для роботи вібромотору. При наближенні перешкоди періоди роботи поступово збільшуються, до того моменту, коли відстань до перешкоди мінімальна. У цьому випадку вібромотор працює постійно, пороги відстані спрацьовування можна виставляти у прошивці пристрою. Також під час роботи Arduino за допомогою датчику освітлення вимірює кількість світла у навколишньому середовищі і при перетинанні порогу вмикаються світлодіоди, які мають позначити слабозору людину у темряві [3].

Висновки. В ході виконання роботи було створено модель «розумної» тростини для слабозорих на базі Arduino. Для реалізації прототипу було обрано відповідні компоненти. Програмну реалізацію було виконано в інтегрованому середовищі розробки Arduino IDE, скетч для якої було написано мовою C++. Дана розробка є актуальною у сфері сучасних комп’ютерних технологій, які використовують для вдосконалення звичних нам речей, щоб зробити їх більш функціональними та зручними. Запропонований прототип «розумної» тростина може бути використан як матеріал для майбутніх досліджень у цій сфері та при доопрацюванні буде корисним для людей з обмеженими можливостями.

Наукова новизна та практична цінність результатів визначається використанням мікроконтролера Arduino для покращення умов життя людей з обмеженими можливостями. «Розумна» тростина надає більше інформації про навколишнє середовище, ніж звичайна. Це допоможе людям із слабким зором краще орієнтуватися у просторі та більш легко пересуватися.

Список використаних джерел:

1. Arduino – Products [Електронний ресурс]. – Режим доступу: www.arduino.cc/Main/Products. − Дата звернення: 01.03.2024. – Загол. з екрана.

2. Хабр-Хабр [Електронний ресурс]. – Режим доступу: https://habr.com/ru/. − Дата звернення: 29.02.2024. – Загол. з екрана.

3. Simon Monk Programming Arduino Getting Started with Sketches / McGraw Hill Professional, 2011. – 176 с.

УДК 004 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.019

КОНЦЕПТ АРХІТЕКТУРИ WEB-ЗАСТОСУНКУ ДЛЯ ПОШУКУ ТА ПРОСЛУХОВУВАННЯ МУЗИЧНИХ КОМПОЗИЦІЙ

Жук М.В., Сергородцев І.Д.
Науковий керівник – д.т.н. проф. Фесенко Т.Г.
Харківський національний університет радіоелектроніки, каф. ЕОМ,
м. Харків, Україна
тел. +38(063) 951-73-72, e-mail: maksym.zhuk@nure.ua;
тел.+38(050) 274-67-92, e-mail: illia.serhorodtsev@nure.ua.

The work examines the peculiarities of the development of web applications for searching and listening to musical compositions. A scheme of the three-level architecture of the web application is proposed. The first level is the user interface (using React and Redux technologies). The second level is business logic (using the Nest.js framework). The third level is data access (using MongoDB databases in JSON format).

Відомо, що музика має значний вплив на тільки на моральний, емоційний, інтелектуальний стан людини, а й на роботу внутрішніх органів і фізичний стан людини в цілому. Музика розглядається як ефективний інструмент для розвитку покращення пам’яті, розумових здібностей логічного мислення [1]. Підтримка різних культурних та соціальних ініціатив, збереження історичного характеру і відновлення естетичного та культурного середовища міста віддзеркалюється на інфраструктурі міста [2], стратегіях сталого розвитку [3]. В проєктах післявоєнної відбудови українських міст необхідно враховувати спеціальні соціально-культурні ландшафти, у тому числі із застосуванням сучасних інформаційно-комунікативних технологій (ІКТ).

В галузі ІКТ все більшої популярності отримують розробка web-застосунків для пошуку та прослуховування музичних композицій. Вони дозволяють користувачам швидко та зручно знаходити музику, зберігати улюблені треки та створювати власні плейлисти. Розробка таких web-застосунків реалізується із застосуванням алгоритму трирівневої архітектури, де кожен рівень абстракції (або шару) відповідає за певні функції і має чітко визначений інтерфейси для взаємодії з іншими рівнями (рисунок). На першому рівні – інтерфейс користувача – розміщуються всі інтерфейсні елементи (кнопки, текстові поля і меню), використовуються технології React та Redux. Другий рівень – бізнес-логіка – відповідає за обробку даних і визначення логіки програми, використовується фреймворк Nest.js, заснований на архітектурі Module–Controller–Provider. Третій рівень – доступ до даних – відповідає за зберігання і взаємодію з даними. Третій рівень реалізовано на документоорієнтованій базі даних MongoDB у форматі JSON із використанням горизонтального масштабування, управління централізованими базами даних облікових записів [4] та ін.

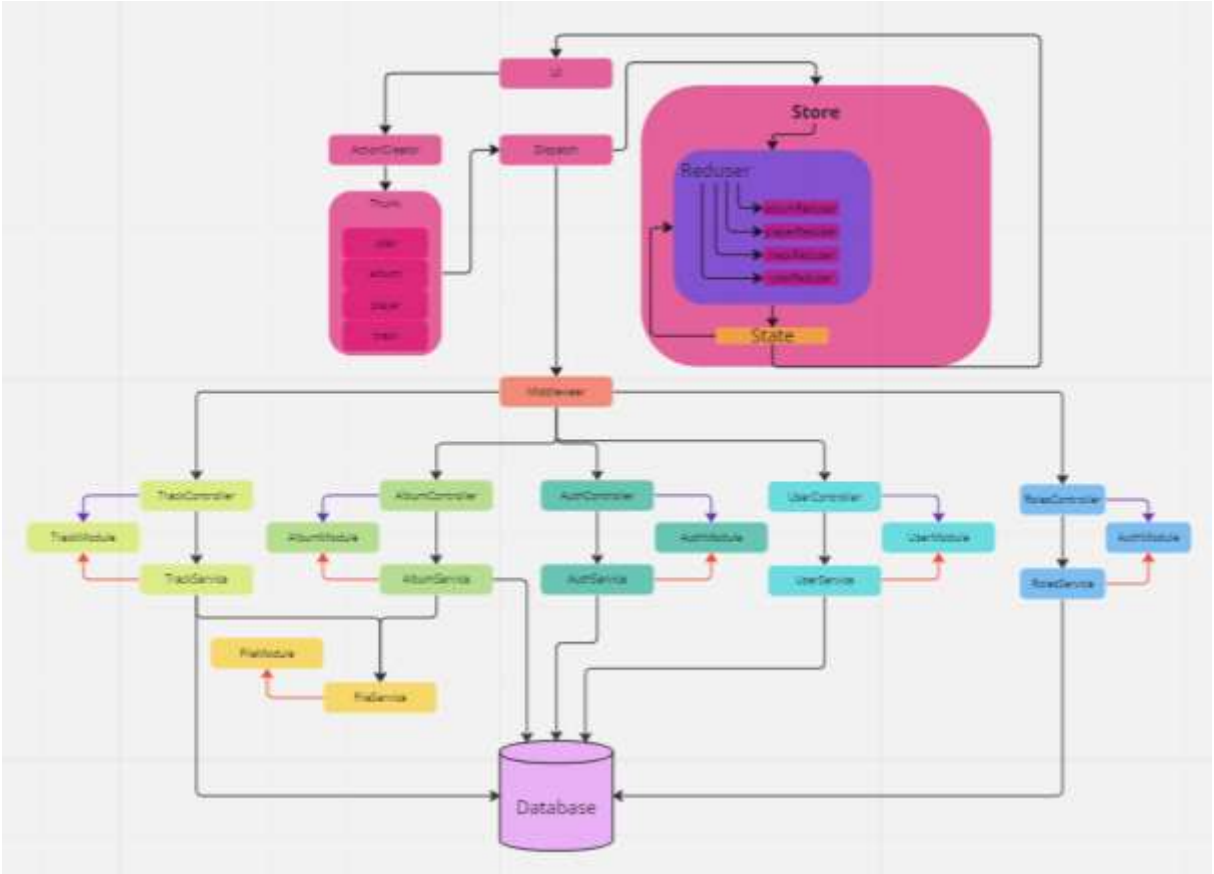


Рисунок. Схема архітектури web-застосунку для пошуку та прослуховування музичних композицій

Список використаних джерел:

1. Рєзанова В. В. & Фесенко Т. Г. (2012). Фінансування шкіл естетичного виховання м. Чугуєва Харківської області: гендерний вимір бюджетної політики. Гендерні аспекти бюджетування на місцевому рівні : практ. посібн., Київ, 27–29.

2. Фесенко Г.Г. & Фесенко Т.Г. (2018). Креативні локації як форма редевелопменту міських територій. Матеріали X Ювілейної Міжнародної науково-практичної конференції «Європейський вектор модернізації економіки: креативність, прозорість та сталий розвиток». Тези доповідей. Частина 2 , Харків: ХНУБА, 219–221.

3. Фесенко Г.Г. & Фесенко Т.Г. (2012). Cultural Management как механизм реализации муниципальных стратегий устойчивого развития городов. Исследование систем менеджмента отраслевых организаций: теория и практика: сб. науч. ст. VIII междун. науч.-практ. конф.: Урал. гос. пед. ун-т; под науч. и общ. ред. Л. Ю. Шемятихиной, 234–237.

4. Rezanov, B., Semenova, A., Petrovska, I. & Fesenko T. (2021). Model for Providing the Second Factor of Authentication Into Authentication Services with Centralized Account Databases. Fifth International Scientific and Technical Conference “Computer and information systems and technologies”, 46–47. https://doi.org/10.30837/csitic52021232201.

УДК 004.93 : 159.9 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.021

СИСТЕМА ВИЗНАЧЕННЯ РИЗИКІВ РОЗВИТКУ ПТСР ПІД ЧАС ДИСТАНЦІЙНОГО НАВЧАННЯ З ВИКОРИСТАННЯМ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ

Заброда І.С.
Науковий керівник – к.т.н., доц. Барковська О.Ю.
Харківський національний університет радіоелектроніки, каф ЕОМ,
м. Харків, Україна
e-mail: ivanzabroda62@gmail.com

This article considers the relevance and problematics of diagnosing PTSD in students who study with the help of distance learning in wartime. The experience of the state institution "Institute of Eye Diseases and Tissue Therapy named after V.P. Filatov of the National Academy of Medical Sciences of Ukraine" in diagnosing PTSD by means of eye movement is considered.

Вже більше двох років триває повномасштабне вторгнення російських військ на територію України та понад десять років, як бойові дії ведуться на території Донбасу та анексованого Криму. Ці події змінили відчуття безпеки людей, призвели до стресу, психологічні наслідки якого проявлятимуться в майбутньому в дорослих та дітей. Для декого це може стати причиною розвитку посттравматичного стресового розладу (далі ПТСР), як крайньої реакції психіки на сильний стрес, що загрожує життю людини [1]. В учнів та студентів ПТСР може мати різні прояви. Наприклад, діти, які зазнали психологічних травм мають затримки в когнітивному та мовному розвитку [2]. Слід відмітити, до у дітей з ПТСР значно погіршується увага та виконавчі функції під час навчання [3]. Бойові дії та підвищена ракетна небезпека в окремих регіонах нашої держави унеможливлюють навчання дітей у школах в режимі оффлайн, що ускладнює вербальне спілкування між учнем та викладачем. За таких умов викладання вчасно виявити проблему та порекомендувати звернутися до відповідного спеціаліста за допомогою виявляється складно.

Тому, створення системи дистанційного визначення ризиків розвитку ПТСР під час дистанційного навчання з використанням загорткових нейронних мереж є задачею актуальною у нас час.

Запропонована система базується на отриманні потоку відео та аудіо даних з підсистеми комунікації (наприклад, під час онлайн-відеоконференцій із підключеною веб-камерою учня з роздільною здатністю не нижче Full HD), як складової системи управління навчанням (LMS), із подальшим аналізом отриманої інформації та зберігання на віддаленому сервері. За допомогою використання штучного нейромережевого аналізатора згорткового типу пропонується виконати детектування та аналіз одного із діагностичних критеріїв посттравматичного стресового розладу, а саме – реакцію очей на

подразники – нестабільність фіксації погляду на предметі (як результат підвищеної збудливості пацієнта), гіперреакція та підвищена чутливість симпатичної нервової системи на стрес та інші подразники (наприклад, звуження зіниць) [4,5]. Встановлено, що за наявності ПТСР змінюється рух очей. Непомітні дрібні, швидкі та безсвідомі рухи очей називаються мікросакадами. Саме ці рухи очей є об'єктом дослідження у роботі. Визначити характер мікросакад можливо використовуючи технологію ай-трекінгу.

Вітчизняні вчені з ДУ "Інститут очних хвороб і тканинної терапії ім. В.П. Філатова НАМН України", опублікували дослідження в 2019 році про вивчення стану зіниць як маркерів ПТСР в осіб, які проживають у зоні АТО. В ході дослідження було встановлено, що діаметр зіниць в групі людей, що проживають в зоні АТО більший, найближча точка конвергенції видалена, а обсяг акомодації значно менший порівняно з контрольною групою. Виявлено пряму позитивну достовірну кореляцію між діаметром зіниці та найближчою точкою конвергенції — 0,71 ($p<0,05$) [6].

Одним з ефективних рішень для дослідження руху очей та стану зіниці ока є розробкою температурних або туманних шкал погляду для аналізу емоційного стану людини. Результатом роботи запропонованої системи є сформований звіт про динаміку змін психо-емоційного стану пацієнта, що також може бути використано вчителями для пояснення можливої причини відставання учня при вивченні навчального матеріалу.

Список використаних джерел

1. Ressler, K. J., Berretta, S., Bolshakov, V. Y., Rosso, I. M., Meloni, E. G., Rauch, S. L., & Carlezon Jr, W. A. (2022). Post-traumatic stress disorder: clinical and translational neuroscience from cells to circuits. Nature Reviews Neurology, 18(5), 273-288.

2. Pfeiffer, E., Sachser, C., Tutus, D. et al. Trauma-focused group intervention for unaccompanied young refugees: "Mein Weg"–predictors of treatment outcomes and sustainability of treatment effects. Child adolesc psychiatry ment health. 2019. Vol. 13, no. 18. URL: https://doi.org/10.1186/s13034-019-0277-0. 4)

3. Sue R. Beers, Ph.D., and Michael D. De Bellis, M.D., M.P.H. Neuropsychological Function in Children With Maltreatment-Related Posttraumatic Stress Disorder. The American journal of psychiatry. 2002. Vol. 159(3). P. 483–486. URL: https://doi.org/10.1176/appi.ajp.159.3.483.

4. Fawcett, C., Wesevich, V., Gredebäck, G. (2016). Pupillary contagion in infancy: Evidence for spontaneous transfer of arousal. Psychological science, 27(7), 997-1003.

5. Barkovska, O., Axak, N., Rosinskiy, D., & Liashenko, S. (2018). Application of mydriasis identification methods in parental control systems. In 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (pp. 459-463).

6. Науменко В. А. та ін. Особливості зорових функцій в осіб, які проживають у зоні АТО, як маркер посттравматичного стресового розладу //Український медичний журнал. - 2019. - №. 1 (2). - С. 43-44.

УДК 004.5+004.7 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.023

WEB-ЗАСТОСУНОК ДЛЯ РОЗРАХУНКУ МАРШРУТУ ЕЛЕКТРОМОБІЛІВ

Зюнд Б.В.
Науковий керівник – ас. Андрусенко Ю.О.
Харківський національний університет радіоелектроніки, каф. ЕОМ, м. Харків, Україна
тел. +38(067)573-37-46, e-mail: bohdan.ziund@nure.ua

This work is devoted to the development of a web application for finding and routing to charging stations for electric vehicles. Problems that drivers of electric cars may face were considered. The relevance of the program and its necessity in the modern world, possible functionality, such as wayfinding considering charging stations and preferences of different types of charging stations, are considered. Technologies that will be used were considered. Algorithms for finding the shortest path were considered. Analogues of this program and their shortcomings are considered.

У сучасному світі електромобілі стають дедалі популярнішими, наразі електроенергія дешевше будь-якого різновиду палива, також вкрай важливою перевагою електромобілів є їх екологічність. Це стало однією з основних причин по якій даний вид транспорту став дуже популярним у всьому світі. Відсутність вихлопів дозволяє ефективно знизити негативний вплив на навколишнє середовище і природу[5].

Електромобілі мають обмежену дальність поїздок в порівнянні з автомобілями з двигуном внутрішнього згоряння. Веб-додаток може надати їм можливість швидко знаходити оптимальні маршрути з урахуванням доступних зарядних станцій.

В багатьох регіонах недостатньо зарядних станцій, або вони розташовані у важкодоступних місцях - це ускладнює пошук станцій під час планування маршруту. Також існують різні типи зарядних станцій з різною потужністю та сумісністю з різними моделями електромобілів. Водії потребують інформацію про доступні типи станцій та їхню сумісність з їхнім транспортним засобом.

Використання електромобілів сприяє зменшенню викидів шкідливих речовин у атмосферу. Розробка додатка, який сприяє зручнішому користуванню електромобілями може заохочувати більше людей переходити на електромобілі, що має позитивний екологічний вплив.

При огляді існуючих веб-додатків для планування маршруту та пошуку зарядних станцій для електромобілів було виявлено, що вони мають обмежену базу даних зарядних станцій або не мають можливості розраховувати маршрути.

Наприклад, єдиний аналог додатку для розрахунку маршруту електромобілів в Україні: «UGV Chargers» відображає не всі наявні зарядні станції.

Запропонований Веб-додаток зможе визначати найкоротший шлях до точки призначення з урахуванням можливих зупинок для зарядки, збирати та обробляти інформацію про доступні зарядні станції, включаючи їхнє розташування, типи станцій, потужність зарядки, ціни та режими роботи, використовувати картографічні інструменти для візуалізації маршруту та розташування зарядних станцій на мапі.

Для розрахунку найкоротшого шляху може використовуватися алгоритм A* або алгоритм Дейкстри.

Алгоритм A* шукає найкоротший шлях у графі від початкової точки до кінцевої точки, використовуючи два критерії: вартість поточного шляху та оцінку залишкової вартості до кінцевої точки. Він вибирає найбільш перспективні вершини для перегляду, що дозволяє ефективно знаходити шляхи. A* ефективно використовує оцінки відстані для керування процесом пошуку та шляхом зменшує кількість вершин, які необхідно обробити, що робить його швидшим і менш вимогливим до ресурсів[1].

Алгоритм Дейкстри шукає найкоротший шлях від початкової точки до всіх інших точок у графі, рухаючись від вершини до вершини та оновлюючи відстані до сусідніх вершин. Він обирає найкоротший доступний шлях на кожному кроці, поступово розширюючи зону, що відвідується[1].

Користувач зможе фільтрувати зарядні станції за різними критеріями та встановлювати свої власні налаштування, такі як уподобані типи зарядних станцій.

Для клієнтської частини веб-додатку будуть використовуватися технології HTML/CSS/JavaScript для створення користувацького інтерфейсу, включаючи розміщення елементів на сторінці, стилізацію та інтерактивність[4]. Фреймворки такі як React.js, Angular або Vue.js, для зручного управління станом додатка та створення складних інтерфейсів[3].

У серверній частині буде використовуватися мова програмування Java та фреймворк Spring, для швидкої і ефективної розробки серверної логіки та API[2].

Список використаних джерел:

1. Sedgewick R., Wayne K. Algorithms. 4th edition. Princeton University: Addison-Wesley, 2019. 848 p.

2. Андрусенко Ю.О. Нестаціонарність ресурсів та послуг хмарної інфраструктури / Ю.О. Андрусенко, Т.Г. Фесенко // Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, 2023. - Т.4(74). – С. 129–133. doi: https://doi.org/10.26906/SUNZ.2023.4.129.

3. Ткачов В.М. Критерії вибору стандарту безпровідної передачі даних у високомобільних комп'ютерних мережах / В.М. Ткачов, К.Р. Гальченко, А.А. Коваленко, О.А. Єрошенко // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 4 (66). – С. 63-68. – doi: https://doi.org/10.26906/SUNZ.2021.4.063

УДК 004.27

ОСОБЛИВОСТІ МОВИ ПРОГРАМУВАННЯ JAVA ТА ХМАРНИХ ТЕХНОЛОГІЙ

Ілляшенко І.Б.
Науковий керівник - доцент кафедри інформаційних управляючих систем, кандидат технічних наук Сердюк Н. М.
Харківський національний університет радіоелектроніки, каф. КІТС
м. Харків, Україна
e-mail: ilona.illiashenko@nure.ua

This article demonstrates the benefits of using cloud computing in Java-based software as an important component of modern web development. Cloud computing is considered so revolutionary because it frees companies from maintaining their own servers, paying for a huge IT department and being responsible for cyber security in a rapidly changing security environment. It enables companies to quickly deploy and manage applications, minimizing infrastructure costs and ensuring optimal performance. Cloud computing is another area of the IT market that is the future and where Java is not only used, but often the main language. This paper describes an attempt to predict the future of Java and cloud computing based on the current situation.

Хмарні технології за останнє десятиліття перестали бути чимось особливим в розробці програмних систем і сьогодні вони є невід´ємною частиною більшості бізнес-процесів. Крім того, хоча ринок хмарних обчислень стабільно зростав із середини 2000-х років, криза COVID-19 швидко прискорила впровадження хмарних технологій у різноманітних секторах [1].

Зі зростаючим попитом на масштабовані, надійні та економічно ефективні рішення компанії переносять свої веб-програми в хмару, щоб скористатися її численними перевагами [2]. Cloud computing дозволяє швидко розгортати програми та керувати ними, мінімізуючи витрати на інфраструктуру та забезпечуючи оптимальну продуктивність, що є звичайно є ключовим аспектом, але не єдиним, під час прийняття рішення переходу до хмарних технологій. До переваг їх використання можна також віднести високу доступність, підтримку провайдерів, глобальне охоплення та керовані зони доступності.

Прогнозується, що ринок хмарних обчислень продовжить рости швидше, ніж будь-коли, і очікується, що мова програмування Java відіграватиме велику роль у цьому типі розробки програмного забезпечення [3]. Розробники, що використовують cloud computing, цінують дану мову програмування не тільки через використання розподілених і паралельних обчислень, а й також через широкий набір засобів автоматизації.

Крім того, завдяки своїй платформонезалежності, обширним бібліотекам і широкому спектру фреймворків Java добре підходить для розробки масштабованих і підтримуваних хмарних веб-додатків. Її надійність і здатність виконувати складні завдання роблять Java популярним вибором серед розробників. Серед найвідоміших хмарних інструментів, які роблять процес розробки програмного забезпечення більш простим, ефективним і безпомилковим можна виділити наступні, які є найвикористовуванішими в цій сфері:

– AWS SDK for Java – це комплект засобів розробки для роботи з сервісами AWS [4];

– Oracle Java Cloud Service. Тут можна створювати, налаштовувати, керувати та масштабувати середовище додатків Java Enterprise Edition в Oracle Cloud [5];

– Cloudfoundry дозволяє сформувати інфраструктуру для виконання в хмарних оточеннях кінцевих застосунків на Java та інших мовах, що працюють поверх JVM;

– Microsoft Azure надає ряд послуг і інструментів для створення, розгортання та керування веб-додатками Java у хмарі;

– Heroku Java. Це хмарна платформа, заснована на керованій контейнерній моделі, з інтегрованими службами даних та потужною екосистемою для розгортання та запуску сучасних додатків;

– Google App Engine дозволяє легко розгортати та запускати стандартні веб-програми Java з використанням Servlet.

Використовуючи потужність Java і хмарних обчислень, можна створювати масштабовані, безпечні та високопродуктивні веб-програми, які відповідають постійно зростаючим вимогам сучасного бізнесу.

Всі вищенаведені переваги можуть гарантувати, що Java залишатиметься важливою для розробників хмарних обчислень як у найближчій, так і в довгостроковій перспективі.

Список використаних джерел:

1. How The Pandemic Has Accelerated Cloud Adoption. https://www.forbes.com/sites/forbestechcouncil/2021/01/15/how-the-pandemic-has-accelerated-cloud-adoption/?sh=65ebb96e6621

2. О.Ф. Лановий, А.К. Кульмінський. Біоніка інтелекту. Використання даних як сервісу за допомогою хмарних технологій. 2017. № 2 (89). С. 177–182.

3. Moving Java workloads to cloud environments. https://redhat.com/en/resources/java-in-cloud-computing-detail.

4. AWS SDK for Java. https://aws.amazon.com/de/sdk-for-java/.

5. Oracle Java Cloud Service. https://docs.oracle.com/en/cloud/paas/java-cloud/index.html.

УДК 004.415:331.536 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.027

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ РОЗМІЩЕННЯ ВАКАНСІЙ

Кузнєцов Д.О.
Науковий керівник – ас. Андрусенко Ю.О.
Харківський національний університет радіоелектроніки, каф. ЕОМ,
м. Харків, Україна
тел. +38(095) 888-95-42, e-mail: dmytro.kuznietsov@nure.ua.

This work was created with the aim of developing an up-to-date workable model related to the placement of a finished product that will be competitive in the labor market and will be relevant for a wide range of clients. The application is a web development for distributing content related to resumes, vacancies, and projects. It is completely competitive and implements all the necessary functionality. The program is capable of storing, searching and retrieving the necessary data for the client, such as information about the client, projects, vacancies, all relevant data, and is also capable of validating them.

Сьогодні ринок веб-застосунків досить обширний, але через значні витрати на розробку, кожна з програм має явні недоліки, найпоширенішим з яких є відсутність складної валідації даних за багатьма параметрами через потребу в потужній середі підтримки серверу. Якщо прибрати витрати на розробку продукту, то забезпечення підтримки хостингу стоїть на першому місці серед усіх витрат на тестування, безпеку та реалізацію. З метою надання конкурентності було створено веб-додаток з можливістю пошуку за всіма параметрами, які існують у програмі. Завдяки цьому, кожен користувач має можливість знайти найбільш необхідну інформацію [1].

На відміну від аналогів, цей застосунок надає клієнту весь необхідний інтерфейс для пошуку, додавання та редагування інформації. Сучасні фреймворки дозволяють мати значно більший ніж у конкурентів та адаптований під сучасний ринок функціонал [2].

Можна навести наступні основні переваги додатку:

1) використання сучасної мови розробки, а саме Java 17 та React;
2) спрощена та оптимізована база даних з використанням реляційної бази PostgreSQL;
3) розширений функціонал з покроковим тестуванням на рівні програмного коду (Unit tests, Integrational tests) та мануального тестування (Swagger, Postman);
4) надання додатку конкурентно-спроможного функціоналу згідно з аналогами на ринку веб-додатків;
5) використання усіх найсучасніших модулів розробки та тестування задля забезпечення стабільної та швидкої роботи програми.

Найголовнішою перевагою є те, що оптимальна база даних забезпечує швидкий пошук та обмін даними між усіма сервісами. Найсучасніші модулі

дозволяють використовувати усі необхідні бібліотеки для розробки повноцінного застосунку. Явною відмінністю програми є також використання фреймворку Spring, що є похідним інструментом від мови Java. Унікальністю цього фреймворку є використання усіх оптимізованих паттернів програмування та структуризації даних. Завдяки цьому, подальша розробка та підтримка продукту є досить оптимальною та легкою для будь-якого веб-розробника.

Як і у застосунках-аналогах, кожен користувач може зареєструватися та увійти у свій профіль, який у свою чергу буде мати підтримку всіх сучасних модулів безпеки. Він матиме свій віртуальний кабінет, де можна буде розташовувати всі вакансії та використовувати весь можливий функціонал задля налаштовування інформації.

Для коректної та стабільної роботи в інтернет просторі, необхідно мати сервер із швидким інтернет-налаштуванням та наступними мінімальними параметрами [3]:

1) сервер Amazon AWS;
2) мінімум 1 тб швидкої пам’яті SSD;
3) мінімум 32 гб оперативної пам’яті;
4) процесор Intel Xeon або Intel Atom останній поколінь.

Серед необхідних потреб рекомендовано мати актуальні версії програмного забезепечння та системи перешкодження DDos атак, які встановлені на стороні серверу.

У результаті відгук на будь-яку функцію буде не більше 1 секунди та зростатиме за всіма правилами складності сортування із збільшенням обсягу даних на сервері. Інформація буде перебувати на сервері не більше 5-ти років, після чого він буде оновлювати дані задля оптимізації та швидкості відгуку сайту, зокрема надання актуальних результатів пошуку. Веб-застосунок підтримується усіма необхідними браузерами та може використовуватися як на мобільному девайсі, так і на комп’ютері, ноутбуці або планшеті, що робить застосунок кросплатформенним та збільшує кількість потенційних користувачів.

Список використаних джерел:

1. Крейг Уоллс. Spring in actions. — Третє. — М. : «Manning», 2014. — 624 с. — ISBN 9781617291203

2. Андрусенко Ю.О. Нестаціонарність ресурсів та послуг хмарної інфраструктури / Ю.О. Андрусенко, Т.Г. Фесенко // Системи управління, навігації та зв’язку. Збірник наукових праць. Полтава: ПНТУ, 2023. - Т.4(74). – С. 129–133. doi: https://doi.org/10.26906/SUNZ.2023.4.129.

3. Ткачов В.М. Критерії вибору стандарту безпровідної передачі даних у високомобільних комп’ютерних мережах / В.М. Ткачов, К.Р. Гальченко, А.А. Коваленко, О.А. Єрошенко // Системи управління, навігації та зв’язку. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 4 (66). – С. 63-68. – doi: https://doi.org/10.26906/SUNZ.2021.4.063

УДК 004.85 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.029

АНАЛІЗ ПІДХОДІВ У ВИЯВЛЕННІ АНОМАЛІЙ В ЗОБРАЖЕННЯХ ОПТИЧНОГО МОНІТОРИНГУ

Мельніченко Ф. О.
Науковий керівник - проф. Рубан І. В.
Харківський національний університет радіоелектроніки, каф. ЕОМ,
м. Харків, Україна
E-mail: fedir.melnychenko@nure.ua

In today's world, image processing and analysis from optical monitoring sources is an important area of research due to its wide range of applications. Analyzing such images poses a major challenge for researchers and scientists due to the high variability, low resolution, and large volume of satellite imagery data. One of the fundamental tasks of image analysis from optical monitoring sources is anomaly detection. Anomaly detection in optical monitoring images (satellites, drones, unmanned aerial vehicles) is an important area of remote sensing and geospatial analysis that uses advanced algorithms and machine learning models to detect unusual patterns or changes in data that deviate from the norm. This capability is essential for a wide range of applications, from environmental monitoring and urban planning to military defense, reconnaissance and disaster response. In this article, we will look at common anomaly detection methods and technologies.

В сучасному світі обробка та аналіз зображень з джерел оптичного моніторингу (супутники, дрони, безпілотні літальні апарати, тощо), є важливою сферою досліджень завдяки широкому спектру застосувань. Аналіз зображень такого роду створює ряд викликів для дослідників та науковців через високу мінливість та неоднорідність, низьку роздільну здатність та великі розміри зображень. Одна із фундаментальних задач в аналізі зображень оптичного моніторингу є виявлення аномалій та текстурних аномалій.

Процес виявлення аномалій (з англ. *anomaly detection*) – це процес виявлення незвичайних патернів або поведінки у даних, які суттєво відрізняються від більшості даних. Ці невизначені патерни, також відомі як аномалії, викиди, винятки або новинки, не відповідають очікуваній поведінці та часто вказують на критичні інциденти, нестандартну поведінку, або появу нового, тощо. В свою чергу, виявлення текстурних аномалій — це підмножина задач у виявленні аномалій, зосереджена саме на аналізі текстурних патернів у зображенні. Даний метод спрямований на виявлення областей, де структура текстури відхиляється від норми, що вказує на потенційні аномалії або дефекти. Можна побачити, що виявлення аномалій і виявлення текстурних аномалій – це методи, які використовуються для виявлення порушень у наборах даних або зображеннях, але вони зосереджені на різних аспектах і застосовуються в різних контекстах.

Розкриваючи методи та технології, що використовуються для виявлення аномалій на зображеннях, ми розглянемо, які методи існують, їх основні принципи та конкретні проблеми, які вони вирішують. Ця сфера поєднує методи обробки зображень, моделі машинного навчання та предметні знання для ефективного виявлення аномалій із даних оптичного моніторингу. Розглянемо їх.

Одним із перших класів методів можна виділити машинне навчання та глибоке навчання.

Метод навчання з вчителем: цей підхід вимагає позначених наборів даних для навчання моделей, які можуть класифікувати або ідентифікувати аномалії на нових зображеннях, які не бачили. Даний підхід особливо корисний, коли потрібно виявити певні типи аномалій або змін (тобто класифікація аномалій). Навчання з вчителем вимагає правильно формування набору даних для навчання та постійного тюнінгу моделі.

Метод навчання без вчителя: у випадках, коли помічених даних мало або аномалії не чітко визначені, алгоритми такого типу навчання можуть ідентифікувати незвичні шаблони або кластери в даних без попереднього помічення. Типовими прикладами є такі методи, як K-mean кластеризація або аналіз головних компонентів (PCA).

Методи глибокого навчання: згорткові нейронні мережі (CNN) і рекурентні нейронні мережі (RNN) це доволі потужні моделі глибокого навчання, які використовуються для обробки та аналізу зображень. ЗНМ чудово розпізнають просторові візерунки на зображеннях, а РНМ можуть аналізувати часові зміни даних з часом. Також в цю категорію можна віднести Автокодери (Autoencoder), які використовуються для виявлення аномалій, навчаючись стискати (encoding process) та потім розтискати (decoding process) вхідні дані. Помилка реконструкції (різниця між входом і виходом) може сигналізувати про аномалії.

Наступним окремим класом методів можна винести виявлення змін. У контексті виявлення аномалій в зображеннях методи виявлення змін відповідають визначенням значних змін на поверхні з часом шляхом порівняння зображень, зроблених у різні дати однієї зони інтересу. Методи виявлення змін відрізняються за складністю та застосовністю залежно від конкретних вимог завдання, таких як роздільна здатність зображень, область інтересу та тип зміни, який потрібно виявити. Методи виявлення змін можуть бути реалізовані шляхом звичайного порівняння значень піксель, або їх співвідношень, закінчуючи методами комп’ютерного зору та машинного навчання.

Але все ж таки існують виклики та додаткові проблеми у виявленні аномалій. Це пов’язано в першу чергу з величезним обсягом і різноманітністю даних у поєднанні з такими проблемами, як хмарний покрив або атмосферні та погодні умови, створюють значні проблеми, що, в свою чергу, потребує додаткових методів та рішень для фільтрації та

підготовки вхідного зображення для подальшого процесу у виявленні аномалій.

Як підсумок можемо впевнено сказати, що виявлення аномалій в зображеннях оптичного моніторингу є багатогранним завданням, яке потребує поєднання методів, адаптованих до конкретних характеристик даних і характеру аномалій, що цікавлять. Можемо сказати впевненно, що досягнення у методах машинного та глибокого навчання разом із традиційними статистичними методами та методами комп'ютерного зору пропонують потужні інструменти для вирішення такого роду задач. Однак вибір методу залежить від різних факторів, включаючи тип аномалії, доступність даних, вплив погодних умов, тощо. Також маємо зазначити, що аналіз зображень такого роду для вирішення задачі у виявлені аномалій потребує попередньої обробки: фільтрація та вирівнювання зображення, зниження шумів, виявлень хмар, розподіл зображення на тайли для паралельних обчислень.

Список використаних джерел

1. Бодянский Е.В., Руденко О.Г. Искусственные нейронные сети: архитектуры, обучение, применения. // Телетех. 2004. Vol. 369.
2. Ruban I., Khudov H., Makoveichuk O., Khizhnyak I., Khudov V., Podlipaiev V., Shumeiko V., Atrasevych O., Nikitin A., Khudov R. Segmentation of Optical-electronic Images From On-board Systems of Remote Sensing of the Earth by the Artificial Bee Colony Method //Eastern-European Journal of Enterprise Technologies. 2019. No 9. P. 37-45.
3. Ruban I., Smelyakov K., Martovytskyi V., Pribylnov D., Bolohova N. Method of neural network recognition of ground-based air objects. // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). 2018. Vol. 34. P. 589-592.
4. D. Jude Hemanth. Artificial Intelligence Techniques for Satellite Image Analysis. Springer. 2020.
5. Anomaly Detection Techniques: A Comprehensive Guide with Supervised and Unsupervised Learning. URL: https://medium.com/@venujkvenk/anomaly-detection-techniques-a-comprehensive-guide-with-supervised-and-unsupervised-learning-67671cdc9680

УДК 004.925 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.032

МОДЕЛІ ТА ІНСТРУМЕНТАЛЬНІ ЗАСОБИ ДЛЯ СТВОРЕННЯ ПІКСЕЛЬНИХ КАРТИН

Мідіна С.С.
Науковий керівник – к.т.н., доц. Ларченко Л.В.
Харківський національний університет радіоелектроніки (61166, Харків, пр. Науки, 14, каф. АПОТ, тел. (057) 702-13-26)
e-mail: serhii.midina@nure.ua

The work examines graphic editors for creating pixel paintings, and also considers ways to create pixel paintings both with the help of graphic editors and with the help of artificial intelligence and converting photos into pixel style. A microcontroller-based pixel picture model using a mobile application was developed and investigated. Methods of connecting a mobile device to a microcontroller are considered.

Актуальність теми, пов’язаної зі створенням “піксельних картин” збільшується з кожним роком. За останній час піксельне мистецтво здобуло значну популярність в кінематографі, відеоіграх та графіці. Разом з розвитком популярності піксельних картин йде розвиток програмного забезпечення для їх створення. З’являються нові можливості та функції для творчості в піксельному форматі. Нові інструменти роблять процес створення піксельних картин набагато легше та приємніше.

Мета дослідження – огляд та аналіз доступних програмних засобів та редакторів для роботи з піксельними картинами, включаючи їх функціональні можливості, переваги та недоліки; надання користувачам можливості створення фізичних та цифрових піксельних картин; розробка мобільного застосунку, що має легкий та простий функціонал для малювання піксельних картин й підключення до фізичного пристрою для їх відображення.

Растрова графіка – це спосіб показу картини як набір пікселів і кожен піксель має інформацію про колір та свою поточну позицію [1], тому вона є основою для побудови піксельних картин.

Серед основних способів створення піксельних картин є малювання картин в графічних редакторах, конвертація фотографій в піксельний стиль, генерація піксельних картин за допомогою штучного інтелекту. Найбільш відомими графічними редакторами є Adobe Photoshop, GIMP та ColorDRAW, що використовують технологію растрової графіки для малювання картин.

Для конвертації світлин в піксельні картини використовується растрова графіка разом з алгоритмами обробки зображень. Основний принцип полягає в розділенні зображення на пікселі та його подальшій обробці для набуття піксельного ефекту.

Штучний інтелект все більше набирає обертів та популярності у сфері створення піксельних картин. Існують багато сервісів, які генерують картини, зокрема, DeepArt, Pixel Art Generator.

За допомогою досліджуваної моделі піксельної картини можна створювати цифрові картини на мобільних пристроях як малюванням, так і конвертувати вже готові фотографії в піксельний стиль та передавати створену картину на фізичний пристрій, що буде її відображати. Усі подібні моделі створюються на основі базової структури, яка має у складі компоненти: мікроконтролер, модулі передачі даних, мобільний застосунок, світлодіодна матриця.

Мікроконтролер представляє собою компактний інтегрований пристрій, що містить центральний процесор, пам'ять і периферійні пристрої, які використовуються для керування різними електронними пристроями та системами [2].

Модулі передачі даних - це пристрої або компоненти, які дозволяють обмінюватися інформацією між різними пристроями або системами, наприклад, USB, Bluetooth, WiFi, Ethernet.

За досліджуваною моделлю мобільний застосунок створює піксельну картину, що підключається та передає інформацію про картину на мікроконтролер через модуль передачі даних. Інформацією є колір кожного діода матриці. Після прийому даних, мікроконтролер обробляє дані та оновлює кольори на світлодіодній матриці.

Розглянуто графічні редактори створення піксельних картин, розглянуто способи створення піксельних картин, зокрема, як за допомогою графічних редакторів, так і за допомогою штучного інтелекту та конвертування фотографій у піксельний стиль. Розроблено та досліджено модель піксельної картини на основі мікроконтролера з використанням мобільного застосунку, розглянуто способи підключення мобільного пристрою до мікроконтролера.

Список використаних джерел:

1. R. Shafflbotem, Photoshop CC in easy steps, In Easy Steps. – 2014. – С. 18–20.

2. M. Banzi, M. Shiloh, Getting Started with Arduino, Maker Media – 2015. – С. 15-18.

УДК 004.77 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.034

ОГЛЯД ТЕХНОЛОГІЇ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ У МІКСОВАНИХ VPN-ЛАНЦЮГАХ

Міхнов Є.Д.
Науковий керівник – к. т. н., доц. Ткачов В.М.
Харківський національний університет радіоелектроніки, каф. ЕОМ,
м. Харків, Україна
e-mail: yevhen.mikhnov@nure.ua

In this paper, the most common load balancing technologies in mixed VPN chains are considered. A critical analysis of these technologies has been conducted, including scenarios of their use, potential drawbacks, and implementation challenges. This publication serves as a review and is intended to summarize known methods.

З метою побудови високозахищених систем віддаленого доступу застосовується складні багатошарові або міксовані VPN-тунелі [1]. Такі рішення, як правило, мають місце в організації бізнес-процесів з використанням гібридних хмарних рішень або багатошарових схем віртуалізації на рівні приватних хмар.

Інша сфера застосування може мати місце при вирішенні задач, пов'язаних з досягненням високого рівня анонімності при роботі у мережі Інтернет [2].

Однак, у підходах щодо створення міксованих VPN-ланцюгів виникає проблема ефективного розподілу мережного трафіку між VPN-серверами, VPN-оптимізаторами та іншими підсистемами, які відповідають за маршрутизацію захищеного трафіку. Найчастіше дана задача пов'язана з перевантаженням каналів зв'язку, які представлені у вигляді віртуальних тунелів або шифрованих каналів (рис. 1).

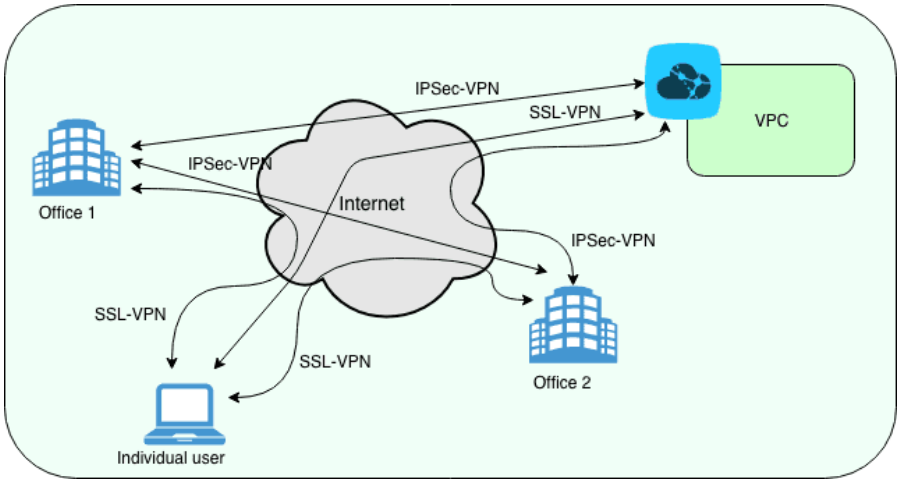


Рисунок 1 – Приклад мульти-VPN архітектури

Метою даної роботи є огляд та критичний аналіз існуючих технологічних рішень щодо вирішення вказаної задачі. В теорії комп'ютерної інженерії цю задачу можна класифікувати як задачу балансування мережного навантаження [3].

Одним із ефективних рішень є класичні мережні балансувальники, наприклад Load Balancer, Finagle та інші. Однак, недоліком даних рішень є недостатній рівень захищеності вхідних та вихідних інтерфейсів міжмережної взаємодії. Таким чином, доцільно розглянути рішення, які побудовані на принципах Round Robin [4]. Його суть полягає у способі балансування мережного навантаження, при якому запити або потоки даних розподіляються між кількома вузлами (у даному випадку, VPN-серверами) у порядку черги. Відповідно, кожен вузол мережі, який задіяний у функціонуванні VPN-ланцюга, отримує запити від спеціального вузла або підсистеми, яка реалізує даний підхід. Ці запити, незалежно від складності, розподіляються за принципом першого-ліпшого вузла. Наприклад, якщо у комунікаційному середовищі VPN-серверів існує три сервери, а четвертий вузол реалізує функцію Round Robin, то перший запит від користувача, який хоче здійснити передачу даних через цю систему, буде оброблятися першим VPN-сервером, який, у свою чергу, буде мати мінімальний час затримки на передачу даних у віртуальному тунелі між цим користувачем та, власне, VPN-сервером. Час буде визначатися сукупністю часових значень затримки передачі тестового повідомлення між задіяними вузлами (користувач та перший VPN-сервер), часом побудови VPN-тунелю та часом передачі тестового повідомлення у тунелі. Відповідно, процес тестування часових затримок між околом вузлів, які є потенційними першими VPN-серверами та користувачем, може також займати певний час. У такому випадку, вузлом, який реалізує функцію Round Robin, здійснюється вирішення додаткових задач побудови першого VPN-тунелю у ланцюгу. Якщо часові затримки даного етапу перевищують допустимі, то користувач може отримати відмову у обслуговуванні або мати значні часові затримки в обслуговуванні.

Аналогічним чином може бути створений маршрут до другого та інших VPN-серверів, таким чином, будуючи VPN-ланцюг (рис. 2).

Наведений алгоритм не враховує ряд інших аспектів, які мають специфіку та певні особливості мережного середовища, в якому здійснюється реалізація даного підходу. Також відомі інші рішення, які дозволяють встановити значення ваги як для кожного VPN-сервера, так і до їх груп [4].

Відомий приклад адаптивного балансування, який використовує інформацію про поточне навантаження на кожному VPN-сервері для прийняття рішення вибору наступного вузла VPN-ланцюга. Однак, такий підхід передбачає наявність динамічно-змінюваних спеціалізованих баз даних із метаданими про стани таких вузлів. Це вимагає наявності певних

складнощів у забезпеченні окремого рівня безпеки для таких баз даних. Як приклад, хмарний балансувальник NaaS з елементами міксування функціонує за вказаним алгоритмом.

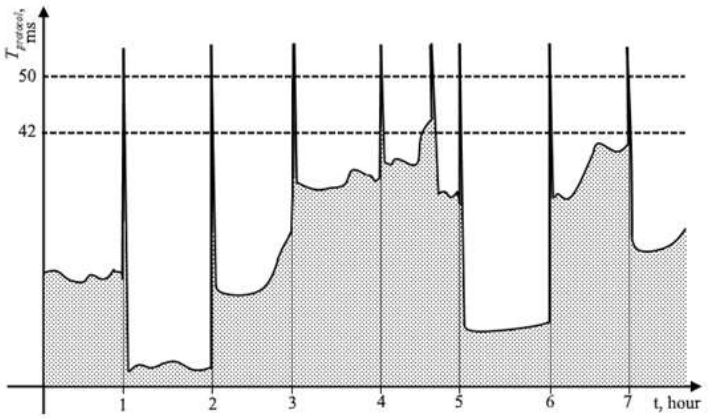


Рисунок 2 – Приклад часових затримок, які виникають при перебудові ланцюга

Окремою задачею, яка найчастіше виникає в оверлейних мережах, є визначення доступності VPN-вузлів перед запуском алгоритму пошуку вузлів при побудові ланцюга [3]. Цю задачу успішно вирішує відомий метод Health Check. Цей метод дозволяє уникати помилок, а також непередбачуваних часових затримок при побудові VPN-ланцюгів.

Інколи, додатковою задачею є побудова матриць пропускних здатностей та інших метрик, які визначають загальний стан пулу VPN-серверів, задіяних при побудові таких ланцюгів. Однак, складність обчислення таких значень напряму залежить від кількості вузлів у такому пулі та динаміки їх завантаженості.

У складних гетерогенних середовищах, де кількість VPN-серверів обчислюється сотнями, час на визначення оптимальних значень часових затримок між вузлом користувача та всіма VPN-вузлами може бути незадовільним. У таких випадках застосовується квазіоптимальні підходи, які дозволяють швидко створювати VPN-ланцюги з можливістю їх швидкої перебудови в залежності від мінливості метрик VPN-серверів мережі. В таких випадках має місце використання методу комівояжера з декількома активними пошукачами точок оптимуму [5].

Також складність задачі балансування навантаження у міксованих VPN-ланцюгах може визначатися кількістю вузлів у ланцюзі. Чим більша кількість, тим більша анонімність користувача, – але при цьому і менша швидкість доставки контенту від вузла, до якого надходить запит, до користувача. Проблема втрати службових даних цього запиту є найбільш критичною, так як у цьому випадку користувач має повторно їх генерувати, що може призвести до розкриття (деанонімізації) вузла користувача. У якості рішення цієї задачі може бути застосований асинхронний режим

обміну даними між користувачем та цільовим вузлом. Сутність цього рішення полягає у тому, що запит від користувача надходить через спрощену схему VPN-ланцюга, але з покращеною криптостійкістю, тоді як прикордонний VPN-сервер, який відповідає за пряме надсилання запиту до цільового вузла, перенаправляє отриману відповідь через повноцінний VPN-ланцюг до користувача [5].

Таким чином, проведений аналіз зазначених рішень дозволяє зробити висновок, про те, що використання міксованих VPN-ланцюгів забезпечує високий рівень анонімності в мережі Інтернет, однак, як і у будь-якій технології віртуалізації, відбувається втрата швидкості, що може бути критичним для передачі, наприклад, нееластичних даних, як-то голосовий, відеоконтент реального часу.

У якості напрямів подальших досліджень необхідно розглянути комбіновані схеми побудови VPN-ланцюгів з урахуванням регіональних особливостей постачальників віртуальних рішень, як-то VDS, VPS тощо.

Список використаних джерел

1. T. Vitalii, B. Anna, H. Kateryna and D. Hrebeniuk, "Method of Building Dynamic Multi-Hop VPN Chains for Ensuring Security of Terminal Access Systems," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2020, pp. 613-618, doi: 10.1109/PICST51311.2020.9467953.

2. V. Tkachov, M. Bondarenko, O. Ulyanov and O. Reznichenko, Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory, 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2019, pp. 161-165. DOI: 10.1109/ATIT49449.2019.9030494

3. Tkachov V. Architecture of overlay network with nested vpn tunneling / M. Hunko, V. Tkachov, M. Bondarenko // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доп. 10-ї міжнар. наук.-техн. конф., 9-10 квітня 2020 р., Баку–Харків–Жиліна : [у 2 т.]. Т. 1 : секції 1, 2 / Військ. акад. збройних сил Азербайджанської Республіки [та ін.]. – Харків : Петров В. В., 2020. – с. 36.

4. Kovalenko Andriy Метод забезпечення живучості комп’ютерної мережі на основі vpn-тунелювання / Andriy Kovalenko, Heorhii Kuchuk, Vitalii Tkachov // Системи управління, навігації та зв’язку. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 1 (63). – С. 90-95. – doi:https://doi.org/10.26906/SUNZ.2021.1.090.

5. Tkachov, Vitalii & Tokariev, Volodymyr & Ilina, Iryna & Partyka, Stanislav. (2021). Modified Traveling Salesman Problem for a Group of Intelligent Mobile Objects and Method for Its Solving. International Journal of Electrical and Electronic Engineering & Telecommunications. 1-7. 10.18178/ijeetc.10.1.1-7.

УДК 004.4’2:004.8

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЗІ ЗБЕРЕЖЕННЯ, ОРГАНІЗАЦІЇ ТА КЕРУВАННЯ ЗАКЛАДКАМИ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Мякшин А.С.
Науковий керівник – д.т.н., проф. Кривуля Г.Ф.
Харківський національний університет радіоелектроніки, каф. АПОТ,
м. Харків, Україна
e-mail: andrii.miakshyn@nure.ua

This work is devoted to the development of software for bookmark management using artificial intelligence. The main goal of the research is the introduction of new functionality based on the analysis of modern products on the market, as well as the use of artificial intelligence to increase interactivity and expand capabilities. The following methods were used to conduct the research: comparative analysis of existing solutions, analysis of user requirements, selection of technologies, implementation and testing of the product. The result of the research was cross-platform software, the functionality of which allows users to create their own working environment for managing bookmarks, as well as actively interact with their content using artificial intelligence capabilities.

Сьогодні користувач інтернету має справу з великим потоком інформації. Браузер є саме тим невід'ємний ресурсом, який виконує роль своєрідного провідника між людиною та цифровою інформацією. Зі збільшенням кількості переглянутих вебсторінок настає потреба в їх збереженні з метою подальшого прочитання. З часом ця потреба була реалізована в вигляді уніфікованого ідентифікатору ресурс (URL), який отримав назву «Закладка».

Слід вказати, що закладки були додані до браузерів у 1992 році (браузер ViolaWWW) та у 1993 році (браузер Mosaic). У наші дні кожен браузер надає вбудований інструмент для керування закладками, але його функції досить обмежені та не забезпечують гнучку взаємодію зі збереженими посиланнями.

Для вирішення цієї проблеми існують спеціальні програми, які надають ширший функціонал і дозволяють використовувати різні можливості для керування збереженими посиланнями та організації. Всі вони мають схожий базовий функціонал, який включає в себе наступні можливості: додання та видалення посилання на сторінку, редагування інформації про закладку, додання нотатки, створення категорій, додання тегів, а також встановлення зображення до закладки, сортування, вибір відображення списку, розділ «Обране», вхід через аккаунт (обліковий запис), зміна теми. Всі програми такого напрямку мають мету, яка полягає у спрощенні роботи користувача та наданні зручного простору для керування закладками. Метою

дослідження є реалізація можливостей, які значно покращать досвід взаємодії між користувачем і програмою, підвищать надійність та актуальність збережених посилань, розширять функціонал, використовуючи штучний інтелект, а також проведення порівняльного аналізу існуючих продуктів на ринку, формування та розробка гнучкої функціональності. Задача дослідження — створення кросплатформного програмного забезпечення для менеджменту закладок з урахуванням функцій і можливостей, які відсутні у програмах такого плану.

На даний момент на ринку існує багато рішень, які надають широкий функціонал для керування закладками. Такі програми, як Raindrop.io (від Rustem Mussabekov), Pocket (від Mozilla Corporation) та Bookmark OS (від David Lynam) мають різноманітний фунціонал, але у цих менеджерах закладок не приділяється багато уваги роботі саме без підключення до мережі інтернет [2]. Бувають ситуації, коли користувач не має доступу до інтернету та через це не може використовувати певний функціонал менеджеру закладок, що обмежує його можливості та негативно впливає на досвід використання продукту. Якщо в програмі були збережені важливі дані, то через відсутність інтернету вони не можуть бути вчасно використані. Слід зазначити, що деякі програми з керування закладками реалізовані у вигляді веб-застосунку, тобто працюють у браузері, а деякі – у вигляді десктопної версії. Залежність від інтернет з’єднання не дозволяє використовувати фунціонал без підключення до мережі, що значно заважає комфортній роботі з закладками. Для вирішення цієї проблеми була реалізована можливість доступу до функціоналу, а саме перегляду збережених посилань та роботи з ними без підключення до інтернету.

Є програми, які надають не тільки функціонал з керування закладками, а й рекомендують матеріал для ознайомлення. Актуальною проблемою є те, що цей контент майже ніяк не пов’язаний з інтересами користувача, що змушує витрачати час на пошук цікавої інформації. За допомогою штучного інтелекту, а саме Open AI API, який надає доступ до різних інструментів та моделей штучного інтелекту, було реалізовано можливість рекомендації контенту (статті, відео) саме на основі того, чим саме цікавиться поточний користувач [3].

Бувають випадки, коли користувач зберіг не дуже коректну адресу з різних причин, але не кожна програма виконує перевірку посилання. Було реалізовано процедуру перевірки під час створення чи редагування посилання, яка дозволяє уникнути збереження некоректної адреси.

Основною мовою розробки є Python. Переносність програм, чистий синтаксис, можливість використання Python в діалоговому режимі, стандартний дистрибутив, який має багато корисних модулів – все це є основним перевагами цієї мови програмування [1]. Під час розробки використовувався мікрофреймворк Flask, так як він є гарним рішенням у

випадку, коли програма, над якою ведеться розробка, спочатку буде не дуже великого розміру, але у перспективі є можливість швидкого розширення [4].

Гнучкість – одна з основних переваг фреймворку. Це важливо, тому що проєкт може бути розвинений у іншому напрямку, а також тому що при певних змінах структура не буде порушена. Бібліотека Tkinter була використана під час створення графічного інтерфейсу та забезпечила широкий набір компонентів [5].

Наукова новизна та актуальність полягає у реалізації можливості працювати в офлайн режимі, що дозволяє використовувати певний фунціонал без необхідності інтернет з'єднання. Завдяки цьому забезпечується постійний зв'язок між користувачем та його даними, які можуть бути оброблені у будь-який момент часу.

Рекомендація схожого контенту, використовуючи штучний інтелект, дозволяє отримати інформацію, яка безпосередньо пов'язана з інтересами користувача. Це формує єдине гнучке інформаційне середовище, яке підлаштовується під саме ті ресурси, які використовує поточний користувач. В свою чергу, перевірка посилань на коректність запобігає збереженню некоректної інформації. Розроблений функціонал підвищує досвід взаємодії, розширює можливості менеджера закладок, а також забезпечує коректність та підвищує надійність збережених даних.

Список використаних джерел

1. Bader D., Amos D., Jablonski J. Python Basics: A Practical Introduction to Python 3. Real Python. Vancouver: Real Python, 2021. 635 p.

2. Найкращі безкоштовні інструменти для створення та управління закладками // IG Internet gate : Новини IT-компаній, бізнесу, електронної комерції. URL: https://igate.com.ua/news/27723-luchshie-besplatnye-instrumenty-dlya-sozdaniya-i-upravleniya-zakladkami (дата звернення: 20.01.2024).

3. OpenAI : вебсайт. URL: https://openai.com/ (дата звернення: 21.01.2024).

4. Grinberg M. Flask Web Development: Developing Web Applications with Python. Sebastopol : O'Reilly Media, 2018. 312 p.

УДК 004.41: 004.92

ІНТЕГРАЦІЯ 3D У ВЕБ-ЗАСТОСУНКАХ

Осипов Д.О.
Науковий керівник – к.т.н., доц. Груздо І. В.
Харківський національний університет радіоелекроніки,
каф. ПІ, Харків, Україна
тел. +38(066) 395-35-57, e-mail: danylo.osypov@nure.ua

The article describes IoT and 3D system for airsoft games aims to enhance analysis by evaluating hit points and strategic moments, transforming the gaming experience. Its versatility extends to civilian and military applications, utilizing physical sensors for player impact data and a web interface for game management, role allocation, team formation, and viewing game history. In summary, the system, designed for various airsoft tasks, enhances entertainment and holds potential applications in civilian and military realms, contributing to training, teamwork, and strategic analysis.

У сучасному світі веб-розробки зростає популярність використання 3D технологій для поліпшення інтерактивності та візуальної привабливості контенту. Ця тенденція розширюється на різні галузі, і однією з областей використання цих технологій є страйкбол. Метою роботи є розробка програмної системи для контролю та аналізу гри у страйкбол, що реалізує головний функціонал та надає можливості ведення, контролю та аналізу гри. Система для контролю та аналізу гри у страйкбол має потенціал не лише змінити сам характер гри, але й надасть можливість гравцям підвищити рівень поглибленності та виконувати більш детальній аналіз. Інноваційність такої системи може привертати нових учасників та глядачів, розширюючи популярність страйкболу та надаючи нові враження.

Завдяки інтегруванню IoT та 3D технологій, система дозволить докладно аналізувати кожен елемент гри – точки влучення, стратегічні моменти тощо. Це відкриває нові можливості для тренування гравців та вивчення їхнього стилю гри.

Перспектива створення системи, яка пропонує страйкбольні ігри з різними задачами, відкриває широкий спектр можливостей для використання у різних сферах, включаючи як цивільні, так і військові аспекти. Важливо визначити, як ця система може вносити вагому користь в різних сферах діяльності, сприяючи інноваціям та ефективній практиці.

Система може служити ідеальним інструментом для тренування та розвитку фізичних та стратегічних навичок в різноманітних сценаріях. Гравці можуть вдосконалювати свою точність стрільби, підвищувати швидкість реакції та розвивати координацію як особисту так і командну.

У цивільному використанні, система може стати ідеальним інструментом для тренування та розвитку командної співпраці в різноманітних сценаріях. Система може бути цікава не лише професійним

спортсменам, але й людям, що бажають гарно провести час – проведення корпоративів, святкування днів народжень чи просто гарно сплановані вихідні.

З іншого боку, військові застосування такої системи можуть бути вирішальними для підготовки військових підрозділів та команд до різних бойових сценаріїв. Ігри можуть моделювати тактичні стратегії, взаємодію військових підрозділів або вдосконалення навичок солдат у міському, закритому або відкритому бойових середовищах. Система може слугувати інструментом для аналізу стратегічних даних та покращення підготовки військового персоналу. Відслідковуючи точки влучання, недосвідченим солдатам буде легше зрозуміти, які помилки вони допускають та надасть можливість досконально відточити власні навички.

Пропонується розробка системи, яка складатиметься з IoT та веб-частин. Фізична частина буде реалізована у вигляді набору датчиків, які фіксують удари різної сили на тілі гравця та передають дані по завершенню гри. Від кількості датчиків залежить точність даних, тому поєднання різних типів датчиків, таких як датчиків удару, гнучкості та вібрації поліпшить систему.

В ході дослідження, було розроблено програмну систему для контролю та аналізу гри у страйкбол. Створена програмна система підтримує багатомовність, дозволяє адміністратору створювати резервні копії, фільтрувати, сортувати та керувати акаунтами користувачів та записами усіх матчів. З боку користувачів система дає можливість керувати обліковими записами, створювати нові і переглядати старі матчі. Система дозволяє гравцям оглядати 3D модель, на якій зображені місця та кількість влучень, отриманих протягом усього матчу. Веб-частина слугує для створення та ведення гри з вибором задачі, формуванням мапи та розподіленням гравців по ролям, запрошення інших учасників, формування команд та перегляду історії усіх ігор. Створена система може дуже допомогти в підвищенні рівня тренування, розвитку командної роботи, а також в області аналізу та вдосконалення стратегій.

Список літератури:

1. DANCHILLA, Brian; DANCHILLA, Brian. Three. js framework. *Beginning WebGL for HTML5*, 2012, 173-203.

2. VIEIRA, Martim, et al. IoT Based Targeting System-Airsoft Use-Case. In: *2022 International Young Engineers Forum (YEF-ECE)*. IEEE, 2022. p. 1-6.

3. Protsenko, I. Y., & Onykienko, Y. O. (2020). Застосування 3D-графіки в мережних технологіях для вирішення практичних завдань. Електронна та Акустична Інженерія, 3(4), 23–27. URL: https://doi.org/10.20535/2617-0965.2020.3.4.199044 (дата звернення: 05.01.2024).

УДК 004.72.057.4

ПОРІВНЯЛЬНИЙ АНАЛІЗ ФУНКЦІОНАЛЬНОСТІ ТА БЕЗПЕКИ ПРОТОКОЛІВ СІМЕЙСТВА FHRP

Піглюк І.М.
Харківській національний університет радіоелектроніки
61000, Харків, просп. Науки,14, каф. ІКІ ім. В.В. Поповського
тел. (095)867-15-92, e-mail: ihor.pihliuk@nure.ua

This article provides a comparative analysis of the First Hop Redundancy Protocols (FHRP) Aimed at enhancing network reliability and service continuity, the research evaluates each protocol's strengths and weaknesses. However, it is important to understand the specifics of each protocol and consider the specific needs of the network when selecting and configuring them.

У сфері розробки та підтримки високодоступних комп'ютерних мереж особливу увагу приділяється механізмам забезпечення безперебійної роботи мережевих сервісів. В цьому контексті велике значення мають протоколи першого кроку резервування (FHRP), які дозволяють мінімізувати простої внаслідок відмов маршрутизаторів, автоматично переключаючи трафік на резервні пристрої. Серед найбільш розповсюджених протоколів FHRP слід виділити HSRP, розроблений компанією Cisco, VRRP — відкритий стандарт, та GLBP — також продукт Cisco, кожен з яких має свої особливості, переваги та недоліки.

HSRP (Hot Standby Router Protocol) забезпечує високу доступність шляхом визначення активного та резервного маршрутизатора, між якими можливе автоматичне переключення у випадку збою. Попри свою простоту та зручність у використанні, HSRP має обмежений набір функцій та не підтримує шифрування даних, що ставить під загрозу безпеку даних які передаються. Крім того, HSRP вразливий до атак типу ARP spoofing, що може призвести до перехоплення трафіку атакуючим.

На відміну від HSRP, VRRP (Virtual Router Redundancy Protocol) є відкритим протоколом, що забезпечує більшу гнучкість та сумісність з обладнанням різних виробників. Однією з ключових переваг VRRP є підтримка механізмів аутентифікації, що покращує загальний рівень безпеки мережі. Проте, незважаючи на це, VRRP, подібно до HSRP, не забезпечує високого рівня безпеки через відсутність шифрування обміну інформацією між маршрутизаторами.

GLBP (Gateway Load Balancing Protocol) вирізняється на фоні HSRP та VRRP завдяки можливості балансування навантаження, що дозволяє не тільки забезпечити високу доступність, але й оптимізувати використання мережевих ресурсів. Протокол дозволяє динамічно розподіляти трафік між кількома активними маршрутизаторами, забезпечуючи ефективне використання кожного з них. Однак, як і інші пропріетарні рішення Cisco,

GLBP характеризується підвищеною складністю управління, що може стати перешкодою для його впровадження в деяких мережевих інфраструктурах.

При виборі між HSRP, VRRP та GLBP необхідно враховувати специфічні потреби мережі, зокрема вимоги до доступності, безпеки, сумісності з обладнанням та можливості балансування навантаження. HSRP може бути оптимальним рішенням для простих мереж, де основним завданням є забезпечення високої доступності без необхідності балансування навантаження. VRRP пропонує більшу гнучкість та сумісність, що робить його підходящим для використання в гетерогенних мережах. GLBP, у свою чергу, є найкращим вибором для складних мережевих середовищ з високими вимогами до ефективності використання ресурсів та балансування навантаження.

Враховуючи вищезазначене, можна зробити висновок, що кожен з розглянутих протоколів FHRP має своє місце в екосистемі мережевих технологій, пропонуючи інженерам різні інструменти для забезпечення надійності та доступності мережевих сервісів. Однак, важливо розуміти особливості кожного протоколу та враховувати конкретні потреби мережі при їх виборі та налаштуванні.

Список використаних джерел:

1. Configuring HSRP, VRRP, and GLBP. URL: https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/www.cisco.com/content/dam/en/us/td/docs/switches/metro/me3400e/software/release/12-2_58_ez/configuration/guide/swhsrp.fm/jcr:content/renditions/Book_ME3400e_swhsrp.html.xml (Дата звернення 29.02.2024).

2. Лемешко О. В. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість : монографія / О. В. Лемешко, О. С. Єременко, О. С. Невзорова – Харків : ХНУРЕ, 2020. – 308 с. – ISBN 978-966-659-282-1.

3. Cisco® CCNA Exam Cram Notes : FHRP. URL: https://www.examguides.com/CCNA/cisco-ccna-64.htm (Дата звернення 29.02.2024).

4. Virtual router redundancy protocol. URL: https://docs.netscaler.com/en-us/citrix-sd-wan-orchestrator-on-premises/site-level-configuration/virtual-router-redundancy-protocol.html (Дата звернення 29.02.2024).

УДК 004.65:004.032.2 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.045

ОСОБЛИВОСТІ ВИКОРИСТАННЯ APACHE KAFKA У РОЗПОДІЛЕНИХ СИСТЕМАХ РЕАЛЬНОГО ЧАСУ

Погорєлова Л.А.
Науковий керівник – к.т.н., доц. каф. КІТС, доц. Сердюк Н.М.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. КІТС, тел.: (057)702-02-45)
e-mail: liliia.pohorielova@nure.ua

The article provides a detailed description of distributed systems for real-time data analysis and processing. In the modern world, where speed, accuracy, and timeliness of information are becoming key success factors, understanding, and using Big Data and data processing is extremely important. To achieve this goal, it is necessary to use appropriate tools and modern approaches that allow efficient processing, analysis, and use of data. Apache Kafka is one of such tools. It supplies useful methods of communication between producers and consumers. The basic principles of the message broker architecture were considered.

У сучасному світі кількість даних, що генеруються та накопичуються, зростає експоненційно. Великі обсяги даних (Big Data) стали нормою, а їх аналіз та обробка в реальному часі стає все більш важливою задачею для багатьох сфер діяльності. Високоефективні системи, що побудовані з використанням брокерів повідомлень, стають ключовим інструментом для вирішення цієї задачі.

На основі таких систем створюються сучасні потокові веб-додатки, головне призначення яких полягає в аналізі даних з різних джерел по мірі їх надходження. Такі програми дозволяють компаніям та організаціям швидко отримувати актуальну інформацію, реагувати на зміни в реальному часі та впроваджувати розумні аналітичні підходи для побудови стратегічно вигідніх рішень. Прикладами таких додатків є системи моніторингу та пропонування рекомендацій, фінансові системи, системи аналізу соціальних мереж, системи прогнозування та багато інших.

На сьогоднішній день існує велика кількість інструментів для обробки великих обсягів даних, серед яких до найпопулярніших належать: Apache Spark та Apache Hadoop. Перед безпосереднім аналізом інформації постає проблема доставки даних. Саме це завдання вирішується багатопотоковою платформою Apache Kafka. Це розподілена система передачі повідомлень з високою пропускною здатністю та низькими затримками. Вона здатна обробляти великі обсяги потокових даних з використанням структурованої архітектури журналів. Kafka надає надійну передачу повідомлень, розділення потоку даних на теми та можливість горизонтального масштабування.

Основу архітектури складає Kafka Cluster, що вміщує у собі набір брокерів, тем та розділів [1]. На рисунку 1 схематично представлено взаємозв'язок усіх компонентів.

Брокери (brokers) утворюють основну складову системи. Кожен брокер є незалежним сервером, який відповідає за зберігання та обробку повідомлень. Саме ці сутності отримують повідомлення від видавців (продюсерів) і відправляють їх підписникам (споживачам). Kafka Cluster може містити кілька брокерів, що дозволяє розподілити навантаження та забезпечити відмовостійкість.

Теми (topics) є категоріями або каналами, до яких видавці публікують повідомлення та на які підписуються споживачі. Вони представляють собою логічне розділення даних або потоків повідомлень. Кожна тема може мати декілька розділів, які розподіляють дані всередині теми між брокерами. Теми можуть бути реплікованими, що дозволяє зберігати копії даних на різних брокерах для забезпечення надійності та доступності.

Розділи (partitions) є фізичними одиницями зберігання даних в межах тем. Вони дозволяють розподіляти дані між брокерами та обробляти їх паралельно. Кожен розділ може мати свій власний набір повідомлень, які зберігаються у впорядкованому логу. Підписники можуть споживати повідомлення з різних розділів відповідно до своїх потреб.

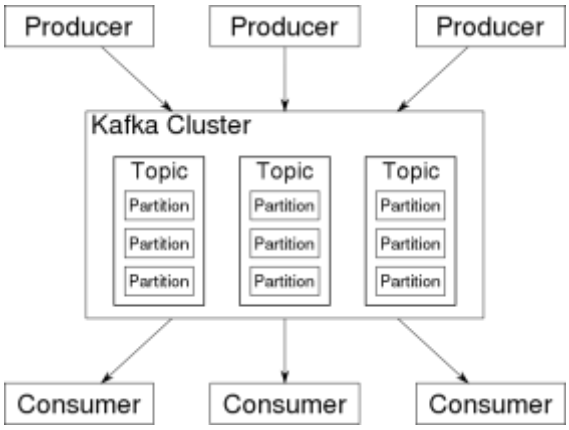


Рисунок 1 – Архітектура Apache Kafka

Прикладом реальної системи з використанням Apache Kafka може стати платформа моніторингу стану здоров'я пацієнтів [2]. Дана система направлена на аналіз та обробку великих і різнорідних даних, зібраних біомедичними датчиками задля полегшення процесів класифікації та діагностування захворювань медичним персоналом. Запропонована платформа складається з чотирьох рівнів: моніторинг пацієнтів у реальному часі, прийняття рішень і зберігання даних у реальному часі, класифікація пацієнтів і діагностика захворювань, а також пошук і візуалізація даних.

На першому етапі відбувається збір даних з різних джерел та їх потокова обробка. Дані з активних біосенсорів, які дозволяють безперервно контролювати стан пацієнтів, надсилаються в режимі реального часу до

сховища даних за допомогою системи обміну повідомленнями Apache Kafka.

Другий етап передбачає використання Spark і Hadoop HDFS (розподілена файлова система Hadoop) для аналізу та зберігання даних відповідно. Після встановлення на головному вузлі кластера Spark отримує дані, що надходять від Kafka, і застосовує алгоритми виявлення надзвичайних ситуацій та пошуку відсутніх записів перед відправкою остаточних даних до HDFS для зберігання.

На третьому етапі здійснюється класифікація пацієнтів і діагностика захворювання з використанням пакетної обробки та пошуком кореляції після збереження даних. Останній етап присвячений отриманню та візуалізації оброблених даних за допомогою модулю SparkSQL.

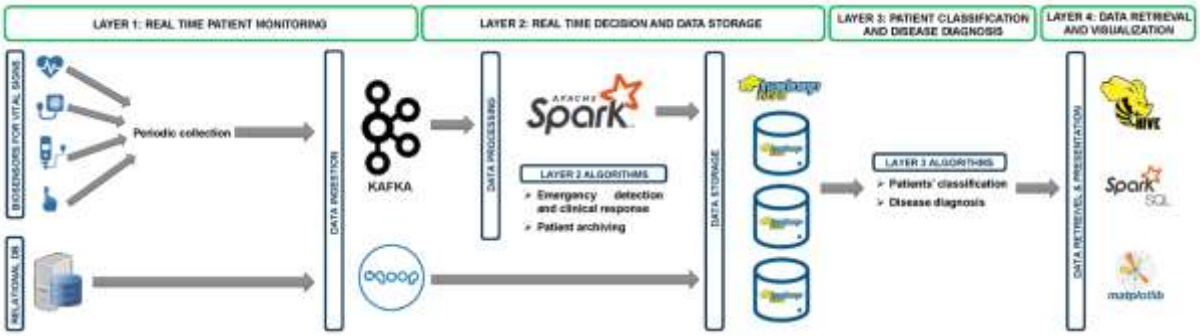


Рисунок 2 – Приклад архітектури системи обробки Big Data

Таким чином, Apache Kafka відіграє першочергову роль системах обробки великих даних, забезпечуючи надійний та ефективний потік даних в реальному часі. Архітектура розглянутого брокеру повідомлень забезпечує зручну інтеграцію з іншими компонентами екосистеми Hadoop, такими як Spark і HDFS, що дозволяє легко обробляти, зберігати і аналізувати великі обсяги даних в розподіленому середовищі.

Список використаних джерел

1. Levy E. Kafka vs. RabbitMQ: Architecture, Performance & Use Cases Blog Upsolver, 2019. URL: https://www.upsolver.com/blog/kafka-versus-rabbitmq-architecture-performance-use-case (дата звернення 03.03.2024).

2. Harb H., Mroue H., Mansour A. Hadoop-Based Platform for Patient Classification and Disease Diagnosis in Healthcare Applications, 2020. URL: https://www.mdpi.com/1424-8220/20/7/1931 (дата звернення 03.03.2024).

УДК 004.75 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.048

ВИКОРИСТАННЯ CLOUD-ТЕХНОЛОГІЙ ДЛЯ УПРАВЛІННЯ ТА МОНІТОРИНГУ В СИСТЕМАХ «РОЗУМНОГО БУДИНКУ»

Потопа В.О.
Науковий керівник– к.т.н, доц. Ларченко Л.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. АПОТ, тел. (057) 702-13-26)
e-mail: lina.larchenko@nure.ua

Home automation and the Internet of Things are important fields of research , Cloud computing will provide easy access to home automation for the general public by providing easy to use online services. Open and standardised protocols for home automation devices further increase the convenience by offering more choice and freedom to the customer.

В даний час набувають подальшої популярності системи «розумного будинку», що забезпечують комфорт, безпеку та ресурсозбереження. Такі технології знаходять застосування в багатьох сферах нашого життя, включаючи побут. Бажання людини отримати додатковий рівень комфорту, підвищити рівень безпеки та встановити контроль використання ресурсів є основними причинами для продовження розвитку такого роду технологій. Сучасні технології систем «розумного будинку» дозволяють інтегрувати підсистеми різного призначення, забезпечуючи їх злагоджену роботу та високу функціональність в цілому і дозволяють споживачеві задавати комфортні для себе умови у середовищі [1]. Складовою систем «розумного будинку» є системи безпеки, що потребують постійного розвитку та удосконалення [2].

Метою дослідження є оцінка ролі хмарних технологій у забезпеченні безпеки та ефективного управління складовими системи «розумного будинку».

Завданням роботи є дослідження впливу та ефективності використання хмарних сервісів для здійснення управління та контролю житлової інфраструктури системи «розумного будинку» для забезпечення комфортного життя, підвищення безпеки житла та оптимізації використання ресурсів. Крім того, завданням є можливість забезпечення легкого доступу до домашньої автоматизації, надаючи прості у використанні онлайн-сервіси, підвищення зручності домашньої автоматизації шляхом використання відкритих та стандартизованих протоколів. При цьому розглянуто інформацію про переваги та недоліки хмарних сервісів у контексті управління та безпеки будинком, а також рекомендації щодо раціонального використання даних технологій при розробці систем «розумного будинку».[1]

За останні роки системи «розумного будинку» досягли безпрецедентного успіху і на даний час здійснюється подальше їх удосконалення. Основною ідеєю роботи є розробка системи домашньої

автоматизації, в якій забезпечено підключення всіх пристроїв через інтернет сервер та здійснюється безпосереднє обслуговування всього домашнього обладнання, яке одночасно направлено на безпеку системи.

Найчастіше керування в системах «розумного будинку», які грунтуються на основі IoT та Cloud технологій, відбувається віддалено за допомогою додатку для смартфона або ж розробники самі пропонують власні девайси для керування. Показники приладів та інша необхідна інформація зберігаються на сервері, що дає можливість до розробки великої кількості способів управління системою на різних платформах.

Досліджуваною системою «розумного будинку» з використанням cloud-технологій можна керувати та бачити поточні дані, що надходять від датчиків з будь-якої точки світу. Наявність потужних процесорів полегшує реалізацію набагато складніших процесорів систем «розумного будинку», що виконують необхідні функції. Для того, щоб надавати означені послуги, усі системи «розумного будинку» будуються за базовою структурою, що містить компоненти: керуючий пристрій, датчики, виконавчі пристрої, інтерфейс користувача, хмарна інфраструктура, мережеве з'єднання.[2]

Досліджувана система «розумного будинку» здійснює функції, що наведені нижче.

1. Збір інформації за допомогою датчиків, камер, мікрофонів та інших побутових пристроїв.

2. Зберігання та обробка зібраної інформації за допомогою основного процесора.

3. Генерація результатів і надання послуг в залежності від обробленої інформації.

Названі функції можуть бути реалізовані за допомогою мікроконтролерних систем. Мікроконтролери, які представляють собою однокристальні мікрокомп'ютери, виконані у вигляді мікросхеми, є компактними і одночасно функціональними пристроями. Існує велика кількість мікроконтролерів, що здатні забезпечувати функціонування названих систем, як NodeMCU, Arduino UNO, MSP430, STM32VL-Discovery, що є функціональними мікроконтролерами.

У даній роботі проведено огляд використання хмарних технологій розумного будинку, розглянуто основні функції системи розумного будинку, зокрема збір, зберігання та обробка інформації, що отримана з датчиків на компонентів системи. Запропонована хмара відповідає основним вимогам розумного «розумного будинку». Сервери для кожного з додатків «розумного будинку» працюють у хмарному середовищі, а отже заощаджують енергію та забезпечують більш екологічне рішення.

Список використаних джерел:

1. Iouliia Skliarova. Smart Home System: A Comprehensive Review.– 2023.–C. 8-15.

2. Pavithra, D., & Balakrishnan, R. (2015, April). IoT based monitoring and control system for home automation. In 2015 global conference on communication technologies (GCCT)(pp. 169-173). IEEE.

УДК 004.4 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.050

ДОСЛІДЖЕННЯ ПРОЦЕСУ МІГРАЦІЇ ВІРТУАЛЬНОЇ МАШИНИ

Радченко В.О., Міхаль О.П.
Харківський національний університет радіоелектроніки, Харків, Україна
Email: viacheslav.radchenko@nure.ua, тел. 0662433413

Abstract. The study is devoted to the process of migration. Namely, the transfer of a virtualized guest system from one node to another. Migration has been proven to be a key aspect of virtualization, as software is hardware independent at this level. Migration can be performed in offline or connected mode. In the process of migration, the memory of the guest system is transferred to the target node; while the guest's file system will be stored in the shared storage. There are two types of migration without stopping the virtual machine and with stopping the virtual machine.

Під міграцією розуміється процес перенесення віртуалізованої гостьової системи з одного вузла в інший. Міграція є основним аспектом віртуалізації, оскільки на цьому рівні програмне забезпечення не залежить від обладнання. Основне призначення міграції:

– балансування навантаження – гостей можна перемістити на хости з меншим використанням, коли хост стає перевантаженим.

– відмова апаратного забезпечення – коли апаратні пристрої на хості починають виходити з ладу, гостей можна безпечно перемістити, щоб хост можна було вимкнути та відремонтувати.

– енергозбереження – гості можуть бути перерозподілені на інші хости та хост-системи вимкнуті для економії енергії та скорочення витрат у періоди низького використання.

– географічна міграція – гостей можна перемістити в інше місце для меншої затримки або за серйозних обставин.

Міграція може бути виконана в автономному або підключеному режимі (так звана «жива» міграція). У процесі міграції пам'ять гостьової системи передається цільової вузол; при цьому файлова система гостя буде збережена в загальному сховищі (вона не передаватиметься цільовому вузлу через мережу) [1, 2].

Тривалість автономної міграції залежить від смуги пропускання та затримки мережі. Жива міграція характеризується тим, робота віртуальних машин не зупиняється при переносі. Усі сторінки пам'яті, що змінюються за цей час, відстежуються і передаються цільовому вузлу після завершення передачі образу. Процес триває доти, доки не будуть скопійовані всі сторінки або поки не закінчиться заданий гіпервізором KVM період часу.

Якщо сторінки джерела змінюються дуже швидко, то робота гостя на вихідному вузлі буде припинена і буде виконано передачу регістрів та буферів. Регістри будуть завантажені на новому вузлі та гість відновить роботу на цільовому вузлі. Якщо синхронізація неможлива, що ймовірно у разі великого навантаження, то віртуальна машина буде призупинена для міграції в автономному режимі [3].

Тривалість такої міграції залежить від смуги пропускання, затримки мережі та активності гостьової системи. Навантаження на процесор і великі обсяги операцій виводу-введення-виводу також можуть позначитися на тривалості процесу.

Існує два типи міграції:

– без зупинки ВМ (жива міграція) – ВМ залишається доступною під час міграції;

– зі зупинкою ВМ – ВМ недоступна під час міграції.

При міграції віртуальної машини з локальним сховищем копіюється пам'ять та копіюється диск. Формати сховища-джерела та сховища-приймача повинні збігатися (RAW або Qcow2) [4].

При міграції віртуальної машини з мережевим сховищем копіюється лише пам'ять, а диск підключається до вузла кластера, який здійснюється міграція. Віртуальна машина з мережним диском при звичайній міграції або міграції зі статусом "зупинена" переноситься, як правило, за кілька хвилин.

Міграція не може бути виконана, якщо:

– вихідний вузол та вузол призначення використовують різні типи віртуалізації. Наприклад, вихідний вузол знаходиться в кластері KVM, а вузол призначення - в кластері LXD;

– у вихідного кластера тип мережевих налаштувань "Маршрутизація";

– на ВМ з моделлю додавання IP-адрес "Windows" не встановлено QEMU Guest Agent;

– ВМ використовує віртуальну мережу Route Reflector, якої немає у кластері призначення;

– якщо у початковому кластері або кластері призначення настроєна відмовостійкість;

– на ВМ створено віртуальну мережу Full Mesh;

– у кластерів різні типи налаштувань мережі [5].

В ході виконання дослідження було проведено огляд технологій віртуальних машин які використовуються на даний момент та їх аналіз, було виявлено їх основні недоліки та переваги застосування в даній проблемі.

У подальших дослідженнях планується моделювання процесу міграції віртуальних машин за допомогою модифікованого мурашиного алгоритму.

Список використаних джерел

1. Kovalenko A., Kuchuk H., Radchenko V., Poroshenko A. Predicting of Data Center cluster traffic // Proceedings of the 7th International Scientific-Practical Conference on Problems of Infocommunications, 2020. – С. 437-441, DOI: https://doi.org/10.1109/PICST51311.2020.9468006

2. Korkhov V. Flexible Configuration of Application-Centric Virtualized Computing Infrastructure // Computational Science and Its Applications – ICCSA, 2015. — С. 342-353.

3. Bulent A. Dhabaleswar K. A case for high performance computing with virtual machines // Proc. of the 20th annual Int. conf. On Supercomputing (ICS), 2016. — С. 189-207.

4. Tuan L. A survey of live Virtual Machine migration techniques // Computer Science Review, Volume 38, 2020, – С. 334-346, DOI: https://doi.org/10.1016/j.cosrev.2020.100304

5. Hummaida R., Norman W., Rizos S. A hierarchical decentralized architecture to enable adaptive scalable virtual machine migration // Concurrency and Computation: Practice and Experience 35.2, 2023. – С. 202-223, DOI: https://doi.org/10.1002/cpe.7487

УДК004.65.001.63 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.053

РЕПЛІКАЦІЯ ДАНИХ У РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Радченко О.П., Ахмедзянова О.А.
Харківський радіотехнічний фаховий коледж
Харківський комп'ютерний фаховий коледж
м. Харків, Україна
e-mail: elenaradchenko0510@gmail.com

This article is dedicated to the methods of designing and supporting databases in distributed information systems. One of the most common methods of data management in distributed systems is data replication. The article describes and discusses replication schemes, their drawbacks and advantages, as well as strategies for placing replicas in distributed systems.

Проєктування баз даних для проектів з розподіленням даних є важливим і критичним фактором розробки.

Як ключові проблеми можуть при цьому виникнути – вузли з даними можуть розміщуватися в різних географічних регіонах і в певні моменти часу може бути відмінності між станами цих даних, при цьому немає центрального органу керування, що ускладнює процес підтримки узгодженості даних; складність горизонтального масштабування вузлів баз даних.

Для зменшення цих проблем для розробників доступні певні шаблони керування. Найпоширеніші з цих шаблонів: database-per-service pattern; shared database pattern; command query responsibility segregation (CQRS) pattern; saga pattern; sharding; replication [1].

Наразі більш детально розглянемо реплікацію, як один з найпоширеніших методів керування даних в розподілених системах.

Реплікація даних – це процес створення кількох копій даних і їх зберігання в різних місцях. При цьому копії даних можна зберігати в одній системі, на локальних і зовнішніх хостах, а також на хмарних хостах.

Сучасні додатки використовують розподілену базу даних у серверній частині, де дані зберігаються та обробляються за допомогою кластера систем замість того, щоб покладатися на одну конкретну систему.

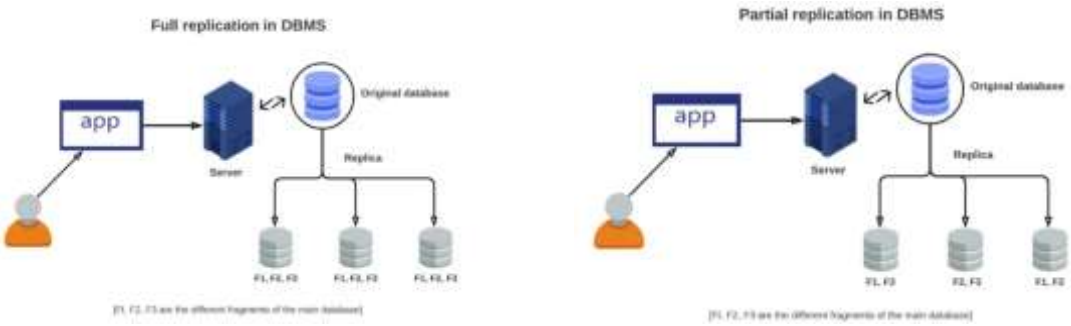
Якщо, наприклад, користувач програми бажає записати частину даних до бази даних, то ці дані будуть розділятися на певні фрагменти і при цьому кожен з цих фрагментів може зберігатися на різних вузлах розподіленої системи. Технологія бази даних також відповідає за збір і консолідацію різних фрагментів, коли користувач хоче отримати або прочитати дані.

Тиражування даних у СУБД (серверах розподілу) може здійснюватися за допомогою відповідної схеми реплікації [2].

– Повна реплікація – на кожному вузлі розподіленої системи реплікується повна база даних (рисунок 1а). У глобальній мережі дана

техніка забезпечує максимальну доступність і надмірність даних, прискорює виконання глобальних запитів. Недоліком повної реплікації є те, що процес оновлення часто відбувається повільно. Це ускладнює підтримку поточних копій даних у всіх місцях.

– Часткова реплікація – на певних вузлах реплікуються тільки певні фрагменти бази даних, які важливі для користувачів даного вузла. ні фрагменти бази даних на основі важливості даних у кожному місці (рисунок 1б). Кількість копій залежить від загальної кількості вузлів, інколи для деяких фрагментів може бути і одна копія.



а) повна реплікація б) часткова реплікація

Рисунок 1 – Схема реплікації

– Без реплікації – на кожному вузлі розміщено лише один фрагмент бази даних, і при цьому він не реплікується на інших вузлах. Перевагою такої схеми є простота відновлення (узгодження) даних, але при цьому може зменшуватися швидкість виконання запитів, оскільки кілька користувачів отримують доступ до одного сервера.

Використання реплікації має як свої переваги та і недоліки. Серед головних переваг: підвищена доступність, продуктивність, безперервність бізнесу, можливість аналітики даних без шкоди для продуктивності системи. До недоліків можна віднести: необхідність синхронізації даних на різних вузлах, витрати на обслуговування та можливе зниження продуктивності при одночасному оновленні багатьох копій [3].

Для покращення ефективності реплікації даних в останні роки достатньо багато уваги приділяють стратегіям розміщення реплік у розподілених системах.

Було запропонував динамічну стратегію розміщення даних для нових реплік, щоб знайти найкраще місце відповідно до їх термінованості. Цей метод може коригувати репліки даних, що зберігаються на кожному вузлі в гетерогенному кластері Hadoop, а також може динамічно скорочувати час відповіді додатків для великих даних [4].

Також використовують метод управління динамічною реплікацією на основі витрат, який називається CDRM. Даний метод розміщує репліки з

урахуванням ємності та ймовірності блокування граничних вузлів. Але це не охоплює погляд на обсяг даних.

Ще один з методів використовує децентралізований алгоритм розміщення копій (D-ReP) для периферійних обчислень. D-ReP базується на величині та місці попиту користувачів і ціні зберігання, щоб зменшити затримку доступу до даних. Це забезпечує найкраще покращення затримки зусиль і зниження витрат, але це не стосується завантаження крайових вузлів і гарантій продуктивності в реальному часі.

Наступний метод – динамічна та децентралізована стратегії розміщення реплік (DDRP), яка також оптимізована для багатьох цілей. Даний алгоритм може приймати рішення набагато швидше, ніж централізований, оскільки йому не потрібно виконувати складні обчислення, щоб отримати глобальне оптимальне рішення.

Таким чином, при проектуванні розподіленої системи даних необхідно враховувати початкові умови - кількість вузлів, їх географічне розміщення, необхідність тієї чи іншої інформації на різних вузлах. І вже в залежності від цих даних використовувати одну з моделей реплікації.

Список використаних джерел:

1. Designing Databases for Distributed Systems: Data Management Patterns for Microservices and Cloud-Native Applications. URL: https://dzone.com/articles/designing-databases-for-distributed-systems

2. Data Replication in Distributed Systems: The Best Guide. URL: https://hevodata.com/learn/data-replication-in-distributed-system/#intro

3. Методи масштабування реляційних баз даних: переваги, недоліки та кейси використання. URL: https://dou.ua/forums/topic/45890/

4. A dynamic decentralized strategy of replica placement on edge computing. URL:
https://journals.sagepub.com/doi/full/10.1177/15501329221115064

УДК 004.89:004.93 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.056

ОЦІНКА ЕФЕКТИВНОСТІ НЕЙРОМЕРЕЖЕВОЇ СИСТЕМИ ДЛЯ КАТЕГОРИЗАЦІЇ ТЕКСТОВИХ ДОКУМЕНТІВ

Рибалов О.О.
Науковий керівник – д.т.н. проф. Фесенко Т.Г.
Харківський національний університет радіоелектроніки, каф. ЕОМ,
м. Харків, Україна
тел +38(067) 451-10-97, oleksandr.rybalov@nure.ua

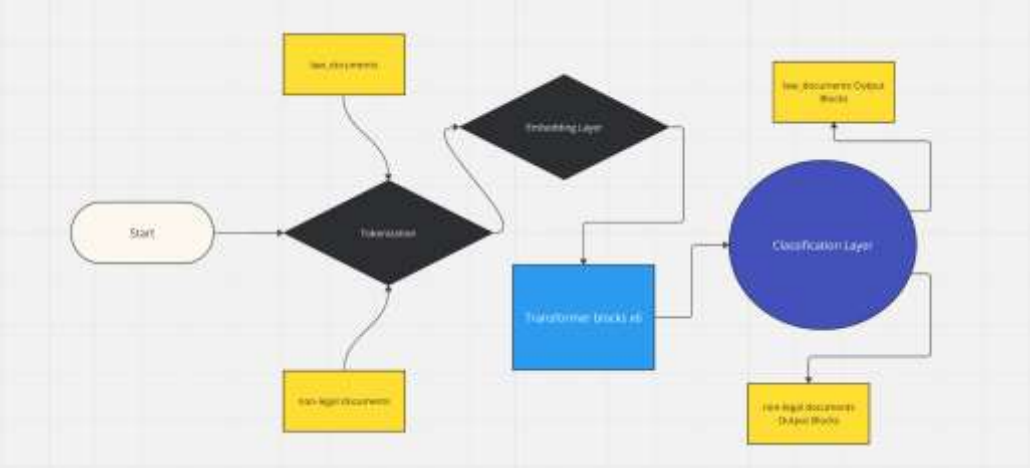
This paper presents an evaluation of the DistilBERT model's effectiveness for categorizing Ukrainian text documents. DistilBERT, a streamlined version of BERT, aims to retain the original's performance with reduced size and increased speed. This study focuses on the model's application for classifying texts into legal and non-legal categories using publicly available data, including court decisions and social media posts. The training encompassed several epochs, enhancing the model's adaptation to data peculiarities. The results, including high accuracy and precision metrics, affirm DistilBERT's efficacy in this context. This research highlights the potential of neural network systems for automating the processing and categorization of Ukrainian texts in various fields.

Відомо, що Natural Language Processing (NLP) – галузь комп'ютерних наук та штучного інтелекту, що займається розробкою методів та технологій для взаємодії між комп'ютерами та людьми через природну мову. Для обробки та категоризації природної мови використовується велика кількість різних моделей. Зокрема, командою вчених у Google запропонована модель Bidirectional Encoder Representations from Transformers (BERT). Для вирішення задач зменшення обсягу пам'яті та ресурсів розроблена скорочена версія моделі BERT – «DistilBERT» [2].

Застосування моделі «DistilBERT» дозволило розробити нейромережеву систему категоризації текстових документів українською мовою на «юридичні» та «неюридичні» (малюнок №1) [2]. Тренування і валідація системи відбувалось із використанням текстів судових рішень, розміщених на платформі Єдиного державного реєстру судових рішень (https://reyestr.court.gov.ua/).

Ефективність нейромережевої системи категоризації текстових документів оцінюється параметрами:

1) Eval loss – середня втрата (або помилка) моделі на тестових даних. Чим нижче цей показник, тим краще модель впоралася із завданням;
2) Eval accuracy – точність моделі, відсоток правильно класифікованих прикладів серед усіх тестових прикладів;
3) F1 Score – гармонічне середнє між точністю (precision) та відтворенням (recall). F1-оцінка, наближена до 0.99 вказує на високий рівень балансу між точністю та відтворенням;



Малюнок №1 – Загальна схема нейромережевої системи для категоризації текстових документів

4) Precision – відсоток правильних позитивних передбачень відносно усіх позитивних передбачень, які зробила модель.
5) Recall – відсоток правильних позитивних передбачень відносно усіх позитивних прикладів у тестовому наборі.

Аналіз продуктивності нейромережевої системи для категоризації на прикладі судових рішень дозволило отримати наступні оцінки параметрів: Eval loss – 0,004677; Eval accuracy – 0,998749; F1 Score – 0,997504; Precision – 0,995020; Recall – 1,000000. Отримані результати демонструють високий рівень точності класифікації документів та підтверджує доцільність застосування моделі DistilBERT. Подальші дослідження ефективності використання нейромережевих систем для категоризації текстів будуть пов’язані з роботою документів з іншої галузі (наприклад, з висновками про результати акредитаційної експертизи освітньої програми [3]).

Список використаних джерел:

1. Sanh V., Debut L., Chaumond J. & Wolf T. (2020). DistilBERT, a distilled version of BERT: smaller, faster, cheaper and lighter. *Cornell Universiti*. doi: https://doi.org/10.48550/arXiv.1910.01108.

2. Рибалов О.О. & Фесенко Т.Г. (2023). Дослідження засобів інтелектуального аналізу текстових документів. Збірник наукових праць XVI Міжнародної науково-практичної конференції «Академічна й університетська наука: результати та перспективи», 12–13 грудня 2023 року. Полтава: Полтавська політехніка, 330–331.

3. Fesenko T., Ruban I., Karpenko K., Fesenko G., Kovalenko A., Yakunin A. & Fesenko H. (2022). Improving of the decision-making model in the processes of external quality assurance of higher education. Eastern-European Journal of Enterprise Technologies. Vol.1(3(115)), 74–85. doi: https://doi.org/10.15587/1729-4061.2022.253351.

УДК: 004.7.032.2 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.058

РОЗУМНИЙ ОРГАНАЙЗЕР ЛІКІВ З ФУНКЦІЄЮ НАГАДУВАННЯ

Савченко Є.Ю.
Науковий керівник – к.т.н., доцент Рахліс Д.Ю.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. АПОТ, тел. (057) 702 1326
e-mail: yelyzaveta.savchenko@nure.ua

The multifactorial problem of reducing patient adherence to treatment was considered in the work. It has been established that one of the negative factors associated with the patient himself is non-compliance with medication. This can lead to serious health problems and lack of positive effect from treatment. The problem solution is to create a “smart” organizer with a reminder function. The organizer is controlled by the Arduino UNO board. The device is configured using buttons; a reminder is a message on the display, as well as a sound and a light signal. A delay function of taking medications has also been implemented.

Вступ. Прихильність до лікування – поняття, що характеризує готовність пацієнта виконувати рекомендації лікаря. Дослідження в області лікування різних хронічних патології показало, що прихильність до лікування у розвинених країнах в середньому становить 50 % [1, 2, 3]. Рівень цього показника у країнах, що розвиваються, є ще нижчим.

Проблема прихильності до лікування залежить від багатьох факторів [1], які можна поділити на: соціально-економічні (низький соціально-економічний рівень, безробіття, віддаленість лікарні, нестабільні умови проживання); фактори, що пов’язані з системою охорони здоров’я (недостатній рівень освіченості лікарів у методах лікування та з питань прихильності до лікування, короткотривалі візити, відсутність зворотного зв’язку); фактори, що пов’язані безпосередньо з захворюванням (важкість, доступність ліків); фактори, що пов’язані з лікуванням (складність і тривалість лікування, побічні ефекти); фактори, що пов’язані з пацієнтом (забудькуватість, низька мотивація до регулярного прийому ліків, відсутність моніторингу).

Використання цифрових технологій у галузі охорони здоров'я може покращити багато з вище вказаних факторів. Майбутнє цифрових технологій пов’язане з розвитком штучного інтелекту, інтернету медичних речей (IoMT), віддаленим моніторингом пацієнтів, віртуальною реальністю, 3D-друком, клінічною автоматизацією, тощо [4].

Об’єктом дослідження є фактори прихильності до лікування, що пов’язані з пацієнтом, а саме контроль прийому ліків. Наразі існує багато інтернет-застосунків, що допомагають контролювати прийом ліків. Але не всі пацієнти мають змогу користуватися інтернетом, смартфоном і взагалі можуть розібратися з ними без сторонньої допомоги. Більш простим

варіантом контролю прийому ліків є використання органайзеру. На ринку їх існує багато, але більшість не вирішує проблему з пропуском прийому ліків. Тому, *предметом дослідження* є автоматизація контролю прийому ліків за допомогою «розумного» органайзеру. *Мета дослідження* – проектування розумного органайзера ліків з функцією нагадування.

Зміст дослідження. Запропонована модель «розумного» органайзера в якості головного блока керування використовує плату Arduino Uno на базі мікроконтролера ATmega328P. Її можна запрограмувати на необхідну періодичність прийому (один, два чи три рази на день) за допомогою відповідних кнопок (тактові кнопки без фіксації). Ці дані зберігаються в EEPROM пам’яті самого мікроконтролера.

Органайзер буде сигналізувати про потребу прийому ліків звуком (активний п’єзо динамік) і світловою індикацією (миготіння світлодіода). Звук буде ввімкнений до тих пір, поки пацієнт не прийме ліки і не натисне відповідну кнопку зупинки сигналу. Також є функція відтермінування прийому ліків на 30 хвилин. На дисплеї з підсвічуванням (LCD 1602) буде відображатися вся необхідна інформація, включаючи поточну дату та час (модуль годинника реального часу DS1302). Для спрощення підключення дисплею до мікроконтролера використовується інтерфейсний модуль I^2C на мікросхемі PCF8574T, а захист від “брязкоту” контактів реалізовано програмно. Програма керуванням органайзеру ліків написана на мові С в середовищі Arduino IDE.

Висновки. Контроль прийому ліків – це важлива частина здорового способу життя, особливо для людей, які страждають на хронічні захворювання. Часто порушення графіка прийому препаратів призводить до серйозних проблем зі здоров'ям, що може вплинути на якість життя і навіть спричинити ускладнення. Деякі медикаменти можуть не діяти, якщо їх приймати не за розкладом, інші можуть призвести до побічних ефектів, якщо перевищено дозування або пропущений прийом. Існує багато причин порушення графіка прийому ліків, але найчастіше люди просто забувають прийняти чергову таблетку. А у випадку прийому багатьох препаратів, пацієнти банально плутаються, чи прийняли вони ліки чи ні. При довготривалому лікування органайзер – річ життєво необхідна. Використання «розумного» органайзера вирішує ці проблеми. Він не тільки допоможе організувати ліки на весь тиждень, але й допоможе не забути їх прийняти згідно зі встановленим графіком. Спроектовано модель «розумного» органайзера та алгоритм його роботи. Тестування розробленого прототипу підтверджує його працездатність.

Наукова новизна визначається використанням мікроконтролера Arduino для керування часом прийому ліків і нагадуванням (як за допомогою дисплею, так і за допомогою світлової та звукової індикації). Пристрій може бути виконано в портативному варіанті з автономним

живленням від батарейки, що дасть можливість використовувати його не тільки вдома чи у лікарні, але і брати з собою в дорогу.

Список використаних джерел:

1. Слепченко Н.С. Прихильність до лікування: методи її покращення при інгаляційній терапії бронхіальної астми / Н. С. Слепченко, К. Д. Дмитрієв // Український пульмонологічний журнал. – 2018. – № 2. – С. 53-60.
2. Прихильність до лікування хворих на ішемічну хворобу серця як дієвий фактор профілактики / Т.А. Трибрат, С.В. Шуть, В.Д. Сакевич, О.О. Гончарова // Вісник проблем біології і медицини. – 2019. – №1 (148). – С. 185-188.
3. Ягенський А.В. Прихильність до лікування пацієнтів у віддалений період після інфаркту міокарда / А.В. Ягенський, І.М. Січкарук // Раціональна фармакотерапія. – 2019. – № 1-2 (50-51). – С. 24-27.
4. Андрощук Г. Цифрова трансформація в охороні здоров'я: аналіз технологічних трендів / Г. Андрощук // Юридична газета online. – 2023. – Режим доступу: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/cifrova-transformaciya-v-ohoroni-zdorovya-analiz-tehnologichnih-trendiv.html. – Дата звернення: 26.02.24. – Загол. з екрану.
5. Margolis M. Arduino Cookbook / M. Margolis. – Sebastopol: O'Reilly Media, 2011. – 724 p.

УДК: 004.7: 004.72 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.061

СЦЕНАРІЙ ПОБУДОВИ ЗАХИЩЕНОГО СЕГМЕНТУ МЕРЕЖІ МІЖ ВІРТУАЛЬНИМИ ОФІСАМИ

Свергун В.А.
Науковий керівник – ас. Чепурна І.С.
Харківський національний університет радіоелектроніки, каф. ЕОМ
м. Харків, Україна
e-mail: vladyslav.sverhun@nure.ua

The article discusses scenarios for building corporate computer networks that take into account the requirements of secure remote access and fault tolerance by creating reliable virtual communication channels. Provision of secure access to nodes of corporate networks is implemented on the basis of hardware and software tools. The article considers the scenario of building a protected network segment between virtual offices according to the site-to-site scheme, where the Mikrotik CHR software is used as the end nodes.

Сучасні технології дистанційної роботи у бізнесі та державному секторі призвели до збільшення попиту на програмні рішення з організації дистанційних робочих місць. Наприклад, в Україні – це стало особливо актуально під час пандемії коронавірусної хвороби COVID-19 та повномасштабної збройної агресії рф [1]. У задачах організації відділених робочих місць виникає й інша задача, пов’язана із забезпеченням належного рівня мережної безпеки та створенню надійних віртуальних каналів зв’язку. Саме тому, у сучасних сценаріях побудови корпоративних комп’ютерних мереж вирішується комплексна задача системного та, власне, мережного рівня з урахуванням вимог захищеного віддаленого доступу, відмовостійкості віддалених віртуальних машин, конфіденційності та цілісності даних.

Мета даної роботи полягає у створенні сценаріїв функціонування корпоративних комп’ютерних мереж, які складаються щонайменше із декількох сегментів, поєднаних між собою за допомогою технології віртуальних тунелів. Цю мету можна досягти використовуючи стандартні підходи, на кшталт, традиційного VPN-тунелювання, а також можна застосувати нестандартні рішення, які включають в себе різні технології, як-от, багатошарове шифрування, агрегацію віртуальних каналів, асинхронні шляхи передачі даних тощо.

Серед інших рішень, які у сукупності можуть забезпечити наведені вище вимоги, для забезпечення захищеного доступу до вузлів корпоративних комп’ютерних мереж можуть бути використані рішення на основі програмно-апаратних засобів. Наприклад, це можуть бути міжмережні екрани та проксі-сервери.

З огляду на організацію сегментації корпоративних комп’ютерних мереж рівня віртуальних офісів можуть використовуватися мікросервіси хмарних

вендорів або класичні рішення VLAN, які підтримуються віртуалізованими рішеннями щодо комутації та маршрутизації трафіку, наприклад Open vSwitch [2].

Інші комплексні рішення можуть включати використання міжмережних екранів, каскадування proxy-серверів та ланцюгів VPN для досягнення зазначених вище вимог, однак це також може призводити до падіння швидкості передачі даних за рахунок багаторазового перепакування пакетів даних, їх шифрування та дешифрування зі сторони користувача [3].

В роботі досліджено сценарій побудови захищеного сегменту мережі між віртуальними офісами за схемою site-to-site, де у якості кінцевих вузлів використано програмне забезпечення Mikrotik CHR. Встановлено, що таке рішення надає такі переваги:

- можливість використання різних VPN-протоколів, за допомогою яких шифруються дані. Наприклад, протокол WireGuard надає можливість використовувати сценарій site-to-site в різних типах мережних топологій із забезпеченням максимальної стійкості віртуальних тунелів [4];
- часові затримки при передачі еластичного трафіку становлять на 15% вище, ніж у традиційних мережах, а нееластичного – до 5%.

Таким чином, розглянутий сценарій, за результатами проведених досліджень, показав, що для побудови захищених сегментів корпоративних мереж наразі є задовільним рішенням використання схеми site-to-site. У якості подальших досліджень планується вивчення питань тунелювання в віртуальних середовищах провідних вендорах.

Список використаних джерел

1. Hvozdetska K. P. Organization of teleworking via VPN technology / K. P. Hvozdetska, V. M. Tkachov // Збірник тез доповідей одинадцятої міжнародної науково-технічної конференції "Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління", 8-9 квітня 2021 року. - Том 2: секція 4. - Баку-Харків-Київ-Жиліна. - 2021. - С. 79.

2. Afanasieva A. DEVELOPMENT OF PRINCIPLES OF VPN-TUNNELING [Електронний ресурс] / A.M. Afanasieva // Information society: technological, economic and technical aspects of formation (issue 67) – 2022. – Режим доступу до ресурсу: http://www.konferenciaonline.org.ua/ru/article/id-520/.

3. Tkachov, V Technology of Load Balancing in Anonymous Network Based on Proxy Nodes Cascade Platform / V.Tkachov, M. Hunko, M. Bondarenko, S. Artyomov // COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES. – 2020. – С. 82.

4. Верховський, І. Методи побудови віртуальних тунелів EXTRANET-систем / І. Верховський, В. Ткачов // Scientific review, –(2023). – 4(89), с. 22-40.

УДК 004 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.063

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ СПІЛЬНОЇ ФІЛЬТРАЦІЇ В MUSIC RECOMMENDATION SYSTEM

Сергородцев І.Д., Жук М.В.
Науковий керівник – д.т.н. проф. Фесенко Т.Г.
Харківський національний університет радіоелектроніки, каф. ЕОМ,
м. Харків, Україна
тел.+38(050) 274-67-92, e-mail: illia.serhorodtsev@nure.ua;
тел. +38(063) 951-73-72, e-mail: maksym.zhuk@nure.ua.

This work is devoted to finding solutions for effective search in music streaming services. The application of Music Recommendation Systems allows the user to learn about new artists, the release of new albums, songs, musical compositions. Two scenarios for the implementation of the joint filtering method were studied. The first scenario – searching for users based on similar music preferences. The second scenario – the search of users is carried out by different (individual) musical preferences. A class diagram scheme is proposed for implementing collaborative filtering in music recommendation systems.

На сьогоднішній день все більшої популярності набувають музичні стрімінгові сервіси (Spotify, Apple Music, Amazon Music, YouTube Music, Tidal), які дозволяють користувачам шукати музику залежно від власних вподобань і слухати її на різних пристроях. Важливою частиною музичних стрімінгових сервісів є системи рекомендацій музики (Music Recommendation System), застосовуючи які користувач може дізнатись про нових виконавців, випуск нових альбомів, пісень, музичних композицій [1, 2]. Підбор контенту може бути реалізований різними методами, зокрема: історія прослуховування; подібна музика, плейлисти та жанри, рекомендації від інших користувачів. З метою залучення більшої кількості користувачів кожен музичний стрімінговий сервіс розробляє власні унікальні алгоритми, підходи та рекомендації для пошуку музичних композицій. Одним із напрямків удосконалення пошукових алгоритмів для систем рекомендації музики є метод спільної фільтрації [3, 4].

Спільна фільтрація (Collaborative Filtering) використовується в системах рекомендацій як метод прогнозування інтересів користувачів на основі їх попередніх взаємодій з системою, взаємодій інших користувачів з подібними вподобаннями. Основною ідеєю спільної фільтрації є передбачення того (наприклад, музики), що може сподобатись користувачу, шляхом оцінювання та взаємодії з іншими користувачами, які мають подібні вподобання або історії. Наприклад, якщо користувач «А» і користувач «Б» мають подібні історії прослуховування, і користувач «А» вподобав певний виконавець, то система рекомендацій музики може рекомендувати цього ж виконавця і користувачу «Б».

Реалізація спільної фільтрації може відбуватись двома сценаріями. Перший сценарій – між користувачами відсутні спільні оцінки або однакові оцінки для всіх елементів. У випадку коли користувач «А» і користувач «Б» не мають спільних оцінок (тобто відсутні данні для порівняння їх музичних вподобань), система рекомендацій музики виявляє подібних користувачів на основі інших критеріїв (наприклад, схожість в музичних жанрах, виконавцях чи характеристиках треків). Тоді пошук користувачів здійснюється за схожими музичними вподобаннями, навіть якщо вони не взаємодіяли безпосередньо у минулому.

Інший випадок – оцінки користувача «А» і користувач «Б» однакові за усіма елементами (користувачі не надали індивідуальних оцінок для різних музичних елементів) – система рекомендацій музики буде сприймати користувачів «А» і «Б» з однаковими інтересами до всього музичного контенту. В цій ситуації пошук здійснюється за популярністю музичного контенту або за додатковими даними про користувача.

Другий сценарій реалізації спільної фільтрації в системах рекомендацій музики пов’язаній з необхідністю аналізувати індивідуальні музичні вподобання користувачів та вироблення персоналізованих рекомендацій. Вирішення такої задачі потребує виокремлення двох класів:

1) «користувач», має ідентифікатор (унікальний код) і словник рейтингів (оцінки користувача для різних елементів). У словнику ключ – ItemId, значення – Rating;
2) «CollaborativeFiltering», сприймає список об’єктів користувача як вхідні дані та реалізує алгоритм спільної фільтрації.

В контексті колаборативного фільтрування для визначення схожості між двома користувачами або предметами на основі їх оцінок або взаємодій застосовується метод PearsonCorrelation. Кожен користувач представляється як вектор, де кожне значення – як оцінка користувача для певного предмета (музичної композиції). На основі цих векторів обчислюється коефіцієнт кореляції Пірсона (Pearson correlation coefficient). Значення коефіцієнта від «+1» до «-1», де «1» – загальна позитивна лінійна кореляція, «0» – лінійна кореляція відсутня, а «-1» – загальна негативна лінійна кореляція.

Метод GetSimilarUsers застосовується для пошуку «схожих користувачів» на основі їх взаємодії із системою. Для цього використовувати різні метрики схожості, зокрема: косинусна схожість, кореляція Пірсона, або інші. Реалізація методу GetSimilarUsers передбачає наступну послідовність дій: підготовка даних; обчислення схожості, сортування результатів; вибір схожих результатів.

У цілому, реалізація спільної фільтрації в системах рекомендацій музики вимагає агрегування оцінок «подібних користувачів» для прогнозування оцінок «цільових користувачів» (рисунок), зокрема за

допомогою середнього зваженого рейтингу «схожих користувачів», де ваговими коефіцієнтами є оцінки подібності.

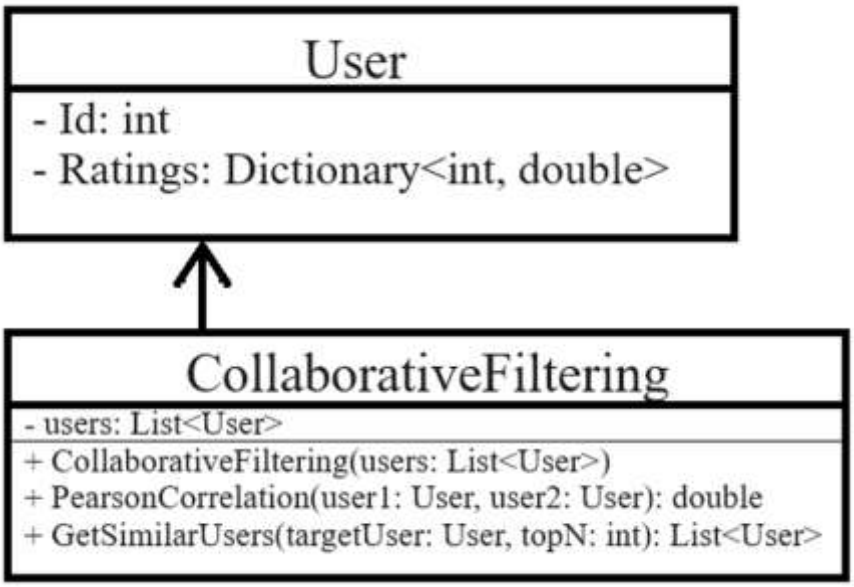


Рисунок – Загальна схема діаграми класів для реалізації спільної фільтрації в системах рекомендацій музики

Список використаних джерел:

1. Фесенко Т.Г. & Фесенко Г.Г. (2023). Управління цифровими проєктами як основа сталого розвитку. Проєктний та логістичний менеджмент: нові знання на базі двох методологій. Том 7 : збірник наукових праць. Одеса: КУПРІЄНКО СВ, 2023,17–20.

2. Андрусенко Ю.О. & Фесенко Т.Г. (2023). Нестаціонарність ресурсів та послуг хмарної інфраструктури. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, Т.4(74), 129–133. doi: https://doi.org/10.26906/SUNZ.2023.4.129.

3. Рибалов О.О. & Фесенко Т.Г. (2023). Дослідження засобів інтелектуального аналізу текстових документів. Збірник наукових праць XVI Міжнародної науково-практичної конференції «Академічна й університетська наука: результати та перспективи», 12–13 грудня 2023 року. Полтава: Полтавська політехніка, 330–331.

4. Rezanov, B., Semenova, A., Petrovska, I. & Fesenko T. (2021). Model for Providing the Second Factor of Authentication Into Authentication Services with Centralized Account Databases. Fifth International Scientific and Technical Conference "Computer and information systems and technologies", 46–47. https://doi.org/10.30837/csitic52021232201.

УДК 004.738.5 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.066

ІНТЕГРАЦІЯ ОБРОБКИ ВЕЛИКИХ ДАНИХ ЗА ДОПОМОГОЮ НЕЙРОМЕРЕЖ У ХМАРНІ ОБЧИСЛЕННЯ

Сердюк С.С.
Науковий керівник – д.т.н., проф. Руденко О.Г.
Харківський національний університет радіоелектроніки, каф. КІТС,
м. Харків, Україна
e-mail: sofiia.serdiuk@nure.ua

The integration of cloud computing and big data processing using neural networks opens wide opportunities for the development and improvement of information analysis. This approach makes it possible to use resources efficiently, speed up data processing, and provide accurate and predictable results thanks to neural networks.

Хмарні обчислення надають широкий спектр послуг і ресурсів, які можна використовувати для зберігання, обробки та аналізу великих обсягів даних [1]. Хмарні обчислення дозволяють легко масштабувати ресурси в залежності від обсягу оброблюваної інформації. Це робить систему більш еластичною, дозволяючи швидко адаптуватися до змін обсягу даних. Хмарні платформи надають можливість зберігати великі обсяги даних і забезпечують швидкий і надійний доступ до них. Використання сховища об’єктів, наприклад Amazon S3 або Azure Blob Storage, може спростити процес зберігання та керування даними. Крім того, хмарні платформи надають величезний потенціал для обчислювальних завдань [2]. Використання віртуальних машин, контейнерів або безсерверної обчислювальної служби може значно полегшити обробку великих обсягів даних.

Хмарні сервіси також надають інструменти для виконання аналітичних завдань і розгортання моделей машинного навчання. Google Cloud AI, Azure Machine Learning або Amazon SageMaker – лише деякі приклади платформ для розробки та розгортання моделей. Оскільки обробка великої інформації часто містить конфіденційні дані, важливо враховувати аспекти безпеки. Хмарні платформи забезпечують засоби шифрування даних, аудиту та контролю доступу.

Використання хмарних обчислень при обробці великої інформації може істотно полегшити і прискорити роботу з даними. При виборі та використанні хмарних рішень важливо враховувати конкретні вимоги та особливості проекту. Інтеграція обробки великих даних за допомогою нейронних мереж у хмарні обчислення є захоплюючою сферою, яка може значно покращити аналітику та прийняття рішень на основі великих обсягів інформації.

Великі дані надають чудову можливість для навчання нейронних мереж на великому обсязі різнорідних даних. Важливо враховувати можливість використання різних архітектур нейронних мереж, таких як глибокі нейронні мережі (Deep Neural Networks) або згорткові нейронні мережі (Convolutional Neural Networks), залежно від конкретних завдань.

У хмарних сервісах є можливості для паралельної обробки великих обсягів даних, що сприяє прискоренню навчання нейронних мереж. Використання графічних обчислювальних ресурсів (GPU або TPU) може бути ефективним для великомасштабних завдань машинного навчання. Хмарні платформи надають зручні інструменти для розгортання моделей нейронних мереж. Хмарні сервіси машинного навчання, такі як AWS SageMaker, Google AI Platform або Azure Machine Learning, спрощують процес розгортання та керування моделями [2].

З огляду на те, що для ефективного навчання нейронним мережам можуть знадобитися великі обсяги даних, оптимізація обробки великих даних стає ключовою. Необхідно розглянути можливості оптимізації та запобігання перекваліфікації. Оскільки обробка великих даних і використання нейронних мереж часто пов’язані з конфіденційністю даних, зверніть увагу на заходи безпеки та шифрування, щоб забезпечити захист інформації.

Поєднання хмарних обчислень і обробки великих даних за допомогою нейронних мереж відкриває нові можливості для швидкого та ефективного аналізу великих обсягів інформації. Хмарні платформи дозволяють легко масштабувати інфраструктуру та використовувати потужні ресурси для навчання та розгортання нейронних мереж.

Такий підхід полегшує доступ до передових технологій машинного навчання та покращує аналітику. Оптимізація обчислювальних ресурсів, паралельна обробка даних і використання спеціалізованих сервісів для машинного навчання в хмарних сервісах роблять цей процес більш ефективним і доступним. Однак важливо враховувати аспекти безпеки та конфіденційності даних, оскільки ці питання стають ключовими при обробці великих обсягів інформації. Захист від несанкціонованого доступу та використання шифрування необхідні для забезпечення конфіденційності даних під час їх обробки та аналізу.

Список використаних джерел

1. Cloud computing [Електронний ресурс]. – Режим доступу: uk.wikipedia.org/wiki/Cloud_computing.

2. Amazon Web Services, Inc. [Електронний ресурс]. – Режим доступу: https://aws.amazon.com/.

УДК 005.8:004.4 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.068

ВЕБ-ТЕХНОЛОГІЙ В УПРАВЛІННІ ПРОЄКТАМИ: БІБЛІОГРАФІЧНА КАРТА ДОСЛІДЖЕННЯ

Снігур А.Р.
Науковий керівник – д.т.н. проф. Фесенко Т.Г.
Харківський національний університет радіоелектроніки, каф. ЕОМ,
м. Харків, Україна
тел. +38(066) 406-53-86, e-mail: anton.snihur@nure.ua

In this work, a bibliometric analysis of trends in web technologies in the field of project management was carried out in order to identify key problems and directions of research. The study analyzed various metrics, such as the annual number of publications and the most used keywords. The following keywords were most relevant: knowledge management, agent, teaching, world, community, information technology. The relevance of these keywords indicates that the topics of training, knowledge management, and information technologies were of great interest to the authors during the research. Thus, on the basis of the obtained results, it is possible to draw a conclusion about the potential directions of further research in this area.

На сьогоднішній день веб-технології стали невід'ємною інструментально-методологічною складовою проєктного менеджменту, оскільки дозволяють забезпечити ефективну комунікацію, спільну роботу та відстеження прогресу. Серед популярних веб-технологій для управління проєктами можна відзначити:

1) системи управління проєктами (Project Management Systems), наприклад, Asana, Trello, Jira, Basecamp та інші.;

2) інструменти для спільної роботи (Collaboration Tools), наприклад, Google Workspace (раніше G Suite), Microsoft 365, Slack та інші платформи;

3) додатки для відстеження часу (Time Tracking Apps), наприклад, Harvest, Toggl, RescueTime;

4) спеціалізовані платформи для управління проєктами, розроблені для певних галузей або типів проєктів [1–4].

Метою даного дослідження є проведення високорівневого аналізу публікацій на тематику «веб-технологій в управлінні проєктами». Для досягнення поставленої мети пропонується провести пошук досліджень в бібліометричній базі Scopus і розробити бібліографічну карту із використанням програми VOSviewer. Це дозволить промаркувати актуальні тенденції для розвитку знань з управління проєктами.

Пошуковий запит здійснювався за ключовими словами: website*, web, web application*, web service*, project* management, project manager*. В результаті знайдено 268 документів, які були опубліковані у період з 1997 по 2023 роки. Аналіз кількості публікацій у часі дозволив встановити, що у 1997 році була опублікована одна стаття, а у 2023 рік – дев'ять. Найбільша

кількість публікацій (двадцять п’ять) опублікована у 2008 році і обумовлена тим, що в цей час ІТ компаній почали активно використовувати веб-сервіси для планування, відстеження і управління ризиками.

Використання програми VOSviewer дозволило у 268 документах ідентифікувати 100 найбільш вживаних термінів та структурувати їх у два кластера (рисунок): перший – «Аспекти управління проєктами та професійний розвиток» (позначено червоним кольором); другий – «Технологічна інтеграція та вплив інформаційних систем» (позначено зеленим кольором).

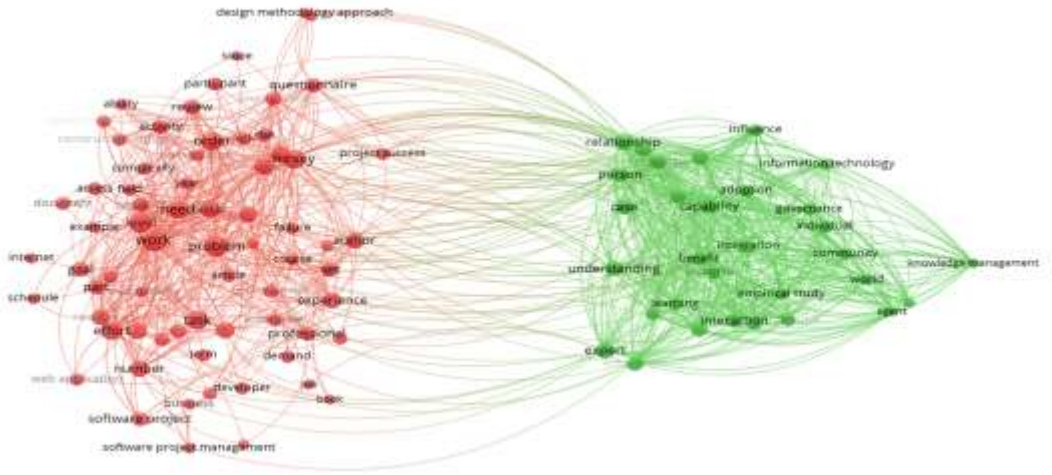


Рисунок – Наукометрична карта для 100 термінів з 268 документів

Список використаних джерел:

1. Фесенко Т.Г. & Фесенко Г.Г. (2023). Управління цифровими проєктами як основа сталого розвитку. Проєктний та логістичний менеджмент: нові знання на базі двох методологій. Том 7 : збірник наукових праць. Одеса: КУПРІЄНКО СВ, 2023,17–20.

2. Григоров М.В. & Фесенко Т.Г. (2022). Комп’ютерні технології управління в будівництві : інфографіка огляду літератури. Проблеми інформатизації : тези доповідей десятої міжнародної науково-технічної конференції 24–25 листопада 2022 року. Том 1. Харків : ХНУРЕ, 29.

3. Фесенко Т. (2022). Сучасні знання для управління будівельними проєктами: бібліографічна карта дослідження. Архітектура та будівництво: Відновлення України. Наука, технологія, практика : Програми і тези доповідей міжнародного науково-технічного форуму, 17 листопада 2022 року. Київ: КНУБА, 344–345.

4. Fesenko T. (2022). Stakeholder management in sustainability construction projects: a preliminary literature review. Механізми забезпечення сталого розвитку економіки: проблеми, перспективи, міжнародний досвід :матеріали III Міжнар. наук.-практ. інтернет-конф., 10 листопада 2022 р. Держ. біотехнологічний ун-т. Харків, 21–24.

УДК 004.8 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.070

ІНСТРУМЕНТИ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ СТВОРЕННЯ КОНТЕНТУ ВЕБ-РЕСУРСІВ

Хрустальов Є. К.
Науковий керівник – д.т.н., проф. Фесенко Т.Г.
Харківський національний університет радіоелектроніки, каф. ЕОМ,
м. Харків, Україна
тел +38(095) 628-33-50, e-mail: yevhenii.khrustalov@nure.ua

The work examines the possibility of using artificial intelligence algorithms in creating and analyzing content on web platforms. Machine learning methods and natural language processing technologies are discussed, which can improve the quality of content, personalize it to the needs of the audience, and ensure the safety of the online environment. The advantages and problems of using artificial intelligence algorithms in content marketing and information management on web resources are considered.

На сьогоднішній день алгоритми штучного інтелекту (Artificial Intelligence, AI) – революційний інструментарій у світі інформаційних технологій. Провідні компанії світу активно впроваджують і використовують AI для ефективної взаємодії з цільовими стейкхолдерами. Використання алгоритмів штучного інтелекту для генерації контенту веб-ресурсів дозволяє автоматизувати процес створення та управління інформацією. Алгоритми AI можуть бути задіяні в різних аспектах контентної стратегії: від створення текстового, графічного або відеоконтенту до його аналізу та оцінки [1, 2]. Отже, застосування алгоритмів AI дозволяє підвищити ефективність процесу та заощадити час і ресурси для виконання інших завдань (наприклад, стратегічне планування контентної стратегії, поглиблений аналіз даних і т.ін.) [3, 4].

Методи машинного навчання можуть бути застосовані для аналізу контенту та визначення його релевантності, якості та унікальності. Також, використання методів машинного навчання дозволяє класифікувати та автоматично розділити контент на різні категорії або класи [5]. Наприклад, текстові статті можуть бути класифіковані за темами, зображення – за змістом, а аудіофайли – за жанром музики тощо. Це допомагає організувати контент на веб-ресурсі та забезпечити найкращу навігацію для користувачів. Також методи машинного навчання допомагають в розробці моделей оцінки якості контенту на основі різних метрик, таких як: унікальність тексту, емоційне забарвлення, стиль та граматична коректність для автоматичного виявлення плагіату (схожість) або дубльованого контенту.

Метод кластеризації дозволяє групувати схожі об’єкти в кластери та виявляти схожі або тематично пов’язані елементи контенту. Наприклад, цей метод можна застосувати для пошуку пов’язаних статей або товарів на веб-

сайті, а також запропонувати користувачам додатковий контент, що може їх зацікавити.

Аналіз контенту різного типу (текст, зображення, аудіо та відео) може бути реалізовано шляхом використання нейронних мереж. Наприклад, нейронні згорткові мережі дозволять проаналізувати зображення і розпізнати об'єкт або особу, а рекурентні нейронні мережі – проаналізувати текст та згенерувати пропозицій, пов'язаних з текстом.

Ключову роль у покращенні досвіду користувача на веб-платформах відіграють системи рекомендацій, засновані на алгоритмах штучного інтелекту. Такі системи працюють на основі аналізу даних про поведінку користувача, історій переглядів, дії та соціальної взаємодії. Ці дані використовуються для персоналізації контенту в рекомендаціях, що, у свою чергу, сприяє підвищенню залученості користувача. Крім того, збільшується задоволеність кінцевого користувача, адже досвід роботи з електронним ресурсом приємний та зручний. Користувач, який задоволений контентом та запропонованими системою рекомендаціями, скоріш за все буде повертатися на веб-ресурс знову і знову. Збільшення кількості повторних відвідувань створює лояльність до бренду чи платформи та може призвести до підвищення конверсії.

Технології обробки природної мови (Natural Language Processing, NLP), дозволяє комп'ютерам розуміти природну мову і передбачає: виділення ключових слів і фраз, визначення зв'язків між ними, розуміння контексту і семантики речень. Додатковою перевагою використання NLP – можливість визначати емоційне забарвлення тексту, що передбачає оцінку ставлення до події, продукту чи послуги, а також розуміти відгуки користувачів або реакцію на новини та події. Аналіз емоційного забарвлення на основі NLP може визначати конкретні емоції, виражені в тексті, такі як радість, сум, страх або злість. Така функціональність дозволить розуміти емоційний контекст тексту та відповідно адаптувати його контент. Наприклад, маркетологи можуть використовувати для створення контенту такі дані, які викликають певні емоції у користувачів.

Крім створення та аналізу контенту, автоматизовані системи можуть бути корисними для підтримки безпечного середовища на веб-ресурсі. Наприклад, імплементація моніторингу в реальному часі може сканувати платформу на наявність шкідливого або небажаного контенту з метою запобігання розповсюдженню такого контенту. Захист даних підвищує рівень довіри користувачів продукту і є пріоритетним завданням для будь-якого веб-ресурсу.

Водночас, як і будь-яка система, генерація та аналіз контенту з використанням AI, має свої недоліки:

1) схильність до упередженості, заснованої на даних, на яких вони навчаються;

2) згенерований контент може містити небажані або шкідливі матеріали, такі як фейкові новини, дезінформація або контент, що порушує правила безпеки та норми поведінки;
3) загроза для приватності та безпеки конфіденційних даних користувачів;
4) виняткова довіра алгоритмам AI для створення та аналізу контенту може призвести до залежності від технологій та втрати здатності до критичного мислення та оцінки контенту.

У підсумку, використання алгоритмів штучного інтелекту може значно підвищити ефективність та прибутковість веб-ресурсу за умов грамотного підходу у виборі методів для створення і аналізу контенту. Під час прийняття рішення щодо вибору методів слід враховувати наявні недоліки використання AI та знаходити оптимальне (збалансоване) рішення.

Список використаних джерел

1. Андрусенко Ю.О. & Фесенко Т.Г. (2023). Нестаціонарність ресурсів та послуг хмарної інфраструктури. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, Т.4(74), 129–133. doi: https://doi.org/10.26906/SUNZ.2023.4.129.

2. Андрусенко Ю.О. & Фесенко Т.Г. (2023). Грід-технології в розподілених обчислювальних середовищах. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, Т.3(73), 148–151. doi: https://doi.org/10.26906/SUNZ.2023.3.148.

3. Rezanov, B., Semenova, A., Petrovska, I. & Fesenko T. (2021). Model for Providing the Second Factor of Authentication Into Authentication Services with Centralized Account Databases. Fifth International Scientific and Technical Conference "Computer and information systems and technologies", 46–47. https://doi.org/10.30837/csitic52021232201.

4. Андрусенко Ю.О. & Фесенко Т.Г. (2023). Планування ресурсів у розподілених обчислювальних середовищах. Проблеми інформатизації : тези доп. 11-ї міжнар. наук.-техн. конф., 16-17 листопада 2023 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 3 т.]. Т.1. Харків: Impress, С. 78.

5. Рибалов О.О. & Фесенко Т.Г. (2023). Дослідження засобів інтелектуального аналізу текстових документів. Збірник наукових праць XVI Міжнародної науково-практичної конференції «Академічна й університетська наука: результати та перспективи», 12–13 грудня 2023 року. Полтава: Полтавська політехніка, 330–331.

УДК 004.93 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.073

ПРИКЛАДНІ ЗАСТОСУВАННЯ СИСТЕМ КОМП'ЮТЕРНОГО ЗОРУ

Ціпковський В. О.
Науковий керівник – д.ф., ас. каф. ЕОМ Єрошенко О.А.
Харківський національний університет радіоелектроніки, каф. ЕОМ,
м. Харків, Україна
e-mail: vadym.tsipkovskyi@nure.ua

This work is devoted to assessing the applied applications of computer vision systems in different spheres of human's life. The exploration of the diverse ways in which the computer vision technology is utilized in practical contexts across the various fields was made. Through the analysis of real-world scenarios, this work delves into how computer vision systems are employed in sectors such as healthcare, manufacturing, transportation, surveillance, and entertainment. By examining specific use cases and implementations, research gains insights into the effectiveness, challenges, and potential advancements of these systems. Overall, investigating the applied applications of computer vision systems offers valuable perspectives on their impact on industry and human experiences.

Сфера комп'ютерного зору – це сфера штучного інтелекту, яка використовує машинне та глибоке навчання, щоб дозволити комп'ютерам бачити, виконувати розпізнавання образів і аналізувати об'єкти на фотографіях і відео так само, як це роблять люди. Комп'ютерне бачення швидко набирає популярності для віддаленого моніторингу та автоматизації. Робота з комп'ютерним баченням має величезний вплив на компанії в різних галузях, від роздрібної торгівлі до безпеки, охорони здоров'я, будівництва, автомобілебудування, виробництва, логістики та сільського господарства. Системи комп'ютерного зору використовують камери для отримання візуальних даних, моделі машинного навчання для обробки зображень і умовну логіку для автоматизації конкретних прикладних випадків використання. Розгортання штучного інтелекту на крайніх пристроях, так званого периферійного інтелекту, полегшує реалізацію масштабованих, ефективних, надійних, безпечних і приватних реалізацій комп'ютерного зору.

У виробництві розпізнавання зображень застосовується для огляду, аналітики продуктивності, контролю якості, віддаленого моніторингу та автоматизації системи. Аналітика продуктивності відстежує вплив змін на робочому місці, як працівники витрачають свій час і ресурси, а також запроваджує різні інструменти. Такі дані можуть надати цінну інформацію про управління часом, співпрацю на робочому місці та продуктивність співробітників. Стратегії економічного управління комп'ютерним баченням спрямовані на об'єктивну кількісну оцінку процесів за допомогою систем бачення на основі камер. Програми для розумних камер забезпечують масштабований метод для реалізації автоматизованого візуального

контролю та контролю якості виробничих процесів і виробничих ліній на розумних заводах. Таким чином, глибоке навчання використовує виявлення об’єктів у реальному часі, щоб забезпечити кращі результати (точність виявлення, швидкість, об’єктивність, надійність) порівняно з трудомісткою перевіркою вручну. Порівняно з традиційними системами, ШІ-інспекція використовує методи машинного навчання, які є дуже надійними та не потребують дорогих спеціальних камер і негнучких налаштувань. Отже, методи бачення штучного інтелекту дуже гарно підходять для масштабування багатьох виробничих локацій і фабрик.

Зараз комп’ютерний зір відіграє життєво важливу роль в службах безпеки. Деякі з його відомих застосувань: автентифікація обличчя, виявлення фейкових новин та камери відеоспостереження, котрі відстежують незвичайні дії. Розпізнавання обличчя та автентифікація є важливою програмою безпеки, за допомогою якої комп’ютерний зір може виявити чиєсь обличчя та зіставити його з базою даних осіб у розшуку. Фейкові новини є великою причиною неспокою в суспільстві. Це може спричинити хаос, а іноді навіть призвести до насильства. Комп’ютерний зір і глибоке навчання можуть допомогти у виявленні цих фейків і видаленні неправдивих новин. Камери відеоспостереження в поєднанні з глибоким навачанням і комп'ютерним зором можуть допомогти нам виявити незвичайні дії, такі як крадіжки, пограбування, переслідування та інші шкідливі дії, такі як бійки. Гарним прикладом програми для виявлення подібних дій є японський стартап для виявлення крадіжок VAAKEYE[1].

З моменту появи глибокого та машинного навчання сфера охорони здоров’я отримала багато переваг. Деякі програми включають точне вимірювання втрати крові, виявлення раку, більш точну діагностику, інтерактивне медичне зображення, автоматичне створення медичних звітів Однією з найбільших причин смертності під час пологів є післяпологова кровотеча. Це відбувається в основному через надмірну втрату крові. Використовуючи комп’ютерний зір, лікарі можуть точно виміряти, скільки крові було втрачено під час процесу пологів, і, отже, лікувати жінок більш належним чином. Сучасні алгоритми глибокого навчання та велика кількість даних звели до мінімуму помилкові діагнози. Діагностика більш точна, і це може зменшити кількість зайвих хірургічних процесів. Комп’ютерне бачення для медичної візуалізації дозволяє 3D-візуалізацію в зручній, інтерактивній та детальній формі. Зразком успішної програми котра використовується для даних цілей є ADAS3D[2]. Тепер глибоке навчання та комп’ютерний зір можна використовувати для візуального аналізу інтерактивних 3D-моделей, щоб поставити точніші медичні діагнози. Широке використання даних медичних зображень дозволило комп’ютерному зору та глибокому навчанню створювати точні та правильні звіти на основі медичних зображень, наприклад, виявлення захворювань легенів за допомогою рентгенівського зображення. Передача даних МРТ,

рентгенівських знімків, комп’ютерної томографії та інших джерел в алгоритми автоматично створюватиме звіти та витягуватиме поглиблену інформацію.

Комп'ютерний зір стає все більш важливим інструментом для аграрних підприємств у сучасному світі. Ця технологія використовується для моніторингу та управління виробничими процесами в сільському господарстві, що дозволяє оптимізувати виробництво та підвищувати його ефективність. Комп'ютерний зір може використовуватися для аналізу стану рослин, виявлення хвороб, шкідників або стресових умов. Високоточні камери та програмне забезпечення спроможні виявляти навіть найменші зміни в рослинах, що дозволяє оперативно реагувати на проблеми та зменшувати втрати врожаю. Завдяки комп'ютерному зорові можна автоматизувати процеси вирощування культур, визначати оптимальний час для поливу, внесення добрив чи захисту від шкідників. Це дозволяє зменшити використання ресурсів і збільшити врожайність. Комп'ютерний зір може допомагати аналізувати стан ґрунту на полях, виявляти його характеристики та потенційні проблеми. Це дозволяє вчасно коригувати агротехнічні заходи та використовувати ресурси з ефективністю. Також, за допомогою комп'ютерного зору можна автоматично визначати врожайність на полях, оцінювати якість та кількість врожаю, що допомагає планувати збирання та зберігання продукції. Гарним рішенням для аграрних підприємств є FarmBeats[3] від Microsoft, ця платформа використовує штучний інтелект, у тому числі комп’ютерне зір, щоб допомогти фермерам стежити за посівами, худобою та станом ґрунту. Він використовує аерофотознімки та датчики для надання інформації та рекомендацій щодо оптимізації роботи ферми.

Комп'ютерний зір – це динамічно розвиваюча галузь штучного інтелекту, яка має значний потенціал для зміни світу на краще. Ця технологія дає можливість комп'ютерам "бачити" та аналізувати візуальні дані, подібно до людей. Комп'ютерний зір вже зараз має значний вплив на різні галузі. З часом його вплив буде лише зростати, адже цю технологію можна використовувати для вирішення безлічі проблем.

Список використаних джерел

1. Prasol I. Method of Diagnostic Parameters Analysis and Software Features / I. Prasol, O. Dovnar, O. Yeroshenko // 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek). - 2022. - Pp. 716-719.

2. Fedorchenko V. Information Technology For Identification Of Electric Stimulating Effects Parameters / V. Fedorchenko, I. Prasol, O. Yeroshenko // CEUR Workshop Proceedings. - 2021. - 3200. - Pp. 189-195.

3. Improved safety with 3D thermal ranging for ADAS/AV applications [Електронний ресурс] / Chuck Gershman // Harvard – 2022 - Режим доступу до ресурсу: https://ui.adsabs.harvard.edu/abs/2022SPIE12107E..1OG/abstract

УДК 004.7 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.076

АЛГОРИТМ ОРГАНІЗАЦІЇ ВІДДАЛЕНОГО ДОСТУПУ ДО ЗАХИЩЕНОГО СЕГМЕНТУ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Чепурна І.С.
Науковий керівник – к. т. н., доц. Ткачов В.М.
Харківський національний університет радіоелектроніки, каф. ЕОМ,
м. Харків, Україна
e-mail: iryna.chepurna@nure.ua

The article considers the application of remote client access in corporate networks using VPN tunneling based on the Proxmox virtual environment. The problem of secure connection of remote users with the internal network of the enterprise through the use of virtualization and VPN technologies is investigated. Emphasis is placed on analyzing the effectiveness of using Proxmox virtualization technology to create secure connections and ensure secure access of remote users to corporate resources. The advantages of using Proxmox-based VPN tunneling in the context of ensuring confidentiality, integrity and availability of data in corporate networks are discussed.

Сучасний стан розвитку інформаційних технологій є двигуном у розвитку інформаційного суспільства. Зокрема, моделі організації IT-екосистем бізнесу та державного сектору відкриває все частіше стикаються з необхідністю побудови підходу до створення дистанційних робочих місць. Так, багато організацій застосовують рішення віртуальних приватних мереж для забезпечення безпеки зв'язку до таких робочих місць та призвані забезпечити умови безпечної роботи.

Одним із шляхів досягнення зазначених вище рішень є те, що, наприклад, під час локдаунів та проблема, яка виникла у потребі дистанційного доступу до ресурсів, може бути вирішена за рахунок створення віртуальних тунелів, які можуть бути створені з використанням технологій віртуалізації [1].

Розглядаючи популярні рішення віртуалізації мережних функцій, варто звернути увагу на VPN, як технологію створення захищених віртуальних тунелів між віддаленими вузлами мережі та кінцевими користувачами в мережі Інтернет. Під час передачі даних через такі віртуальні тунелі, вони шифруються, а пристрої відправника та отримувача маскуються, забезпечуючи безпечне з'єднання. Однак, основним недоліком такого рішення є зменшення швидкості передачі даних через процедури кодування та декодування [2].

Як відомо, застосування засобів віртуалізації надає значні переваги у розгортанні повноцінних мережних інфраструктур організацій для віддаленого доступу та в умовах обмеженого ресурсного забезпечення.

На рис. 1 зображено типову схему підключення мережного клієнта до корпоративної комп'ютерної мережі через OpenVPN-сервер, який з метою підвищення рівня відмовостійкості, розгортається на віртуальній машині. Віддалені користувачі можуть підключатися зі стаціонарних чи мобільних пристроїв до даного сервера. Враховуючи особливості транспортного середовища (проміжні мережі вендорів) можливі різні сценарії організації як тунелів, так і засобів, які забезпечують криптостійкість їх роботи.

В рамках даної роботи розглядається сценарій, де у якості мережного вузла виступає контейнер Proxmox, на якому безпосередньо розгортається OpenVPN-сервер. Загальнодоступна IP-адреса корпоративної комп'ютерної мережі дозволяє здійснити безпечне з'єднання від користувацького комп'ютера до мережного вузла. Таким чином,VPN-сервер виконує функції захищеного мережного шлюзу для доступу до захищеного сегменту корпоративної комп'ютерної мережі (рис. 1).

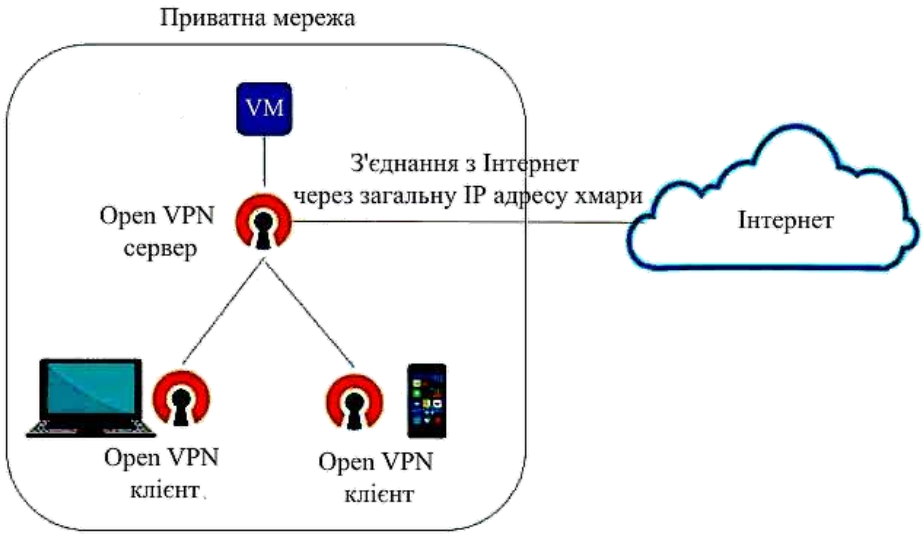


Рисунок 1 – Схема підключення користувачів через VPN-сервер до захищеного сегменту корпоративної комп'ютерної мережі

Налаштування VPN-серверу, формування сертифікатів для користувачів, адміністрування трафіку в даній схемі здійснюється за допомогою веб-інтерфейсу OpenVPN GUI [3].

Можливість використання в OpenVPN стандартних протоколів TCP і UDP дозволяє, наприклад, на відміну від IPsec обійти обмеження, коли Інтернет-провайдер або мережне обладнання, яке використовується, не підтримує або блокує відомі VPN-протоколи. За результатами проведених досліджень щодо використання OpenVPN в різних гетерогенних середовищах, встановлено, що найбільш відповідним для впровадження системи безпечного підключення віддалених користувачів до захищеного сегменту корпоративної комп'ютерної мережі є програмне забезпечення,

яке може мати як уніфіковані, так і не стандартні інтерфейси взаємодії із зовнішньою мережею. Рішення на основі OpenVPN-сервера відрізняється простотою адміністрування, здатністю читати сертифікати та приватні ключі найуживаніших операційних систем, використанням двосторонньої автентифікації сертифікату.

Віртуалізація цього рішення дозволяє розгорнути віддалений доступ до ресурсів корпоративної комп'ютерної мережі, забезпечуючи захист доступу та зменшуючи ймовірність несанкціонованого доступу до ресурсів мережі. Використання контейнерів Proxmox дозволяє встановлювати додаткові сервіси для обслуговування корпоративної комп'ютерної мережі в окремих контейнерах, що призводить як до економії апаратних ресурсів, так і до оптимального їх використання, а механізми віддаленого доступу у такій комбінації спрощують механізми їх взаємодії з віддаленими користувачами.

За результатами проведених досліджень та тестування реальної системи встановлено, що подібні рішення надають високий рівень доступності ресурсів для віддалених користувачів з урахуванням вимог безпеки та надійності. Подальші дослідження необхідно спрямувати на розробку дієвих механізмів мульти-VPN-з'єднань у агрегованих системах доставки контенту.

Список використаних джерел

1. Simon, M., Huraj, L. (2023). VirtualBox and Proxmox VE in Network Management: A User-Centered Comparison for University Environments. In: Silhavy, R., Silhavy, P. (eds) Networks and Systems in Cybernetics. CSOC 2023. Lecture Notes in Networks and Systems, vol 723. Springer, Cham. https://doi.org/10.1007/978-3-031-35317-8_44

2. Ткачов В.М. Застосування технології OpenVPN в рамках сервісу «Health Tracker» / В.М. Ткачов, А.О. Карасьов // 73-я науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів ОНАЗ ім. О.С. Попова, 12-14 грудня 2018 року. – Одеса. – 2018. – С. 157-158.

3. Ткачов В.М. Застосування технології OpenVPN в рамках сервісу «Health Tracker» / В.М. Ткачов, А.О. Карасьов // 73-я науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів ОНАЗ ім. О.С. Попова, 12-14 грудня 2018 року. – Одеса. – 2018. – С. 157-158.

4. Коваленко А.А. Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання / А.А. Коваленко, Г.А. Кучук, В.М. Ткачов // Системи управління, навігації та зв'язку. – Полтава: Полтавський національний технічний університет ім. Ю. Кондратюка, 2021. – № 1 (63). – С. 90-95.

УДК 004.8 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.079

УДОСКОНАЛЕННЯ СИСТЕМИ СОРТУВАННЯ НОМЕРІВ У ГОТЕЛЬНОМУ СЕРВІСІ

Чередниченко І.С.
Науковий керівник – к.т.н., доц. каф. КІТС Сердюк Н.М.
Харківський національний університет радіоелектроніки,
м. Харків, Україна
e-mail: ihor.cherednychenko@nure.ua

This work is devoted to improving the system of sorting rooms in the hotel service by using genetic algorithms (GA) and neural networks (NN) in order to improve efficiency and convenience for customers.

Artificial intelligence (AI) is increasingly becoming a part of our daily lives, and travel is no exception. The field of tourism is undergoing significant changes thanks to the progressive developments in the field of machine learning and data analysis. AI simplifies the process of finding and booking hotels, tickets and other services by providing recommendations based on travelers' preferences. Algorithms analyze a large volume of data and trip history, adapt the budget and individual wishes of the user, offering the best option as a result [1].

In the world of data science and software engineering, finding optimal solutions to complex problems is a constant challenge. Genetic algorithms (GAs) and neural networks (NNs) are two powerful techniques that have revolutionized the field of optimization. Optimization – is searching for values that minimize or maximize a given objective function. The objective function $h\theta$, also known as the prediction function, is the result of a preparation or training process. For example, in machine learning, when training artificial neural networks, the dependence of the network's output error on the state of its weights is used as the objective function to be minimized. In this case, will be the previously known network outputs.

Using neural networks is not a bad solution for optimization problems. A neural network – is a computational model inspired by the structure and function of the human brain. It consists of interconnected nodes, called neurons, organized into layers. Each neuron receives inputs, performs calculations, and produces an output. Neural networks are capable of learning from data and making predictions or decisions based on the learned patterns. Training a neural network involves adjusting the weights based on a learning algorithm, such as backpropagation, to minimize the difference between predicted outputs and the desired outputs. Once trained, a neural network can generalize and make accurate predictions on unseen data [2].

The process of booking a hotel room is simple, but quite responsible. It is at this stage that you will be able to choose the necessary amenities, type of

accommodation and room categories in the hotel. Often, an uncomfortable room, a terrible view from the window, or other minor inconveniences can spoil the vacation experience. To avoid such disappointments, it is important to take seriously the choice of hotel and the room itself at the very beginning of travel planning. In order to choose a suitable option, it is important to consider, first of all, the purpose and duration of the trip. If you are going to a specific country for more than a week, it is recommended to pay attention to rooms with a higher level of comfort. For a one-day stay in the country, the standard will be quite enough. A genetic algorithm will easily help you with this rather difficult choice [3].

A genetic algorithm is a search and optimization method inspired by the principles of natural selection and genetics. It simulates the process of evolution to find optimal solutions to complex problems. The algorithm starts with a set of potential solutions called individuals.

A genetic algorithm goes through a series of iterative steps, known as generations or iterations, to develop and improve the population. These steps include:

- Selection: Is based on their physical fitness, which shows how well they solve a problem;
- Crossover: exchanging genetic information or combining genes to create new ones;
- Mutation: random changes to maintain diversity and explore new areas of the search space;
- Evaluation: The fitness of the offspring is evaluated using a fitness function;
- Eliteness: The best individuals from the current population are preserved.

Through these steps, the genetic algorithm gradually improves the quality of the solutions until an optimal or near-optimal solution is found [4].

Список використаних джерел

1. How Artificial Intelligence can affect global tourism. URL: https://dip.org.ua/ turizm/stalo-vidomo-yak-shtuchnyy-intelekt-mozhe-vplynuty-na-svitovyy-turyzm/

2. Rudenko O.H., Bodyanskyi E.V. Artificial neural networks. - Kharkiv: SMIT Company LLC, 2006. - 156p.

3. Types of rooms in hotels. URL: https://travelyourway.com.ua/ua/planirovanie-samostoyatelnyh-puteshestvij/komfortnoe-prozhivanie/tipy-nomerov-v-otelyah/

4. Genetic Algorithm and Neural Network: A Powerful Combination for Optimization. URL: https://saturncloud.io/blog/genetic-algorithm-and-neural-network-a-powerful-combination-for-optimization/

УДК 004.7

NFC І APPLE PAY - ПОГЛЯД НА ЦИФРОВИЙ СВІТ

Чіві Я.В.
Науковий керівник – Правдіна О.М.
Харківський радіотехнічний фаховий коледж
м. Харків, Україна
e-mail: chiviyrik01@gmail.com

This work is devoted to NFC technology and its relationship with Apple Pay. Information technologies play a key role in the development and security of mobile payment systems like Apple Pay. Encryption mechanisms, biometric authentication, and NFC integration enable a high level of security and data protection for users.

Сучасний світ неможливо уявити без мобільних технологій. Смартфони стали невід'ємною частиною нашого життя, виконуючи функції не тільки звичайного телефону у вигляді засобу зв'язку, а й портативного комп'ютера, фотоапарата, гаманця і багатьох інших пристроїв.

Одним із лідерів у галузі мобільних платежів є Apple Pay - система від Apple, що дає змогу здійснювати покупки з iPhone, iPad і Apple Watch.

Розглянемо, як технології смартфонів змінюють наше уявлення про фінансові операції.

NFC (Near Field Communication) – це технологія бездротового зв'язку малого радіусу дії, що дозволяє пристроям обмінюватися даними на коротких відстанях. Вона ідеально підходить для мобільних платежів, де потрібен швидкий і безпечний обмін інформацією між смартфоном і платіжним терміналом. [1]

Як працює NFC:

1. Ініціатор: Смартфон з підтримкою NFC, який виступає ініціатором транзакції, генерує радіочастотне поле.
2. Встановлення зв’язку: NFC-термінал і другий пристрій встановлюють зв’язок між собою. Для цього вони кілька секунд повинні розташовуватися на відстані до 10 см один від одного.
3. Обмін даними: Відбувається обмін зашифрованими даними, включно з інформацією про платіжну картку, суму транзакції та інші необхідні відомості.
4. Обробка платежу: після зчитування всіх необхідних даних із другого пристрою запускається стандартна транзакція у платіжній системі. Платіжний провайдер відправляє запит на списання коштів у банк-еквайр, той перевіряє валідність платіжних даних клієнта і надсилає запит у банк-емітент і так далі. Після проходження всіх етапів здійснюється операція зняття коштів із рахунку.

5. Підтвердження та завершення: в разі успішного платежу NFC-термінал підтверджує операцію оплати на екрані термінала та/або на пристрої платника. [1]

Інформаційні технології в галузі мобільних платежів використовуються для захисту конфіденційної інформації користувачів, таких як дані кредитних карт. Це включає в себе шифрування даних і зберігання інформації в захищеному вигляді на мобільних пристроях.

Ключова особливість Apple Pay – безпека та підхід до неї. Система оплати від Apple використовує технологію Secure Element.

Secure Element (SE) – захищений мікроконтролер, інтегрований безпосередньо в пристрої Apple. Він забезпечує безпеку ваших платіжних даних, роблячи мобільні платежі не тільки зручними, а й надійними.

Під час додавання картки, ваші банківські дані не зберігаються на серверах Apple. Замість цього SE генерує унікальний код (токен), який використовує для здійснення платежу. Тобто коли ви здійснюєте оплату, продавець не отримує повну інформацію про платіжну картку, а тільки динамічний код (одноразовий токен). [2]

NFC буде використовуватися не тільки для оплати товарів і послуг, а й для: контролю доступу: у будівлі, транспорт, офіси; ідентифікації: перевірка справжності товарів, документів, квитків; обміну даними: контакти, посилання, фотографії, файли; підключення пристроїв: до розумних будинків, переносних пристроїв, IoT-пристроїв. [3]

Загалом, майбутнє Apple Pay і технології NFC залишається світлим і сповненим можливостей, і ми можемо очікувати, що вони й надалі розвиватимуться, щоб задовольнити потреби й очікування користувачів у цифровій епосі.

Apple Pay і технологія NFC міцно увійшли в наш цифровий світ, змінюючи способи, якими ми здійснюємо платежі і взаємодіємо з фінансовими сервісами. Їхній вплив виходить далеко за рамки простого полегшення процесу оплати, зачіпаючи безпеку, зручність та інновації у сфері фінансових технологій.

Таким чином, можна зробити висновок, що Apple Pay і технологія NFC відіграють важливу роль у сучасному цифровому світі, надаючи користувачам зручні, безпечні та інноваційні способи здійснення платежів. Їхній вплив продовжуватиме зростати, відкриваючи нові можливості.

Список використаних джерел:

1. NFC-термінал із телефона: як приймати платежі через NFC.
URL: https://fondy.ua/ru/knowledge/nfc-terminal/

2. Apple Pay: безпечні та зручні оплати.
URL: https://blog.easypay.ua/ru/apple-pay-bezopasnyie-i-udobnyie-oplatyi/

3. Apple Pay And The Future Of Payments.
URL:https://gadgetmates.com/apple-pay-and-the-future-of-payments

УДК 004.8:519.816 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.083

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ АЛГОРИТМІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОГНОЗУВАННЯ ТА ВІДСТЕЖЕННЯ ПОБІЧНИХ ЕФЕКТІВ ЛІКАРСЬКИХ ЗАСОБІВ

Швиденко А.О.
Науковий керівник – к.т.н., доц. Сердюк Н.М.
Харківський національний університет радіоелектроніки, каф. КІТС, м. Харків, Україна
e-mail: alina.shvydenko@nure.ua

This work studies the use of artificial intelligence (AI) algorithms for predicting and monitoring the side effects of medicinal drugs. The first algorithm considers the use of a Geometric Self Expressive Model (GSEM) with data from the SIDER and OFFSIDES databases. In GSEM, the focus is on a matrix approach to predict the likelihood of drug side effects. It is also proposed to use the AI algorithm in post-clinical observation and in collecting patient data from social networks and forums for discussion. This research demonstrates the potential of AI as a complement to traditional methods with the aim of enhancing the safety of medical treatment.

Для кожного нового лікарського засобу виникає необхідність у виявленні його побічних ефектів. Задля їх виявлення лікарський засіб проходить стадії передклінічних та клінічних досліджень, під час яких вчені спостерігають за впливом засобу на контрольні групи [3]. Проте, через обмеження в часі та у виборі учасників контрольних груп, такі дослідження можуть виявити лише частину побічних ефектів. Багато ж інших побічних ефектів виявляються вже після надходження препарату до медичних закладів шляхом відстеження звернень пацієнтів.

Використання алгоритмів штучного інтелекту (ШІ) для прогнозування можливих побічних ефектів лікарських засобів ще до їх надходження до медичних закладів може значно покращити результати досліджень, а отже, й підвищити безпечність препарату.

З такою ціллю розроблені спеціалізовані системи машинного навчання. У статті [2] міжнародна група дослідників створила та використала розумну технологію під назвою геометрична модель, що саморозвивається (Geometric Self Expressive Model - GSEM) для навчання ШІ. Як результат, було виявлено 904 побічних ефектів на 505 лікарських засобів.

Вхідними даними є матриця препаратів/побічних ефектів. Навпроти кожного препарату (рядку) стоять одиниці для тих побічних ефектів (колонок), що були виявлені під час клінічних досліджень, усі інші клітинки заповнюються нулями. Вихідними даними є така сама матриця препаратів/побічних ефектів, за тією відмінністю, що вихідна матриця замість нульових значень містить вірогідності того, що конкретний препарат може мати певний побічний ефект.

Для навчання таких алгоритмів використовуються дані із відкритих медичних джерел, таких як SIDER та OFFSIDES. Ці бази даних містять обширні дані про побічні ефекти препаратів отримані під час клінічних досліджень та після виходу препарату на ринок відповідно. Інформація про ліки, що включають їх хімічну структуру, а також анатомічну та терапевтичну класифікацію отримується за допомогою використання DrugBank, MACCS та RDKit.

На основі вихідних даних та отриманих даних про ліки і побічні ефекти, є можливим розрахувати значення, що являють собою математичні моделі саморепрезентації лікарських засобів та побічних ефектів. Ці дві моделі дають змогу розрахувати вихідну шукану матрицю вірогідностей.

Алгоритми ШІ також можуть бути використані для покращення спостереження за препаратом, що вже знаходиться у використанні. До описаної системи машинного навчання можна додати нові дані, отримані вже після клінічних досліджень, що дає можливість скорегувати прогнози.

Іншим корисним вектором використання автоматичних систем та ШІ можуть бути спеціалізовані системи для допомоги у зборі нових даних про побічні ефекти ліків, що перебувають у використанні. Велика кількість пацієнтів при зіткненні з неочікуваними побічними ефектами часто обговорюють їх на форумах чи у групах в соціальних мережах. Ці дані можуть автоматично збиратися, використовуючи ШІ для виявлення та класифікації [1]. Після цього, також при його використанні, зібрані дані можуть оброблятися з цілями відокремлення ключових даних, таких як: вік та стать пацієнта, обставини та опис ефекту. Оброблені дані можуть бути відправлені вченим для подальшого дослідження.

Використання алгоритмів ШІ у прогнозуванні побічних ефектів лікарських засобів має великий потенціал для підвищення безпеки пацієнтів і ефективності лікування. Розглянуті алгоритми ШІ можуть слугувати доповненням до основного способу виявлення побічних ефектів.

Список використаних джерел:

1. AI in pharma: quickly predict drug side effect in 2024. *DevsData LLC - Premium IT Recruitment Agency and Software Development Services*. URL: https://devsdata.com/artificial-intelligence-pharma-drug-side-effect/ (date of access: 21.02.2024).

2. Galeano D., Paccanaro A. Machine learning prediction of side effects for drugs in clinical trials. *Cell reports methods*. 2022. Vol. 2, no. 12. URL: https://www.sciencedirect.com/science/article/pii/S2667237522002557 (date of access: 22.02.2024).

3. Inside clinical trials: testing medical products in people. *U.S. Food and Drug Administration*. URL: https://www.fda.gov/drugs/information-consumers-and-patients-drugs/inside-clinical-trials-testing-medical-products-people (date of access: 22.02.2024).

УДК 004.7

ВИКОРИСТАННЯ МОБІЛЬНИХ ТЕХНОЛОГІЙ У СФЕРАХ ПРОМИСЛОВОСТІ ТА БІЗНЕСУ

Штонда О.А.
Науковий керівник – Радченко О.П.
Харківський радіотехнічний фаховий коледж
м. Харків, Україна
e-mail: tatar7681@gmail.com

This article is about usage of mobile technologies in the spheres of industry and business. It is about the latest information technologies, which are used in business and industry. It contains description about CIT, CASE, OLAP, Intranet technologies. Essence of methods and their purpose is described.

У сучасному світі мобільні технології знайшли своє місце у різних сферах людського життя. Інформаційно-комунікаційні технології знаходять своє застосування в науці, промисловості, торгівлі, управлінні, банківській системі, освіті, медицині, транспорті, зв'язку, сільському господарстві, системі соціального забезпечення та інших галузях.

В наш час, широкого поширення набули корпоративні інформаційні системи (КІС). Системи базуються на принципах корпоративних інформаційних технологій, а саме:

- формування звітних показників, одержуваних на основі стандартної бухгалтерської та статистичної звітності;
- вироблення стратегічних управлінських рішень з розвитку бізнесу на основі бази високоагрегірованних показників;
- вироблення тактичних рішень, спрямованих на оперативне управління і вирішуються на основі бази приватних, високо деталізованих показників, що відображають різні сторони локальних характеристик функціонування структури. [1]

Управлінські процеси, тобто менеджмент, є невід'ємною частиною будь-якого виробничого процесу. Для сфери бізнесу важливо отримання позитивних результатів, це є однією з складових успішної роботи будь-якого бізнесу. Основна мета менеджменту – це досягнення високої ефективності виробництва, кращого використання ресурсного потенціалу підприємства, фірми, компанії. [2]

Сучасні розробки інформаційних систем менеджменту просуваються вперед досить успішно, застосовуючи технології інформаційних систем та комунікацій. Завдяки цьому інформаційні системи менеджменту стали задовольняти зростаючі вимоги менеджерів до забезпечення інформацією. Головними критеріями в оцінці інформаційних систем стали достовірність, своєчасність, повнота та корисність інформації для прийняття рішень. [3]

Найбільш поширені технології в галузі бізнесу є:

- CASE-технологія.

– Технологія OLAP.
– Intranet-технологія.

CASE-технологія – це сукупність методологій аналізу, проектування, розробки й супроводження складних систем програмного забезпечення, підтримана комплексом взаємозв’язаних засобів автоматизації. CASE надає системним аналітикам, проектувальникам і програмістам інструментарій для автоматизації проектування і розробки ПЗ. Процес створення ПЗ з застосуванням CASE-засобів має такі переваги, як підвищення якості ПЗ завдяки використанню засобів автоматичного контролю проекту; прискорення процесу проектування і розробки; позбавлення розробника рутинної роботи, надаючи йому можливість зосередитись на творчій частині розробки.

Технологія оперативного аналітичного оброблення даних (OLAP) була виокремлена як особливий підхід до обробки даних у зв’язку з появою спеціальних засобів збереження та аналізу накопичених облікових даних. OLAP-програми являють собою сукупність засобів багатовимірного аналізу даних, накопичених у сховищі даних. Системи на основі OLAP дають змогу аналітикам і менеджерам, що потребують оперативного прийняття рішень, досягти розуміння процесів, що відбуваються на підприємстві, шляхом швидкого інтерактивного доступу до даних у сховищі і виконання над ними різноманітних аналітичних операцій: зрізів, поворотів, згорток, розгорток, проекцій тощо.

Технологія intranet розуміє під собою створення локальної інформаційної системи клієнт-серверної архітектури та забезпечує високу пропускну здатність каналів зв'язку між клієнтом і сервером й використання як стандартних серверів і клієнтів, так і стандартних механізмів розширення можливостей системи, наприклад CGI. Системи intranet є значно дешевшими порівняно зі спеціалізованими клієнт-серверними прикладними програмами. [4]

Список використаних джерел

1. Інформаційні технології в промисловості та економіці URL: https://stud.com.ua/59742/informatika/informatsiyni_tehnologiyi_promislovosti_ekonomitsi.
2. Сучасні технології у виробничій діяльності людини. URL: https://disted.edu.vn.ua/courses/learn/3124
3. Ступницький О. Інформаційні технології та корпоративне управління у XXI ст. // Економіка України. – 2005. – № 2. – С. 38–46.
4. Інформаційні технології в менеджменті URL: https://kerivnyk.info/2012/05/mykolyshyn.html

УДК 004.946:[004.6+004.7]

ЗАХИСТ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ РЕСУРСІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ (ІКС)

УДК 004.056 https://doi.org/10.30837/IYF.PCEIP.2024.088

ВИКОРИСТАННЯ МЕТОДІВ, МЕХАНІЗМІВ ТА ЗАСОБІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ПРИКЛАДІ ЗАХИСТУ БІОМЕТРИЧНИХ ДАНИХ

Бабаєва К. Г. гизи
Науковий керівник – к.т.н. Мельникова О. А.
Харківський національний університет радіоелектроніки, каф. БІТ, м. Харків, Україна
e-mail: kamila.babaieva@nure.ua

Information plays a key role in our lives nowadays. Methods, mechanisms and ways for cryptographic information protection allow us to safely store, transmit, and verify information transferred to us. Since, for example, confidential or personal information needs to be protected from being obtained by third parties who can use it for their own purposes. And the life and fate of all people may depend on this information. Nowadays, there are a huge number of methods, mechanisms and ways to protect information. Confidential information must be protected from being leaked or published because it can cause great harm to the owner of the information or to those who disclosed it.

Найважливішим елементом сучасного життя є інформація. Інформація буває відкритою або конфіденційною. Важливість інформації підтверджує вислів Н. Ротшильда: “Хто володіє інформацією, той володіє світом!”. Конфіденційну інформацію потрібно захищати від витоку або публікування, тому що це може нанести велику шкоду власнику такої інформації або тим, хто її передав.

З новими стрімкими технічними проривами, ми отримуємо все більше інформації, яку потрібно зберігати та захищати. Зокрема, це біометричні дані людей, які зараз використовуються, починаючи з безкодового доступу до телефону, комп’ютеру, квартири, дому, закінчуючи підтвердженням оплати рахунків. Наприклад, у Китаї використовують біометричні дані (скан обличчя) для оплати у магазинах. Всю цю інформацію потрібно надійно зберігати, для цього використовується криптографічний захист інформації (шифрування).

Біометричні дані, такі як скани обличчя, відбитки пальців, структура рук чи голос, є важливими елементами в сучасних системах ідентифікації та автентифікації [1, 2]. Вони використовуються для забезпечення вищого рівня безпеки в різних сферах, включаючи фінанси, охорону здоров'я, урядові послуги та багато інших. Проте, захист цих біометричних даних є критично важливою задачею з погляду конфіденційності та цілісності особистої інформації.

Існує багато методів, механізмів та засобів криптографічного захисту інформації: апаратні, програмні та апаратно-програмні системи та комплекси, що реалізують криптографічні алгоритми перетворення.

Основна мета КЗІ полягає в тому, щоб забезпечити високий рівень захисту інформації від несанкціонованого доступу та змін, що можуть спричинити порушення конфіденційності, цілісності або доступності даних [3]. Це особливо важливо в сферах, де обробка та передача конфіденційної інформації є критичною, таких як фінанси, медицина, урядові служби та багато інших.

До засобів криптографічного захисту інформації (КЗІ) можна віднести наступне.

1. Засоби, призначені для виготовлення ключових даних або документів (незалежно від виду носія ключової інформації) та управління ключовими даними, що використовуються в засобах криптографічного захисту інформації.

2. Засоби захисту від нав'язування неправдивої інформації або захисту від несанкціонованої модифікації, що реалізують алгоритми криптографічного перетворення інформації (криптоалгоритми), включаючи засоби імітозахисту та електронного цифрового підпису.

3. Засоби захисту інформації від несанкціонованого доступу (у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки), у яких реалізовані криптоалгоритми.

У засобах КЗІ повинні бути реалізовані різні механізми для контролю та захисту інформації, ось деякі з них:

1) механізми контролю цілісності криптографічних перетворень та захисту ключових даних;

2) механізми захисту від порушення конфіденційності інформації внаслідок помилкових дій оператора, або в разі відхилень у роботі складових елементів засобу КЗІ;

3) механізми розмежування доступу до функцій засобу КЗІ, криптографічної схеми та ключових даних;

4) довірений канал для отримання інформації, що підлягає захисту;

5) механізми знищення ключових даних після закінчення строку їх дії;

6) механізми захисту ключових даних на їх носіях від несанкціонованого зчитування;

7) механізми захисту від порушення конфіденційності та цілісності ключових даних;

Можна вказати наступні криптографічні засоби захисту, які обов’язково використовуються при передачі та зберіганні інформації.

1. Шифрування. Перетворення інформації з використанням ключа для обмеження доступу до неї тільки авторизованим особам, які володіють ключем.

2. Цифровий підпис. Дозволяє визначити, якою саме особою або системою було підписано інформацію, а також підтвердити цілісність інформації.

3. Гешування даних. Використовується для створення унікального геш-коду з вхідних даних за допомогою геш-функцій. Цей геш-код служить для перевірки цілісності даних, оскільки будь-яка зміна вихідних даних призведе до зміни геш-коду.

4. Контроль доступу. Використовується для регулювання доступу до конфіденційної інформації, використовуючи різноманітні механізми, такі як ролі користувачів, політики доступу, аудит доступу та інші.

Для безпечного збереження та передачі конфіденційних, приватних біометричних даних, необхідно використовувати усі механізми, засоби та методи криптографічного захисту інформації (КЗІ). Це означає, що біометричні дані, такі як скан обличчя, повинні бути збережені у зашифрованому вигляді.

Крім того, важливо зберігати геш-коди розшифрованих даних, щоб після розшифрування можна було перевірити цілісність інформації. При передачі навіть зашифрованих біометричних даних важливо використовувати електронний цифровий підпис (ЕЦП), щоб забезпечити їхню автентичність та недоторканість під час передачі через мережу. Це дозволить перевірити, що дані не були змінені або підроблені під час передачі.

Крім застосування криптографічних методів, важливо забезпечити безпеку в процесі збору, зберігання та обробки біометричних даних. Це означає, що пристрої, які збирають біометричні дані, повинні бути захищені від несанкціонованого доступу та фізичної атаки.

У сучасному світі, де біометричні технології широко використовуються в різних сферах, важливо постійно вдосконалювати заходи захисту біометричних даних із урахуванням швидкого розвитку технологій та змін у загрозах кібербезпеки.

Тільки таким чином можна забезпечити високий рівень безпеки та довіру до систем, які використовують біометричні дані.

Список використаних джерел

1. Мироненко Є.В., Сєвєрінов О.В. Біометрична ідентифікація і автентифікація особи за геометрією обличчя. НТУ «ХПІ», 2020.

2. Gvozdov Roman et al. "Method of Biometric Authentication with Digital Watermarks." 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). IEEE, 2021.

3. Про затвердження Вимог до засобів криптографічного захисту інформації, призначених для захисту таємної інформації, яка не становить державної таємниці, та конфіденційної інформації в державних органах, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, військових формуваннях, які створені відповідно до закону : Наказ Адмін. Держ. служби спец. зв'язку та зах. інформації України від 07.05.2021 р. № 278. URL: https://zakon.rada.gov.ua/laws/show/z0696-21#Text (дата звернення: 05.03.2024).

УДК 004.056:355.4511:004.75 https://doi.org/10.30837/IYF.PCEIP.2024.091

SQL ІН'ЄКЦІЯ: ЗАГРОЗА БЕЗПЕЦІ ВЕБ-ЗАСТОСУНКІВ

Блінна В.С.
Науковий керівник – ст., викл. В'юхін Д.О.
Харківський Національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: veronika.blinna@nure.ua

This work is devoted to exploring the threat of SQL Injection to the security of web applications. Five major types of SQL injection attacks were reviewed, their methodologies and potential impact on system integrity were examined. The paper delineates the consequences of a successful SQL Injection attack, highlighting the severity of the threat it poses to web application security. Additionally, the significance of implementing robust security measures and defenses to effectively mitigate the risks associated with SQL Injection vulnerabilities in web applications is emphasized.

У сучасному цифровому світі веб-додатки відіграють ключову роль у забезпеченні доступу до даних і виконанні різних операцій. Однак, разом із розширенням функціоналу веб-додатків зростає і рівень загроз безпеки. Одним із поширених методів атак є SQL ін'єкція, що становить серйозну загрозу для даних.

Метою доповіді є розгляд вразливостей SQL-запитів. SQL-ін'єкція - це вразливість веб-безпеки, яка дозволяє зловмиснику втручатися в запити, які додаток робить до внутрішньої бази даних. Як правило, це дає змогу переглядати дані, які він зазвичай не може отримати. Це можуть бути інші користувачі, або будь-які інші дані, доступ до яких має сам додаток [1]. У багатьох випадках зловмисник може змінювати або видаляти ці дані, викликаючи постійні зміни у вмісті або поведінці програми.

SQL-ін'єкції потребують мінімальних навичок і найчастіше не потребують будь-яких спеціальних програм. Зловмисник просто вводить в адресний рядок потрібні значення і отримує доступ до даних, а іноді й адміністративні права на базу даних [2]. За допомогою цих атак зломщик може отримати дані про конфіденційну інформацію. При цьому структура таблиць не порушується, і виявити злом можна тільки в разі зміни (зловмисником) чогось на сайті або в паролі. Існує 5 основних типів SQL ін'єкцій [3]:

1. Класична (In-Band або Union-based) [4]. Найнебезпечніша і найрідкісніша сьогодні атака. Дає змогу відразу отримувати будь-які дані з бази. У цьому методі хакер використовує результати з бази даних і зламує базу даних, щоб досягти мети. Це також називається внутрішньо смуговою ін'єкцією SQL.

2. На основі помилок (Error-based). Дає змогу отримувати інформацію про базу, таблиці та дані на основі виведеного тексту помилки СУБД. У цьому типі впровадження хакер аналізує різні операції і знаходить зразок помилки в базі даних. Потім він/вона отримує доступ до нього, щоб зламати/пошкодити базу.

3. Булева сліпа атака (Boolean-based). Замість отримання всіх даних, зловмисник може поштучно їх перебирати, орієнтуючись на просту відповідь типу true/false.

4. Сліпа атака, заснована на часі (Time-based). Схожа на попередню атаку принципом перебору, маніпулюючи часом відгуку бази. Атакуючі направляють SQL-запит до бази даних, змушуючи її зробити затримку на кілька секунд, перш ніж вона підтвердить або спростує отриманий запит.

5. Поза смугове впровадження (Out-of-Band). Дуже рідкісні та специфічні типи атак, засновані на індивідуальних особливостях баз даних. Така атака відбувається у двох випадках: коли атакуючі не можуть провести атаку і зібрати дані через один і той самий канал зв'язку, або коли сервер працює занадто повільно чи нестабільно, щоб досягти потрібного результату.

Успішна атака на основі SQL-ін'єкції може мати серйозні наслідки для бізнесу, крім розкриття конфіденційних даних, атака також може призвести до отримання зловмисниками адміністративного доступу до системи, з можливістю втручання в її функціонування. Водночас можливе порушення приватності користувачів, включно з розкриттям адрес, номерів телефонів і відомостей про банківські картки, що спричинить фінансові втрати та втрату довіри з боку клієнтів.

Для запобігання SQL-ін’єкціям критично важливо впроваджувати комплексні стратегії безпеки. По-перше, слід використовувати параметризовані запити, що дозволяють передавати значення окремо від запиту та автоматично екранувати спеціальні символи, таким чином запобігаючи впровадженню шкідливого коду. Крім того, важливо проводити валідацію всіх введених даних перед їх використанням у запитах, щоб запобігти можливим атакам. Необхідно також належно керувати привілеями доступу до бази даних для уникнення несанкціонованого доступу та злому системи. Використання об'єктно-реляційних маперів (ORM) може додатково забезпечити захист від SQL-ін'єкцій, оскільки вони автоматично генерують безпечні запити на основі об'єктів моделей даних. Не менш важливим є регулярне оновлення бази даних, програмного забезпечення та бібліотек з метою виправлення вразливостей та недоліків, включаючи потенційні ін'єкції, тим самим забезпечуючи максимальний рівень безпеки веб-додатка.

Однак, додавання додаткових перевірок або постійних перевірок запитів може сповільнити роботу сайту. Це через те, що система буде витрачати

додатковий час на виконання цих перевірок перед обробкою запитів. Таким чином, існує дилема: ми можемо забезпечити високий рівень захисту від SQL-ін'єкцій за рахунок сповільнення роботи сайту, оскільки він постійно проводитиме перевірки та оновлення даних, або ми можемо робити сайт швидким, але менш безпечним, залишаючи деякі ризики.

Прикладом такої ситуації є Denuvo Anti-Tamper[5], яка була розроблена австрійською компанією Denuvo Software Solutions GmbH. Ця технологія використовується для захисту від несанкціонованого доступу до комп'ютерних ігор та програм. Вона запобігає піратству шляхом ускладнення процесу копіювання та модифікації програмного коду. Проте, використання Denuvo може призвести до деякої затримки в роботі гри або програми, оскільки система постійно перевіряє їх автентичність під час виконання. Таким чином, вона впливає на продуктивність, крім того, може спричинити незручність через довгий час завантаження або затримки під час гри, проте забезпечує високий рівень захисту від несанкціонованого доступу.

Отже, SQL-ін'єкції являють собою серйозну загрозу безпеці інформаційних систем, оскільки вони дають змогу зловмисникам несанкціоновано отримувати доступ до баз даних і впливати на дані. Такий тип атак може призвести до втрати конфіденційної інформації, порушення цілісності даних і впливу на доступність системи. Розуміння різних видів цих атак та їхніх можливих наслідків є важливим кроком для запобігання таким атакам і забезпечення безпеки інформаційних систем. Окрім цього, провадження комплексних стратегій безпеки, таких як використання параметризованих запитів, валідація даних і керування привілеями доступу, є критично важливими для запобігання SQL-ін'єкціям і забезпечення безпеки веб-додатків. Проте, додаткові перевірки запитів можуть призвести до сповільнення роботи сайту, створюючи дилему між високим рівнем захисту та продуктивністю.

Список використаних джерел

1. Clarke J. SQL Injection Attacks and Defense. Elsevier Science & Technology Books, 2009. 496 p.
2. Imperva.What is SQL Injection. SQL (Structured query language) Injection, 2023. URL: https://www.imperva.com/learn/application-security/sql-injection-sqli/(дата звернення: 20.01.2024).
3. Ettore Galluccio, Edoardo Caselli, Gabriele Lombari. SQL Injection Strategies. Packt Publishing, 2020. 210 p.
4. Ляшко М. С. Безпека даних в веб-додатках: як захистити від Union-based SQL Injection / М. С. Ляшко, Д. О. В'юхін // Проблеми інформатизації : тези доповідей одинадцятої міжнар. наук.-техн. конф., 16–17 листопада 2023 р. – Баку–Харків–Бельсько-Бяла, 2023. – Т. 2, секція 3,6. – С. 67.
5. Denuvo. The global #1 Games Protection and Anti-Piracy technology, 2023. URL: https://irdeto.com/denuvo/(дата звернення: 05.02.2024)

УДК 004.056

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ СТОРОННЬОГО ДОСТУПУ ТА ЗАХИСТУ IP КАМЕР

Веселовський О.Г.
Науковий керівник – ст. викладач кафедри БІТ Данилов А.Д.
Харківський національний університет радіоелектроніки, каф. БІТ, м. Харків, Україна
тел.: +38(099)-441-96-64, e-mail: oleksii.veselovskyi@nure.ua

The paper provides a comprehensive analysis of methods for detecting and protecting IP cameras from unauthorized access. Focusing on the use of intrusion detection systems and artificial intelligence algorithms, the author examine their effectiveness and limitations in the context of modern cyber threats. In addition, they analyze security measures such as the use of strong passwords, encryption, and virtual private networks. The paper highlights the need for further research and development in this area to effectively counter the ever-increasing cyber threats to IP camera security.

З поширенням IP-камер в сферах громадської безпеки, домашньої безпеки і промислового відеоспостереження, забезпечення їх захисту від несанкціонованого доступу стало важливим завданням. IP-камери відіграють важливу роль у системах відеоспостереження, забезпечуючи можливість моніторингу та запису в режимі реального часу, також пропонують розширені функціональні можливості, такі як віддалений моніторинг і хмарне зберігання, проте мають свої вразливості, якими можуть скористатися зловмисники. Несанкціонований доступ до цих камер не тільки ставить під загрозу приватність осіб, а й створює значні ризики для безпеки організації.

В роботі проведено аналіз методів виявлення несанкціонованого доступу та захисту IP-камер. У сучасному світі, де кіберзагрози продовжують розвиватися, вкрай важливо вживати надійних заходів безпеки для захисту цілісності та конфіденційності відеозаписів з камер. Вивчаючи існуючі методи і нові технології, ми маємо на меті дати уявлення про ефективність, обмеження і потенційні можливості вдосконалення існуючих механізмів безпеки, розгорнутих в системах IP-камер.

Одним з основних методів виявлення стороннього доступу є використання систем виявлення вторгнень (СВВ). Ці системи відстежують мережевий трафік на предмет підозрілих дій і видають сповіщення, коли такі дії виявляються. Незважаючи на те, що СВВ ефективні у виявленні відомих загроз, вони можуть бути не настільки ефективними у виявленні нових, невідомих загроз [1].

Іншим методом виявлення стороннього доступу є використання алгоритмів штучного інтелекту (ШІ) та машинного навчання (МН). Ці алгоритми можуть аналізувати закономірності мережевого трафіку та виявляти аномалії, які можуть свідчити про стороннє вторгнення. Перевага алгоритмів ШІ та МН полягає в тому, що вони здатні адаптуватися і вчитися на нових загрозах, що робить їх потенційно більш ефективними, ніж традиційні СВВ [2].

Що стосується методів захисту IP-камер, то одним із поширених підходів є використання надійних, унікальних паролів і регулярне оновлення паролів. Це може запобігти несанкціонованому доступу до каналу IP-камери. Крім того, використання шифрування може захистити дані, що передаються з IP-камери, запобігаючи їх перехопленню та перегляду третіми особами [1].

Використання віртуальних приватних мереж (VPN) може забезпечити додатковий рівень безпеки. VPN створюють безпечне, зашифроване з'єднання через Інтернет, яке може захистити канал IP-камери від перехоплення [2].

Ще одним ефективним методом захисту IP-камер є використання систем виявлення та запобігання вторгнень. Ці системи можуть виявляти і запобігати поширенню шкідливих програм на терміналах користувачів і цифрових відеореєстраторах [3].

Шифрування даних також є важливим аспектом захисту IP-камер. Всі відеопотоки, а також така інформація, як імена користувачів і паролі, повинні бути зашифровані, щоб захистити дані, що передаються, особливо якщо вони проходять через Інтернет. Найпоширеніші варіанти шифрування включають SSL/TLS для інформації про користувача та IPsec або MACsec для даних. Належне шифрування допомагає запобігти підслуховуванню та маніпуляціям з пакетами, які можуть відбуватися під час атак типу "людина посередині" (MitM) [3].

У роботі проведено аналіз методів виявлення та захисту IP-камер від несанкціонованого доступу. Подальше вдосконалення і застосування методів захисту може значно підвищити безпеку систем відеоспостереження з використанням IP-камер.

Список використаних джерел:

1. Biondi P., Bognanni S., & Giampaolo B. Vulnerability Assessment and Penetration Testing on IP cameras. *Universita di Catania.* 2022

2. Kalbo, N., Mirsky, Y., Shabtai, A., & Elovici, Y. The Security of IP-Based Video Surveillance Systems. *Sensors.* 2020

3. 5 Ways to Protect IP Video Surveillance Systems. Allied Telesis : вебсайт URL: https://www.alliedtelesis.com/be/en/blog/5-ways-protect-ip-video-surveillance-systems (дата звернення: 04.03.2024)

УДК 004.7.032.2:004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.096

ФІНАНСОВІ ОРГАНІЗАЦІЇ, ЗАСНОВАНІ НА БЛОКЧЕЙН-РОЛАПАХ НА БАЗІ ДОКАЗІВ ІЗ НУЛЬОВИМ РОЗГОЛОШЕННЯМ

Гаража Р.Ю.
Науковий керівник — к.т.н. Мельникова О.А.
Харківський національний університет радіоелектроніки, каф. БІТ
м. Харків, Україна
e-mail: roman.harazha@nure.ua.

This work is devoted to the research of the potential of accounting systems of financial organizations, implemented with the help of zero-knowledge blockchain rollups. Such accounting systems will allow to combine the positive qualities of traditional accounting systems and decentralized accounting systems based on the blockchain. To do this, it is necessary to use the following set of technologies: a blockchain-based accounting system, a decentralized consensus protocol, an EVM-like virtual computing environment, zero-knowledge blockchain rollups to ensure information security and low transaction costs.

Зважаючи на прогрес у галузі блокчейн-технологій, втілення банківських та інших фінансових систем на їх базі стає все більш надійним рішенням для забезпечення цілісності банківських (фінансових) даних. При цьому окремі невід'ємні якості децентралізованих облікових систем на базі блокчейну сповільнюють їх впровадження у банківському секторі. Серед таких — доступність даних, що в традиційних банківських системах є приватними (баланси і транзакції користувачів), а також висока вартість оновлення стану системи в популярних децентралізованих облікових системах, таких як Bitcoin та Ethereum.

З іншого боку, вже існують рішення, що дозволяють значно зменшити вартість оновлення стану системи. Саме до таких рішень відносяться блокчейн-ролапи (англ. Blockchain Rollups) та їх модифікація — блокчейн-ролапи на базі доказів із нульовим розголошенням (англ. Zero-Knowledge Blockchain Rollups), які здатні забезпечити приватність транзакцій.

Блокчейн — база даних у формі зв'язного списку блоків даних. Зазвичай зв'язність забезпечується не лише за допомогою порядкових номерів блоків, а й за допомогою геш-суми, що міститься у кожному блоці разом із геш-сумою попереднього блоку. Таким чином, зміна вмісту блоку призводить до зміни його геш-суми і розриву списку, що допомагає у перевірці цілісності даних. Блокчейн зазвичай лежить в основі децентралізованих облікових систем, що мають свої протоколи досягення консенсусу (Proof-of-Work, Proof-of-Stake, Proof-of-Authority та ін.) щодо стану облікової системи.

EVM (Ethereum Virtual Machine) — віртуальне обчислювальне середовище, що лежить в основі децентралізованої облікової системи Ethereum. У цьому середовищі виконуються смарт-контракти та зберігаються дані, що є результатом їх виконання (при цьому виконання смарт-контрактів вимагає витрати нативної валюти системи Ethereum). Мова програмування смарт-контрактів Solidity є повною за Тюрінгом і дозволяє втілення наскільки завгодно складних операцій над отриманими смарт-контрактом даними. Облікова система Ethereum стала основою для багатьох застосунків у сфері децентралізованих фінансів (DeFi).

Доказ із нульовим розголошенням (англ. Zero-Knowledge Proof) — тип доказу, який дозволяє одній стороні довести істинність певного твердження іншій стороні без розкриття будь-якої іншої інформації, крім істинності цього твердження. В області інформаційних технологій доказ із нульовим розголошенням дозволяє довести правильність виконання певних обчислень, не розкриваючи при цьому вхідні дані, над якими обчислення були проведені. Особливістю доказів із нульовим розголошенням є константна, логарифмічна або поліноміальна складність перевірки доказу, значно менша у порівнянні зі складністю створення доказу (зазвичай лінійно-логарифмічна).

Блокчейн-ролапи (англ. Blockchain Rollups) — технологія для протоколів другого рівня для облікових систем на базі EVM, основною метою використання якої є зменшення витрат на виконання транзакцій. Це досягається за рахунок об’єднання великої кількості транзакцій другого рівня в єдиний пакет (батч, англ. batch), що публікується в якості однієї транзакції в цільовій обліковій системі (першого рівня), до якої висуваються ті ж вимоги щодо правильності, що й до інших транзакцій. Таким чином, використання ролапів дозволяє поєднати високу швидкість виконання транзакцій та низькі витрати із інформаційною безпекою, що гарантує значно децентралізована облікова система першого рівня.

Блокчейн-ролапи на базі доказів із нульовим розголошенням (англ. Zero-Knowledge Blockchain Rollups) — технологія ролапів, ключовою особливістю якої є застосування доказів із нульовим розголошенням для ще більшої оптимізації обчислень в обліковій системі першого рівня.

Облікова система другого рівня може мати додаткові властивості у порівнянні з обліковою системою першого рівня:

— бути приватною, тобто для доступу до неї може бути потрібен дозвіл;

— транзакції в ній можуть мати додаткові засоби забезпечення інформаційної безпеки (докази із нульовим розголошенням, гомоморфне шифрування і таке інше);

— реалізовувати вбудовані механізми управління, не властиві системі першого рівня (наприклад, голосування);

— мати додаткові обмеження щодо стану системи та перевірки на їх задовільнення (наприклад, банківська установа не повинна мати зобов'язань більше, ніж активів).

Таким чином, стає можливим окреслити особливості системи банку на базі комплексу вищезазначених технологій:

— облікова система на базі блокчейну для зберігання даних;

— децентралізований протокол досягнення консенсусу;

— EVM-подібне віртуальне обчислювальне середовище для виконання фінансових операцій;

— блокчейн-ролапи на базі доказів із нульовим розголошенням для забезпечення додаткової інформаційної безпеки засобами системи першого рівня та нижчої вартості транзакцій.

Додатковими рішеннями можуть бути блокчейн-мости (бріджі, англ. bridges), що дозволяють виконувати транзакції між різними децентралізованими обліковими системами (таким чином зможуть комунікувати між собою різні банківські установи, які використовують описаний комплекс технологій, а їх клієнти — переводити між ними кошти і т. п.).

Крім операцій з переводу коштів, можливо також реалізувати й інші банківські та біржеві фінансові інструменти, що вже знайшли своє втілення у DeFi-сфері. До таких інструментів відносяться:

— децентралізовані біржі: традиційні (побудовані на біржевих ордерах) або автоматизовані маркет-мейкери (англ. Automated Market Makers); другі втілюють механізм пулів ліквідності (англ. Liquidity Pools), тобто автоматично визначають ціну одного активу відносно другого в залежності від співвідношення їх пропозиції у визначеному пулі;

— протоколи кредитування: дозволяють отримувати позику в обмін на заставу, причому управління заставою здійснюється смарт-контрактом;

— децентралізовані стейблкоїни (англ. Stablecoins) — активи, ціна яких прив'язана до вартості певних активів реального світу (національних валют, акцій, золота і т. д.);

— інші (наприклад, децентралізовані автономні організації, що керують коштами інвесторів).

Список використаних джерел

1. Кравченко П., Скрябін Б., Дубініна О. Блокчейн і децентралізовані системи: навч. посібник для студ. закл. вищ. осв. У трьох частинах. Ч. 1. Харків : ПРОМАРТ, 2023. — 460 с. — ISBN 978-617-7634-40-8.

2. Ethereum Virtual Machine (EVM). URL: https://ethereum.org/en/developers/docs/evm/ (дата звернення: 05.03.2024).

3. Rollup. URL: https://www.techopedia.com/definition/rollup (дата звернення: 05.03.2024).

4. Zero-knowledge proofs explained: Part 1. URL: https://www.expressvpn.com/blog/zero-knowledge-proofs-explained/ (дата звернення: 05.03.2024).

УДК 621.38 https://doi.org/10.30837/IYF.PCEIP.2024.099

МЕТОДИ КРИПТОАНАЛІЗУ СУЧАСНИХ ШИФРІВ

Гузенко Н. В.
Науковий керівник – к.т.н. Мельникова О. А.
Харківський національний університет радіоелектроніки, каф. БІТ, м. Харків, Україна
e-mail: nikita.huzenko@nure.ua

Nowadays, information plays a key role. Ciphers are used for information protection. Cryptanalysis deals with the discovery of the output text or key that will allow the ciphertext to be decrypted. It plays a very significant role in information security, as it is used both by cipher developers and by hackers who want to gain access to protected data. In order to understand how secure a particular cipher is, you need to analyze it and find bottlenecks in its mathematical base. Cryptanalysis is very important because it studies the security of a cipher and its key, and the key denotes the strength of the entire cryptosystem.

Інформація — це найважливіше, що може бути у сучасному світі. При передаванні та зберіганні конфіденційної інформації треба точно знати, що доступ до неї отримають тільки авторизовані користувачі. Для забезпечення безпеки інформації використовуються криптографічні засоби, які дозволяють виконувати шифрування та автентифікацію джерела інформації.

Для підтримки безпеки необхідно не тільки шифрувати дані, а й проводити аналіз безпеки того чи іншого шифру, тобто аналізувати можливості криптоаналізу. Криптоаналіз — це розділ криптології, що займається математичними методами порушення конфіденційності та цілісності інформації без знання ключа. Він дозволяє також знайти слабкі місця в криптосистемі, що у кінцевому рахунку, призведе до тих же результатів. Криптоаналізом можуть користуватись не тільки розробники, а також і ті, хто бажає отримати доступ до конфіденційних даних (зашифрованої інформації).

Стійкість криптосистеми визначається тільки таємністю ключа, тому що криптосистема являє собою сукупність апаратних і програмних засобів, яку можна змінити тільки при значних витратах часу та ресурсів, тоді як ключ є легко змінюваним об’єктом.

Виділяють такі основні методи атак:

1) на основі шифротексту;
2) на основі відкритих текстів і відповідних шифротекстів;
3) на основі підібраного відкритого тексту;
4) на основі адаптивно підібраного відкритого тексту.

Також можуть розглядатися такі додаткові методи:

1) атака на основі підібраного шифротексту;

2) атака на основі підібраного ключа;
3) “бандитський” криптоаналіз.

Для симетричних шифрів найбільш відомими є наступні методи криптоаналізу:

1) диференційний криптоаналіз (блокові або потокові шифри);
2) лінійний криптоаналіз (блокові або потокові шифри);
3) кореляційний криптоаналіз (потокові шифри);
4) статистичний криптоаналіз (блокові або потокові шифри);
5) атака “грубої сили” (перебір варіантів).

Для асиметричних шифрів можуть застосовуватись:

1) диференційний криптоаналіз;
2) лінійний криптоаналіз;
3) атака “людина посередині”;
4) атака “грубої сили”.

Атака “людина посередині” означає, що між відправником та отримувачем є деякий посередник, який перехоплює всі повідомлення. А також, на початку сесії (на етапі узгодження спільного ключа), цей посередник перехоплює дані та з їх допомогою відновлює ключ. Атака “грубої сили” припускає перебір всіх можливих варіантів ключа шифрування до знаходження пошукового ключа.

Диференційний криптоаналіз — це спроба розкриття секретного ключа блокових шифрів, які засновані на повторному застосуванні криптографічно слабкої цифрової операції шифрування *r*-разів. При аналізі передбачається, що на кожному циклі використається свій підключ шифрування. Конкретний спосіб застосування диференційного криптоаналізу залежить від алгоритму шифрування, що аналізується. Лінійний криптоаналіз використовує лінійні наближення перетворень, що виконуються алгоритмом шифрування. Даний метод дозволяє знайти ключ, маючи досить велику кількість пар {незашифрований текст, зашифрований текст}.

Кількість та потужність методів криптоаналізу збільшується з кожним роком, а існуючі методи модернізуються, але й методи шифрування постійно вдосконалюються. Також на складність криптоаналізу та стійкість шифрів значно впливає вдосконалення технічної бази. У вітчизняній та іноземній практиці криптоаналізу використовуються одні й ті самі методи але, звичайно, з урахуванням індивідуальних особливостей шифрів.

Список використаних джерел

1. Cryptanalysis | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-community/attacks/Cryptanalysis (дата звернення: 05.03.2024).

УДК 004.056 https://doi.org/10.30837/IYF.PCEIP.2024.101

ЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ КІБЕРВІЙНИ

Дорофєєва К. І.
Науковий керівник – Євгеньєв А.М.
Харківський національний університет радіоелектроніки, каф. БІТ, м. Харків, Україна
e-mail: dorofieieva.kseniia@nure.ua

The current issues of protecting critical infrastructure facilities in the context of cyber warfare is considered. In addition, the importance of continuously updating and improving protection measures to effectively counter rapidly changing cyber threats is considered. The threats that affect the security of critical infrastructure in the conditions of cyber warfare have been identified The importance of paying attention to this issue and emphasizing the need for continuous improvement of cybersecurity strategies to ensure the continuity of critical infrastructure in the era of digital threats is described.

В умовах війни захист об’єктів критичної інфраструктури є одним із важливих пріоритетів держави. В сучасних умовах відбувається й кібервійна, у зв’язку з чим ризики для інфраструктури суттєво зростають. Адже саме від стану захищеності її об’єктів багато у чому залежить і національна безпека. Тому численні та цілеспрямовані кібератаки ворога спрямовані, у першу чергу, на підрив основ національної безпеки країни, насамперед, шляхом заподіяння шкоди державним інформаційним ресурсам та об’єктам критичної інфраструктури [1].

Здійснення заходів з кіберзахисту передбачає [2-5]:

- ідентифікацію – виявлення реальних і потенційних кіберзагроз для запобігання та їх нейтралізації;
- захист – розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення сталості і надійності функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних та технологічних систем;
- виявлення – проведення моніторингу визначення, збору та обробки нетипових подій у кіберпросторі;
- реагування – вжиття заходів, спрямованих на запобігання кіберінцидентам, кібератакам, мінімізацію їх можливих наслідків, удосконалення систем кіберзахисту, з урахуванням необхідності забезпечення пропорційності та співрозмірності можливостей таких систем реальним та потенційним ризикам;

- відновлення – поновлення штатного режиму функціонування інформаційно-телекомунікаційних, технологічних систем після кібератаки, відновлення інформації та відомостей у разі їх пошкодження або видалення, створення передумов для проведення розслідування за наслідками кібератаки.

Під час забезпечення функціонування базисної інфраструктури кіберзахисту забезпечується:

- захист у кіберпросторі національних електронних інформаційних ресурсів, комунікаційних і технологічних систем, зокрема тих, що використовуються для задоволення суспільних потреб;
- захист об’єктів критичної інфраструктури;
- захист інтересів громадянина та суспільства у кіберпросторі;
- здійснення заходів з формування культури кібербезпеки в установах, на об’єктах критичної інфраструктури і підприємствах;
- інформування громадян про кіберінциденти.

Головним завданням технологічної інфраструктури кіберзахисту є оперативний та ефективний захист кіберпростору в частині протидії кібератакам, кіберзлочинам, кібертероризму, кібершпигунству, в тому числі шляхом: збору, аналізу, оцінювання, узагальнення та поширення інформації про кіберінциденти; надання методичної допомоги іншим суб’єктам кіберзахисту; взаємного інформування суб’єктів кіберзахисту про нові реальні та потенційні загрози; створення умов для відповідального та довіреного обміну інформацією між суб’єктами кіберзахисту всіх секторів кіберзахисту [1, 4, 5].

Об’єкти критичної інфраструктури – це стратегічно важливі підприємства та установи, необхідні для функціонування суспільства країни та її економіки. Захист об’єктів критичної інфраструктури – комплексне та пріоритетне завдання держави в умовах сьогодення.

Список використаних джерел

1. Yevseiev, Serhii, et al. "Development of a concept for building a critical infrastructure facilities security system." Eastern-European Journal of Enterprise Technologies 3.9 (2021): 111.
2. Іваненко О.І. Підхід до національної оцінки ризиків для критичної інфраструктури. Вісник ХНТУ. 2020. № 2(73). С. 9-22.
3. Овчаренко М.Ю., Сєвєрінов О.В. Аналіз сучасних систем управління інформаційною безпекою та інцидентами безпеки. ЧДТУ, НТУ "ХПІ", ВА ЗС АР, УТіГН, ДП" ПД ПКНДІ АП", 2019.
4. Про затвердження Положення про організаційно-технічну модель кіберзахисту. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text (дата звернення: 01.03.2024).
5. Про критичну інфраструктуру. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 04.03.2024).

УДК 004.056.5

АНАЛІЗ БЕЗПЕКИ ЦП НА ОСНОВІ ГЕШ ФУНКЦІЇ KECCAK

Івашов В.А,
Науковий керівник – ст., викл. В'юхін Д.О.
Харківський Національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: vladyslav.ivashov@nure.ua

An analysis of the security of digital signatures using the Keccak hash function was carried out in order to determine their resistance to modern cryptanalytic attacks and justify their suitability for protecting digital information. Analysis of the security of a digital signature includes an assessment of the resistance of such a signature to various attacks, including cryptanalysis, collisions, and other types of attacks on the hashing algorithm and the signature scheme itself.

В сучасному цифровому світі захист інформації від несанкціонованого доступу є однією з найважливіших проблем. Останнім часом кількість загроз та атак на інформаційні системи постійно зростає. Аналіз сучасних методів атак на інформаційні системи показав на необхідність забезпечення цілісності та автентичності на високому рівні [1, 2]. Одним з методів вирішення цієї задачі є використання стійких цифрових підписів, що використовуються для забезпечення цілісності та автентичності електронних документів. Дослідження безпеки ЦП на основі геш-функції Keccak є актуальним у контексті постійного розвитку кіберзлочинності та криптографічних атак.

Метою цього дослідження є проведення аналізу безпеки цифрових підписів, які використовують геш-функцію Keccak, з метою визначення їхньої стійкості до сучасних криптоаналітичних атак та обґрунтування їхньої придатності для захисту цифрової інформації.

Аналіз безпеки цифрового підпису (ЦП) на основі геш-функції Keccak включає в себе оцінку стійкості такого підпису до різних атак, зокрема криптоаналізу, колізій та інших видів атак на алгоритм гешування та саму схему підпису.

Геш-функція Keccak, яка є основою стандарту SHA-3, має відмінності від попередніх алгоритмів, таких як SHA-1 та SHA-2. Ці відмінності можуть включати розмір вихідного геша, стійкість до певних видів атак, швидкодію та інші
фактори [3].

При аналізі безпеки ЦП на основі Keccak слід розглядати такі аспекти:

– стійкість геш-функції Keccak. Це забезпечується реалізацією криптографічної губки на 24 раунди;

– використання Keccak в протоколах ЦП. Оцінка, як саме використовується Keccak в протоколі ЦП, включаючи методи гешування, конкатенації та інші операції [4]. Також ця схема більш швидка бо в процесі відбору на конкурс SHA-3 розробники змінили спосіб заповнення блоків губки. Що дало більш високу ефективність;

– стійкість самої схеми ЦП. Оцінка того, наскільки безпечно використання Keccak у протоколі ЕЦП, враховуючи усі можливі атаки на схему підпису;

– відповідність стандартам безпеки. Перевірка відповідності протоколу ЦП на основі Keccak сучасним стандартам безпеки та рекомендаціям криптографічної спільноти [4]. За результатами різноманітних спроб криптоатак на Keccak, було прийнятий висновок що пошук прообразів його геш-функцій повинен мати потужність мінімум квантового рівня.

На основі проведеного аналізу можна зробити висновок, що цифрові підписи, побудовані на базі геш-функції Keccak, виявляють високий рівень стійкості до сучасних криптоаналітичних атак [5]. Але якщо рівень технічного обладнання дозволяє провести атаку постквантового рівня то це шифрування буде вже не ефективним. Це приводить нас до того, що хоч алгоритм і є на наш час досить безпечним, але майже 10 років його існування потребує нових конкурсів на генерування геш-функцій.

Список використаних джерел

1. Сєвєрінов О.В., Хрєнов А.Г., Поляков А.О. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі // Системи обробки інформації 9 (2015): 101-104.

2. Голубничий Д.Ю., Сєвєрінов О.В., Коломійцев О.В., Місюра О.М., Третяк В.Ф., Власов А.В., Крук Б.М. Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації. (2021).

3. Bertoni, Guido, Joan Daemen, Michael Peeters, and Gilles Van Assche. Keccak sponge function family main document. NIST. 2010.

4. Aumasson, Jean-Philippe. The hash function Keccak. In Fast Software Encryption. Springer. 2013 р.. 313 с.

5. Качко Е. Г. Дослідження застосування SMT/SAT доказів у криптоаналізі хеш-функцій сімейства Keccak / Е. Г. Качко, Д. К. Телевний // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. - 2017. - Вип. 189. - С. 75 – 80.

УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.105

МЕТОДИ ТА МОДЕЛІ БАГАТОДЖЕРЕЛЬНОЇ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

Кайдалов В.Д.
Науковий керівник – к.т.н., доцент Голян В.В.
Харківський національний університет радіоелектроніки, каф. ПІ,
м. Харків, Україна
e-mail: vadym.kaidalov@nure.ua

Authentication can be achieved using one or more of three fundamental factors: knowledge-based, possession-based, and biometric features. The latter has gained popularity as a reliable alternative solution. Biometric features are categorized into physiological features, behavioral features, and “soft” features. Each of them has its advantages and disadvantages, including the financial cost of installing appropriate sensors and the amount of time spent by users to interact with these sensors. Multimodal biometric authentication utilizes several independent features (such as face and voice) and does not rely on a single characteristic. As a result, it is much more resistant to spoofing attacks and mitigates the negative impact of noise and low-quality data.

Автентифікація користувача широко використовується як засіб захисту будь-якої інформаційної системи (ІС) від дій зловмисників. Інформаційній системі необхідно перевірити ідентичність користувача, зазвичай використовуючи такі облікові дані, як ім’я користувача та пароль, щоб потім наділити користувача певними привілеями (авторизувати) для доступу до ресурсів системи. Оскільки ІС тісно пов’язані з нашим повсякденним життям, надійна автентифікація є надзвичайно важливою для забезпечення безпеки в будь-якій ІС. Більше 40 років проводиться інтенсивне дослідження методів автентифікації – це підтверджує важливість процесу автентифікації для створення безпечних середовищ, які захищають ІС від підробки ідентичності користувача, а також намагаються полегшити або спростити сам процес взаємодії користувача з системою автентифікації.

Автентифікація користувача може бути здійснена за допомогою одного або декількох з трьох фундаментальних факторів:

- на основі знання (щось, що користувач знає),
- на основі володіння (щось, чим користувач володіє),
- на основі біометричних ознак (щось, чим користувач є).

Останній фактор, біометричні ознаки, набув популярності як надійне альтернативне рішення [1].

Біометричні ознаки, за походженням, діляться на наступні групи:

– фізіологічні ознаки базуються на унікальних фізичних рисах особи (відбитки пальців, райдужна оболонка ока, форма та риси обличчя тощо);

– поведінкові ознаки відносяться до поведінки особи (аналіз ходи, динаміка натискання клавіш на клавіатурі, рух комп'ютерної миші, рух пальців на сенсорному екрані, голос тощо);

– «м'які» ознаки не надають можливості унікально ідентифікувати особу, але надають корисну додаткову інформацію (стать, зріст, колір волосся тощо).

Використання тих чи інших ознак має свої переваги та недоліки, включаючи фінансову вартість встановлення відповідних сенсорів та час, який користувачу необхідно витрачати на взаємодію з цими сенсорами. Наприклад, збір даних про взаємодію з клавіатурою під час роботи користувача не вимагає ні додаткових фінансових витрат, ні додаткового часу на надання користувачем біометричних даних на відміну від сканування райдужки очей, яке, з іншого боку, надає більшу постійність даних і призводить до вищої точності автентифікації [2].

Задачу проведення автентифікації можна представити у вигляді задачі однокласової класифікації, в якій за зразком вхідних даних необхідно встановити, чи належить наданий зразок до визначеного класу, чи ні. Зразок вхідних даних – це зразок даних біометричної ознаки користувача, наприклад, двовимірне зображення райдужки ока чи двовимірна таблиця, що зберігає ідентифікатори клавіш клавіатури та моменти часу, в які вони були натиснуті. Відношення зразку вхідних даних до визначеного класу означає, що зразок був згенерований в результаті взаємодії справжнього користувача з ІС, що підтверджує ідентичність. Якщо зразок вхідних даних не відноситься до цього єдиного класу, то ідентичність не підтверджується, і тоді ІС перериває сесію користувача і припиняє надання доступу до себе, поки ідентичність не буде підтверджена тим чи іншим шляхом знову.

Залежно від кількості біометричних джерел, які використовуються, біометричну систему автентифікації можна класифікувати на два типи: одноджерельну (одномодальну, унімодальну) або багатоджерельну (багатомодальну, мультимодальну). Одноджерельні біометричні системи ґрунтуються на одному джерелі для автентифікації і тому їх легше розробляти, оскільки вони базуються на одному ідентифікаторі. Однак, одноджерельна система стикається з такими викликами, як шумні дані, погана продуктивність розпізнавання, нижча точність та атаки підробки, оскільки для успішної атаки достатньо підробити усього одну біометричну ознаку. Багатоджерельна біометрична автентифікація, навпаки, використовує кілька незалежних ознак (наприклад, обличчя та голос), не ґрунтується на одній ознаці і тому набагато

більш стійка до атаки підробки та зменшує негативний вплив шумів і низької якості даних [3].

У випадку з багатоджерельною біометричною аутентифікацією, виникає потреба обчислити єдину оцінку схожості на основі обробки даних, отриманих з декількох джерел – здійснити так зване «злиття» (англ. «fusion»). В залежності від етапу, на якому відбувається злиття, існують наступні найуживаніші методи:

– злиття на рівні оцінок (англ. «score level fusion») – метод, що об'єднує оцінки схожості, незалежно отримані від декількох класифікаторів, кожен з яких працює зі своїм джерелом біометричних даних. Незалежність роботи класифікаторів надає можливість приєднувати додаткові класифікатори, які будуть впливати на загальну оцінку тільки на етапі злиття, не впливаючи на роботу інших компонентів;

– злиття на рівні ознак (англ. «feature level fusion») – є другим за популярністю методом злиття, що поєднує різні ознаки, витягнуті з сирої біометричної інформації, в один єдиний масив даних, що надалі обробляється єдиним класифікатором. Цей процес може усунути шум в сирій біометричній інформації, що потенційно покращує точність автентифікації. Об'єднання на рівні ознак дозволяє анонімізувати зображення та набори ознак, створюючи новий "непрозорий" масив даних для автентифікації, що також може сприяти підвищенню конфіденційності зберігання біометричних даних у системах віддаленого доступу. Однак через високу розмірність даних, об'єднання на рівні ознак генерує вище обчислювальне навантаження.

Неперервна багатоджерельна біометрична автентифікація (англ. «continuous multimodal biometric authentication») з'явилася для покращення точності перевірки ідентичності та усунення вразливостей статичної автентифікації [1]. Однак, виникають проблеми з використанням та масштабованістю, оскільки CMBA вимагає неперервної перевірки заявленої ідентичності впродовж сесії користувача, що веде до підвищення споживання обчислювальних ресурсів, розміру збережених даних тощо.

Список використаних джерел

1. Continuous Multimodal Biometric Authentication Schemes: A Systematic Review / R. Ryu et al. *IEEE Access*. 2021. Vol. 9. P. 34541–34557. URL: https://doi.org/10.1109/access.2021.3061589 (date of access: 12.03.2024).

3. Dee T., Richardson I., Tyagi A. Continuous Nonintrusive Mobile Device Soft Keyboard Biometric Authentication. *Cryptography*. 2022. Vol. 6, no. 2. P. 14. URL: https://doi.org/10.3390/cryptography6020014 (date of access: 12.03.2024).

3. Continuous and transparent multimodal authentication: reviewing the state of the art / A. Al Abdulwahid et al. *Cluster Computing*. 2015. Vol. 19, no. 1. P. 455–474. URL: https://doi.org/10.1007/s10586-015-0510-4 (date of access: 12.03.2024).

УДК 004.75 https://doi.org/10.30837/IYF.PCEIP.2024.108

ANALYSIS AND COMPARISON OF THE PALA CONSENSUS PROTOCOL

Кравченко А.А.
Науковий керівник: д.т.н, проф. Олійников Р.В.
Харківський національний університет радіоелектроніки, каф. БІКС,
м. Харків, Україна
e-mail: anastasiia.kravchenko@nure.ua

The PaLa protocol is known for its simplicity and effectiveness in achieving Byzantine Fault Tolerance (BFT). This thesis discusses the main properties of the PaLa – partially synchronous blockchain protocol, its advantages and disadvantages, and key aspects of its structure. We also compare PaLa with other algorithms, such as Tendermint, Hotstuff, and Casper FFG, which have fewer limitations due to their more complex structure. Based on the considered limitations, the following modifications are presented, which allow to extend them: Pipelet protocol, Committee rotation algorithm, and Streamlet protocol.

The PaLa protocol was proposed as a new consensus protocol based on simplicity and efficiency, aiming to streamline the consensus process while maintaining security standards. It is considered one of the simplest and most efficient classical BFT consensus protocols, focusing on removing unnecessary complexities present in previous protocols to enhance performance. PaLa is inspired by the pipelined-BFT paradigm and a generalization called "doubly-pipelined PaLa", which is oriented towards settings that require high performance [1].

PaLa stands out as a simple partially synchronous blockchain protocol inspired by the pipelined-BFT paradigm. Unlike its predecessors, PaLa focuses on removing unnecessary complexities to streamline the consensus process. By leveraging a partially synchronous network model and tolerating up to ⅓ corruptions, PaLa aims to achieve fast transaction confirmations while maintaining security. The PaLa protocol has several advantages over other blockchain consensus protocols making it an outstanding solution in this field.

Key features of PaLa:

– Efficiency: PaLa minimizes the number of messages required to reach a consensus and increases transaction speed without compromising security;

– Simplicity: by eliminating the inefficiencies present in traditional protocols, PaLa provides a simple and elegant solution for Byzantine fault tolerance;

– Security: While speed is a priority, PaLa incorporates robust security measures to protect against malicious activity and guarantee transaction integrity;

– Network Model Adaptability: PaLa is based on partially synchronous network assumptions and can tolerate up to ⅓ corruptions, making it adaptable to various network settings while maintaining efficiency. The protocol's ability to achieve consensus with just O(n) messages showcases its adaptability and scalability in different blockchain environments [3].

Perhaps, the key features sufficiently describe the advantages of using this protocol, so we should move on to the disadvantages and limitations, which are also here. Although PaLa is recognized as the simplest and most efficient classic BFT consensus protocol, it does not introduce many new innovations compared to other protocols such as Tendermint, FBFT, Casper FFG, and Hotstuff. In addition, there are scalability issues: for a network with more nodes, maintaining speed becomes more difficult, which affects performance. In addition, the focus on simplicity, speed, and increased throughput can lead to various security issues. The protocol's responsiveness to real-world network delays, denoted as δ, is essential for achieving fast transaction finality. Adapting to network conditions and minimizing delays is crucial for enhancing transaction speed within the PaLa protocol. The risks associated with generating a large number of orphan blocks should not be overlooked: maintaining a balance between block production rate and network latency is crucial to prevent high rates of empty blocks that can affect transaction completion and overall network efficiency.

As noted, one of the advantages of using PaLa is speed, so for a clearer understanding, let's compare it with other protocols used:

– Tendermint: Tendermint is known for its high throughput and fast finality, making it a scalable solution for blockchain networks. It achieves consensus through a practical Byzantine Fault Tolerance (PBFT) algorithm, offering robustness in handling a large number of transactions [2]. It also has an optimal solution to improve the efficiency of work in such conditions is to perform load balancing or use rpc nodes, not just individual network validators. This allows to increase the speed and avoid cases of node overload [5];

– Hotstuff: Hotstuff is another protocol that focuses on scalability and efficiency by utilizing a leader-based approach for consensus. It offers fast confirmation times and high throughput, addressing scalability challenges effectively [2];

– Casper FFG: Casper FFG introduces a hybrid Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus mechanism to enhance scalability and security. By combining these two approaches, Casper FFG aims to achieve a balance between transaction speed and network scalability [2].

It becomes apparent that in comparison to these protocols, PaLa may face limitations in scalability due to its partially synchronous nature and the challenges associated with handling network delays as the network grows.

1. Pipelet protocol

Pipelet protocol: the Pipelet protocol was introduced as a practical streamlined consensus protocol to improve scalability. Pipelet protocol: the Pipelet protocol was introduced as a practical streamlined consensus protocol to improve scalability, including extending the longest chain and finalizing the middle of three consecutive normal notarised blocks, using familiar rules [4].

Pipellet aims to combine the advantages of simplicity, performance and practicality found in other protocols such as Streamlet and PaLa, and offers a conceptually different approach that reduces the message costs required to finalize a block.

2. Committee rotation algorithm

A committee rotation algorithm is proposed to enhance the scalability and security of PaLa. The algorithm aims to dynamically rotate consensus nodes in dynamic networks using verifiable random functions (VRFs) to reduce communication requirements in stable network conditions [4].

3. Streamlet protocol

The Streamlet protocol provides a simple and natural paradigm for building consensus protocols, inspired by core technologies discovered in the past Streamlet and PaLa messages grow exponentially with the number of nodes. To address scalability concerns, detailed specifications on assumptions, consistency and effectiveness under partial synchronization are provided [4].

Recent studies have evaluated the performance and scalability of prominent consensus protocols like PBFT, Tendermint, HotStuff, Streamlet, and PaLa under identical conditions. These evaluations highlight limitations in communication complexity for larger networks and emphasize the need for practical solutions like Pipelet to address scalability challenges effectively.

In conclusion, this paper has discussed the general properties of the PaLa algorithm, its advantages and disadvantages in comparison with some other popular algorithms. This protocol is quite simple and robust, but it may have some scaling issues due to its structure. However, several modifications almost solve these problems while maintaining the basic structure of the protocol, the best of which, in the author's personal opinion, is Pipelet due to its practical applicability.

Список використаних джерел

1. KARIHALOO, Vivek, et al. Pipelet: Practical Streamlined Blockchain Protocol. *arXiv preprint arXiv:2401.07162*, 2024.

2. Qi G., Lu P. Consensus Protocols 101. *https://docs.thundercore.com/consensus-protocols-101.pdf.*

3. Kim C. Blockchain Project Thundercore Releases Code for 'Pala' Consensus Protocol. *CoinDesk: Bitcoin, Ethereum, Crypto News and Price Data*. URL: https://www.coindesk.com/markets/2019/05/15/blockchain-project-thundercore-releases-code-for-pala-consensus-protocol/

4. CHAN, TH Hubert; PASS, Rafael; SHI, Elaine. Pala: A simple partially synchronous blockchain. *Cryptology ePrint Archive*, 2018.

5. Дубіна В.В., Олійников Р.В. Аналіз властивостей децентралізованого протоколу консенсусу із підвищеною пропускною здатністю. Проблеми інформатизації: десята міжнародна науково-технічна конференція. Харківський національний університет радіоелектроніки - Черкаси – Баку – Бельсько-Бяла – Харків – 2022.

УДК: 004.75:004.056.5

ПРОБЛЕМИ БЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ В ХМАРНИХ СХОВИЩАХ

Леонова А.О.
Науковий керівник - ст. викл. Данилов А.Д.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: anna.leonova@nure.ua

Instead of storing files on your company's hard drive or local storage device, you can use cloud storage, which allows you to store them in a remote database. Cloud storage is becoming increasingly popular among people who need more storage space and for businesses looking for an efficient off-premises data backup solution. Due to the growing popularity and use of cloud storage, cloud security has become a major concern to protect data integrity, prevent hacking attempts, and prevent file or personal data theft.

У сучасному світі цифрових технологій хмарні сховища набули великого значення. Більшість приватних даних зберігається в хмарі, за власним бажанням співробітника або за рішенням компанії. Тому питання безпеки інформації в хмарних сховищах є серйозною проблемою [1].

Важливо мати стратегію безпеки в хмарі. Незалежно від того, чи має постачальник хмарних послуг вбудовані засоби безпеки, чи користувач співпрацює з провідними постачальниками хмарних технологій, можна отримати численні переваги від хмарної безпеки [2]. В іншому випадку, можуть з’явитися наступні проблеми:

– відсутність видимості. Легко втратити інформацію про те, як і хто отримує доступ до ваших даних, оскільки доступ до багатьох хмарних служб здійснюється за межами корпоративних мереж і через треті сторони;

– неправильні конфігурації. Частину зламаних записів можна віднести до неправильно налаштованих активів, що робить ненавмисне внутрішнє користування ключовою проблемою для середовищ хмарних обчислень [3];

– тіньові IT – це практика використання пристроїв, програм і систем без погодження з IT-відділом організації. Хмарна безпека має охоплювати всі точки доступу до хмари, щоб співробітники не могли порушити безпеку всієї організації, входячи в систему з приватних пристроїв;

– керування доступом. Як і в традиційних системах кібербезпеки, права доступу користувачів мають бути пропорційні їхнім посадовим обов’язкам. Співробітники з надлишковими правами можуть завдати шкоди даним через недосвідченість або через хакерські атаки на їхні облікові записи [4].

Для забезпечення надійної безпеки в хмарі можна використовувати різні підходи та інструменти, адаптовані до конкретних вимог і рівнів захисту. Ось деякі приклади заходів захисту в хмарних середовищах [4, 5]:

– шифрування даних. Шифрування є фундаментальним стовпом безпеки, перетворюючи дані в нерозбірливий формат за допомогою алгоритмів кодування та криптографічних ключів;

– ефективний контроль доступу. Впровадження суворого контролю доступу є необхідним для підтримки цілісності хмарних ресурсів. Сюди входить надійна автентифікація користувачів, політики авторизації та контроль доступу на основі ролей (RBAC);

– надійні брандмауери. Брандмауери слугують захисними бар'єрами між внутрішніми і зовнішніми мережами, ретельно фільтруючи вхідний і вихідний мережевий трафік;

– надійне резервне копіювання та відновлення. Впровадження надійних стратегій резервного копіювання та відновлення є важливим аспектом безпеки хмари, забезпечуючи доступність і цілісність даних;

– ефективні системи виявлення та запобігання вторгнень (IDPS). Засоби IDPS активно контролюють мережевий трафік і системи, відстежуючи підозрілі дії або потенційні порушення безпеки;

– централізоване управління інформацією та подіями безпеки (SIEM). Ці системи об'єднують і аналізують дані журналів із різних джерел у хмарній інфраструктурі, забезпечуючи централізоване спостереження за подіями безпеки.

Хмарні обчислення забезпечують зручний доступ до даних та стають об'єктом збільшеного ризику щодо безпеки. З метою запобігання можливим загрозам, необхідно вживати комплекс заходів безпеки (шифрування даних, контроль доступу та використання надійних брандмауерів та антивірусного програмного забезпечення). Надійна стратегія безпеки в хмарних обчисленнях є ключовим елементом для збереження цілісності та конфіденційності даних у цифровому середовищі.

Список використаних джерел

1. Cloud Security: Definition, How Cloud Computing Works, and Safety. investopedia.com: веб сайт. URL: https://www.investopedia.com/terms/c/cloud-security.asp(дата звернення: 2.03.2024).

2. CLOUD SECURITY. crowdstrike.com: веб сайт. URL: https://www.crowdstrike.com/cybersecurity-101/cloud-security/(дата звернення: 2.03.2024).

3. What is cloud security? ibm.com: веб сайт. URL: https://www.ibm.com/topics/cloud-security(дата звернення: 2.03.2024).

4. Що таке хмарна безпека? nordvpn.com: веб сайт. URL: https://nordvpn.com/uk/cybersecurity/cloud-security/ (дата звернення: 2.03.2024).

5. Рудий С.В., Сєвєрінов О.В. Дослідження моделі безпеки при використанні хмарних сервісів. 2022.

УДК 004.056.53 https://doi.org/10.30837/IYF.PCEIP.2024.113

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ЦИФРОВОГО КОНТЕНТУ: DRM І ТЕХНОЛОГІЯ DENUVO

Лісняк Д.С.
Науковий керівник – асист. Гвоздьов Р.Ю.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: danylo.lisniak@nure.ua

The rapid evolution of the distribution of digital content has led to the need to create reliable mechanisms for protecting intellectual property from unauthorised access and distribution. This article examines two main methods of protecting digital content: Digital Rights Management (DRM) and Denuvo technology. DRM acts like a set of locks and keys, controlling who can access digital content and what they can do with it. Denuvo, on the other hand, serves as a sophisticated defence against unauthorised access and piracy, especially in the gaming industry. This article is dedicated to figuring out how to make sure that digital content remains secure in a world where sharing and copying is easy.

Існує загальновідома думка, що захист авторських прав є надмірно обмежувальним, але з огляду на той факт, що кожного разу, коли хтось завантажує цифровий контент, захищений авторськими правами, замість того, щоб купляти право на використання цифрового продукту, несанкціоновано копіюють, використовують та розповсюджують такі продукти [1]. Не варто забувати і про ігрову та кіноіндустрію, які втрачають мільярди доларів через піратство. Технології управління цифровими правами (DRM) здатні захистити цифровий контент і обмежити його використання.

DRM (Digital Rights Management) – це технологія, яка захищає цифрові авторські права шляхом управління та обмеження доступу до цифрових носіїв, захищених авторським правом [2, 3]. Програмне забезпечення DRM також містить у собі різні заходи проти несанкціонованого копіювання, розповсюдження та зміни зазначених матеріалів, захищених авторським правом. Технологія захисту DRM дає видавцям і творцям повний контроль над тим, хто може отримати доступ до їхнього контенту і що вони можуть з ним робити. DRM захищає IP-адреси і запобігає крадіжці та незаконному розповсюдженню їхніх робіт в Інтернеті. Хоча DRM не бореться і не переслідує тих, хто займається піратством, він насамперед запобігає потраплянню цифрового контенту у відкритий доступ.

Також варто розглянути використання DRM на мобільних пристроях, які є невід’ємною частиною сучасних технологій. Можливість використовувати DRM на мобільних телефонах забезпечує повну безпеку контенту. OMA DRM – це механізм DRM, визначений Open Mobile Appliance. Мобільний DRM

спроектований таким чином, щоб зберігати контроль над медіа-об'єктами. Він може керувати використанням контенту, даючи змогу розробляти нові функції для кінцевих користувачів і різні види послуг мобільного контенту для розробників послуг, постачальників контенту, постачальників послуг і операторів.

DRM захист часто зіштовхується з критикою, наприклад за наступними пунктами. Незручність для користувачів: DRM завдає незручностей законним користувачам. Дана технологія обмежує передачу контенту з одного пристрою на інший, обмін контентом з членами сім'ї та створення резервних копій. Проблеми сумісності: системи DRM можуть спричиняти проблеми сумісності між різними пристроями, програмними платформами та екосистемами. Контент, захищений однією системою DRM, може бути недоступний на пристроях або в програмному забезпеченні, які не підтримують цей формат DRM. Потенційна невдача: якщо компанія, що захищає контент за допомогою DRM, збанкрутує або припинить підтримку системи DRM, користувачі не зможуть отримати доступ до придбаного контенту. Таке вже траплялося в минулому, внаслідок чого споживачі залишалися без доступу до своїх електронних бібліотек.

В якості прикладу системи DRM, можна розглянути Denuvo –програмне забезпечення DRM, крім того, це рішення захисту для ігрової індустрії, яке не дає змоги людям зламувати та розповсюджувати ігри, а також виявляє та блокує шахраїв у багатокористувацьких іграх [4]. Перш за все, Denuvo не є системою захисту від несанкціонованого доступу. Розробники повинні інтегрувати свій код із Denuvo, включно з маркуванням функцій, які не впливають на продуктивність, але є важливими для обфускації Denuvo. Наприклад, це може бути функція, що ініціалізує ядро програми. Її слід запускати тільки один раз, тому її уповільнення не вплине на загальну продуктивність.

На перший погляд, це проміжне програмне забезпечення для захисту від шахрайства, яке аналізує ігрові файли та читерські інструменти, встановлені на комп'ютері. Як і багато інших античит-програм, Denuvo Anti-Cheat використовує драйвери рівня ядра. Іншими словами, коли Denuvo працює, він має найвищий рівень привілеїв, який тільки може мати програмне забезпечення, крім ядра операційної системи.

Список використаних джерел

1. Gvozdov Roman et al. "Method of Biometric Authentication with Digital Watermarks." 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). IEEE, 2021.

2. «What is Digital Rights Management (DRM)?», Conor Roach, May 2023.

3. «A Publishers Guide to DRM: What Is DRM, How It Works, and When Publishers Need It», Video Technology, April 2023, посилання на джерело: https://target-video.com/what-is-drm/

4. «What Is Denuvo and Why Do Some Gamers Hate It?», Debarshi Das, April 2023, посилання на джерело: https://www.makeuseof.com/what-is-denuvo/

УДК 004.056:355.451

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ В СИСТЕМАХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Лось Д.І.
Науковий керівник – асистент Гвоздьов Р. Ю.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: dmytro.los1@nure.ua

The transition of client services online and the shift to remote work by banks demand a reassessment of information and cybersecurity. Even minor security incidents can cost financial institutions reputation and business loss. Essential protective measures include continuous security level evaluation, penetration testing, and cybersecurity risk assessment. Ongoing training for users and administrators focuses on reducing the impact of the "human factor." Monitoring events, incident response, and behavioral analysis are crucial amid the rising cyber threat landscape. Machine learning, secure endpoints, and server management enhance transaction security.

Перехід багатьох клієнтських сервісів в онлайн, а також вимушене переведення банками і фінкомпаніями своїх співробітників на віддалену роботу вимагає перегляду заходів інформаційної та кібербезпеки [1].

Навіть незначний інцидент у сфері безпеки платежів, як наприклад, витік конфіденційних даних, може коштувати фінансовій установі втрати репутації, що рівнозначно втраті бізнесу.

Для базового захисту своїх систем, операцій і даних потрібно зробити такі дії:

1. Постійна перевірка рівня захищеності і оцінка вразливостей – тестів на проникнення [2]. Постійний аудит та тест на проникнення для виявлення слабких місць у системі захисту фінансових установ. Тест на проникнення включає аналіз елементів IT-інфраструктури, прав доступу, привілейованих облікових записів та можливостей відновлення після можливої атаки.

2. Постійне навчання персоналу для зменшення впливу "людського фактора" на кібербезпеку. Тести на стійкість до соціальної інженерії для перевірки уваги користувачів. Тренінги для виявлення ознак атак, правильної реакції та роботи в інцидентах безпеки. Спеціальні тренінги для банківських працівників, які включають ідентифікацію загроз, дії при атаках та реагування на інциденти.

3. Моніторинг подій і реагування на інциденти [3]. З урахуванням зростання числа кібератак важливо ретельно враховувати всі аспекти безпеки для уникнення негативних наслідків. Основні заходи включають:

1) ведення журналу та записів системного аудиту на всіх пристроях;
2) збір даних, порівняння і аналіз подій з різних джерел;
3) виявлення загроз і реагування на них, аналіз поведінки.

4. Забезпечення безпеки кінцевих точок за допомогою аналізу даних та поведінкового аналізу. Каталогізація зовнішніх систем та блокування підозрілих IP, доменів і веб-сайтів.

5. Керування ідентифікацією і привілейованими обліковими записами. Централізоване керування ідентифікацією та доступом привілейованих облікових записів є ключовим аспектом для захисту конфіденційної інформації від кібератак:

1) використання greylisting для запобігання надання незнайомим додаткам доступу в Інтернет і отримання прав на запис, читання, зміну прав, необхідних для шифрування даних;
2) використання whitelisting на серверах для визначення дозволених команд і додатків, які можна запускати;
3) регулювання прав локальних адміністраторів, використання принципу найменших привілеїв, видача необхідних привілеїв лише на певний час, контроль над додатками;
4) повне приховування облікових даних (паролів, ключів), завдяки чому користувачі не зможуть передати ці дані зловмисникам;
5) керування паролями (складність, періодичність, термін дії);
6) використання багатофакторної автентифікації для всіх користувачів.

6. Моніторинг стану інфраструктури. За допомогою функції керування моніторингом стану інфраструктури здійснюється:

1) моніторинг за рівнем використання ресурсів (CPU, RAM, HDD);
2) аналіз шляхів доступу до даних і виконання виробничої діяльності;
3) оцінка ризиків і впливу.

У зв'язку з постійним тиском кіберзагроз, важливо вдосконалювати бізнес-процеси та використовувати сучасні технології для забезпечення ефективного кіберзахисту. Фінансові установи повинні виявляти та протистояти загрозам, реалізовувати кращі світові практики та вдосконалювати технологічні рішення для мінімізації ризиків та забезпечення безпеки операцій в онлайн-банкінгу та інших платіжних системах.

Список використаних джерел

1. Minfin. URL:https://minfin.com.ua/ua/2021/08/31/70762402/ (дата звернення: 12.03.2024).
2. Poddubnyi V., Sievierinov O., Pustomelnik O. Менеджмент вразливостей як складова частина політики безпеки ІТС. // Системи управління, навігації та зв’язку. Збірник наукових праць 4.62 (2020): 55-58.
3. Ушатов В., Сєвєрінов О.В. "Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки." (2019).

УДК 004.056.53:355.451]:004.7 https://doi.org/10.30837/IYF.PCEIP.2024.117

РІЗНОВИДИ ТА МЕТОДИ АТАК НА DNS СЕРВЕРИ

Ляшко М.С.
Науковий керівник – ст. викл. В'юхін Д.О.
Харківський Національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: mykyta.liashko@nure.ua

This work is devoted to the growing threat of cyberattacks on DNS systems and their implications for Internet security. It explains what DNS is and the role it plays in determining IP addresses for domain names. The importance of learning about and understanding the different types of DNS attacks, such as zero-day, rapid-flow, and DNS spoofing, along with their potential consequences, is highlighted. It also discusses effective defence strategies to help prevent or mitigate the effects of such attacks.

Останнім часом постійно збільшується кількість атак на електронні ресурси [1]. При цьому одним з основних факторів захисту є забезпечення безпеки DNS серверів.

Мета доповіді полягає в дослідженні різновидів та методів захисту від атак на Domain Name System (DNS). Доповідь спрямована на розкриття сутності DNS атак, визначення їхніх типів та потенційних наслідків для інформаційної безпеки. Основна мета – висвітлити ефективні та сучасні стратегії захисту, які допомагають уникнути або пом'якшити негативні наслідки DNS атак.

Хоча система доменних імен (DNS) є досить потужною, вона, здається, менше орієнтована на безпеку, тому за останні кілька років спостерігається різке збільшення DNS-атак, і ці атаки не обмежуються лише невеликими веб-сайтами. Багато популярних сайтів, таких як Reddit, Spotify, Twitter, також скаржаться на недоступність для тисяч своїх користувачів.

Розглянемо типи DNS-атак:

– Zero—day attack (Атака нульового дня): У цьому типі атаки зловмисник використовує раніше невідому вразливість у програмному забезпеченні сервера DNS або стеку протоколів.

– Fast Flux DNS (Швидкий потік): Хакери змінюють частоту DNS-запису на вищу, щоб перенаправити DNS-запити. Цей метод допомагає зловмиснику уникнути виявлення.

– DNS-Spoofing (DNS-спуфінг): DNS-спуфінг, також відомий як отруєння кешу DNS, це тип взлому комп'ютерної безпеки. Зловмисники або хакери пошкоджують весь DNS-сервер, замінюючи схвалений IP-адрес фальшивим

IP-адресом в кеші сервера. Таким чином, вони перенаправляють весь трафік на злонамірений веб-сайт і збирають важливу інформацію.

Схематична робота атаки на DNS-сервер представлена на рисунку 1.

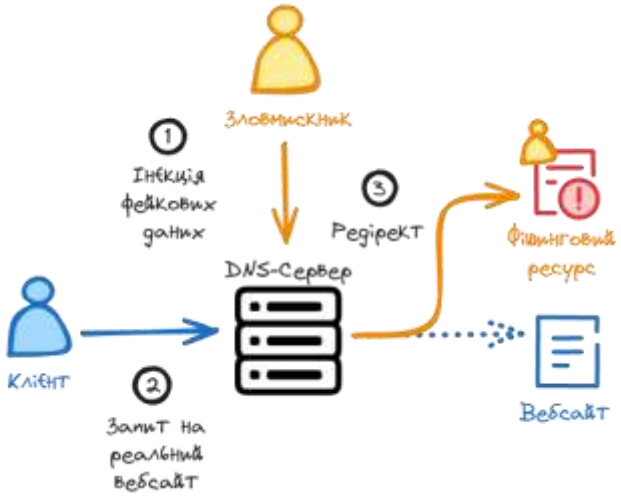


Рисунок 1 – Схематична робота атаки на DNS-сервер

DNS-спуфінг, а також інші методи для отруєння кешу, виконують тільки частину роботу для зловмисників. Наступний і головний крок є відключення користувачів від доступу в Інтернет за рахунок веб-сайтів, які залишились в локальному кеші.

Це одна з найпоширеніших технік фішингу, яку зловмисники регулярно використовують для крадіжки інформації. Оскільки користувачі вводять правильну адресу домена у своїх браузерах, вони ніколи не розуміють, що отримують доступ до підробленого або вкраденого веб-сайту.

Тому стає складніше виявити цю атаку. Іноді користувачі не можуть ідентифікувати її до закінчення часу життя (time to live (TTL)). TTL або час для життя — це час, коли DNS-розпізнавач пам'ятає DNS-запит до закінчення терміну його дії.

DNS-атаки (атаки, спрямовані на систему доменних імен) можуть бути широким спектром, і для їх захисту використовують різні методи. Ось деякі популярні методи захисту:

– DNSSEC (DNS Security Extensions): DNSSEC є розширенням DNS, яке надає механізми для перевірки цілісності та автентичності даних DNS. Вона захищає від атак, таких як DNS-підробка (DNS spoofing) та DNS-отруєння.

– Фаєрволи (Firewalls): Використання фаєрволів може допомогти обмежити доступ до DNS-серверів та блокувати небезпечний трафік. Регулярно оновлюйте правила фаєрвола, щоб враховувати нові загрози.

– Моніторинг трафіку: Системи моніторингу трафіку можуть виявляти незвичайний або великий обсяг запитів до DNS-серверів, що може бути

індикатором DNS-атаки. Автоматизовані системи можуть блокувати або обмежувати такий трафік.

– Фільтрація DNS-запитів: Використання фільтрів DNS дозволяє блокувати доступ до веб-сайтів зі списком небезпечних або небажаних доменних імен. Це може допомогти захистити від атак, які використовують зловмисні домени.

– Anycast DNS: Anycast є технологією, яка дозволяє розміщувати одне і те саме IP-адресу на різних місцях у мережі. Це підвищує доступність та стійкість до витоку DNS-атак, розподіляючи трафік між кількома серверами.

– Обмеження DNS-запитів: Встановлення обмежень на кількість запитів від одного користувача або IP-адреси може допомогти уникнути перевантаження DNS-сервера через DDoS-атаки.

– Регулярні оновлення програмного забезпечення: Переконайтеся, що програмне забезпечення DNS-серверів і DNS-клієнтів регулярно оновлюється для усунення вразливостей і покращення безпеки.

– Безпека внутрішньої мережі: Захищайте внутрішню мережу від зловмисних елементів, які можуть впливати на DNS. Це включає в себе застосування методів захисту від вірусів, шкідливих програм і внутрішніх загроз.

– Отримуйте регулярне уявлення про те, що відбувається в мережі. Ви можете скористатися такими технологіями, як IPFIX, NetFlow і інші, щоб досягти бажаного результату.

Для зменшення ризиків DNS-атак адміністратори серверів повинні прийняти кілька заходів безпеки. Це включає використання оновлених версій програмного забезпечення DNS та регулярне налаштування серверів для здійснення дублювання. На особистому рівні користувачі також можуть допомогти уникнути загроз безпеки, скинувши свій DNS-кеш. Атаки на систему DNS можуть мати серйозні наслідки для безпеки даних та інформаційної інфраструктури, тому важливо вжити всі можливі заходи для їх уникнення.

Список використаних джерел

1. Сєвєрінов О.В., Шевцов В.О., Сокол-Кутиловська А.С. Аналіз сучасних методів атак на електронні ресурси органів управління. // Системи озброєння і військова техніка 1 (2017): 65-68.

2. What Are DNS Attacks? Paloalto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-a-dns-attack (дата звернення: 03.03.2023)

3. What is DNS Spoofing | Cache Poisoning Attack Example. Imperva. URL: https://www.imperva.com/learn/application-security/dns-spoofing/ (дата звернення: 03.03.2023)

4. DDoS-атаки з DNS-посиленням: як це працює і як їх зупинити?. Triolan.net. URL: https://triolan.net/wiki/knowledgebase.php?article=11 (дата звернення: 03.03.2023)

5. Колтаков О. А. Аналіз основних показників якості з'єднання з сервером DNS / О. А. Колтаков // Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2023): матеріали дев'ятої Міжнародної науково-технічної конференції, 7 грудня 2023 р. – Харків : ХНУРЕ, 2023. – С. 91-92.

УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.120

ЕФЕКТИВНІСТЬ ТА МАЙБУТНІЙ РОЗВИТОК СИСТЕМ ЗБОРУ МЕРЕЖЕВИХ АРТЕФАКТІВ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

Малахова А. А.
Науковий керівник – Євгеньєв А. М.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
email: anna.malakhova@nure.ua

This report explores the current state, effectiveness, and future development prospects of network artifact collection systems, focusing on their role in cybersecurity. It highlights the importance of evolving these systems to cope with the increasing complexity of cyber threats in our digital world. The discussion encompasses the current landscape of network artifact collection methods, their limitations, and the potential for future improvements. Emphasis is placed on innovative approaches such as automation, artificial intelligence integration, and blockchain technology to enhance the efficiency of these systems. The report concludes by underscoring the necessity of continued research and investment in advancing these technologies to ensure robust cybersecurity measures.

У сучасному цифровому світі, де мережева активність постійно зростає, а загрози кібербезпеки стають все складнішими, ефективні системи збору мережевих артефактів відіграють важливу роль у виявленні та протидії кіберзагрозам. У цієї доповіді розглянемо сучасний стан та майбутні перспективи розвитку таких систем, а також ключові інновації, які можуть забезпечити їхню ефективність та надійність [1].

Сучасні системи збору мережевих артефактів базуються на різноманітних технологіях, включаючи сенсори, журнали подій, системи моніторингу мережевого трафіку тощо [2]. Однак, багато з цих систем мають обмежену масштабованість, низьку швидкість аналізу та виявлення аномалій, а також вимагають значних зусиль для обробки та аналізу отриманих даних.

Ефективність систем збору мережевих артефактів є ключовим аспектом в забезпеченні кібербезпеки та виявленні потенційних загроз. Ці системи відіграють важливу роль у зборі, аналізі та моніторингу мережевої активності, дозволяючи виявляти аномальні зміни та підозрілу поведінку, яка може свідчити про кібератаку або інші загрози безпеці [3].

Майбутні перспективи розвитку систем збору мережевих артефактів досить передбачувані і можуть характеризуватись такими аспектами як:

– автоматизація та інтелектуалізація: застосування штучного інтелекту та машинного навчання для автоматичного виявлення аномалій та відстеження кіберзагроз;

– розширення області застосування: розвиток систем збору мережевих артефактів для виявлення загроз у Інтернеті речей, хмарних середовищах, облікових записах користувачів та інших аспектах цифрового життя;

– безпека та конфіденційність: розробка технологій шифрування, анонімізації та захисту персональних даних для забезпечення конфіденційності та захисту інформації, зібраної системами збору мережевих артефактів.

Якщо говорити за інновації у розвитку збору мережевих артефактів, то використання блокчейн технологій і розвиток нових алгоритмів аналізу даних – це необхідні міри для забезпечення невідворотності, цілісності та автентифікації даних, зібраних системами збору мережевих артефактів, а також для виявлення найбільш складних та витончених атак, які можуть ухилятися від традиційних методів виявлення загроз [4].

Майбутній розвиток систем збору мережевих артефактів відкриває перед нами широкі перспективи для підвищення безпеки та ефективності цифрових мереж. Інновації в області штучного інтелекту, машинного навчання, блокчейн технологій та аналізу даних дозволять побудувати більш реактивні та надійні системи, які забезпечать нам захист від кіберзагроз у майбутньому. Для досягнення цілей необхідно продовжувати інвестувати в дослідження та розробки в цих напрямках, що дозволить забезпечити нам безпеку та стабільність у цифровому середовищі [5].

Список використаних джерел:

1. Arvidsson V., Mønsted T. Generating innovation potential: How digital entrepreneurs conceal, sequence, anchor, and propagate new technology. The Journal of Strategic Information Systems. 2018. Vol. 27, no. 4. P. 369–383. (дата звернення: 05.03.2024).

2. Сєвєрінов О.В., Хрєнов А.Г. Аналіз сучасних систем виявлення вторгнень. // Системи обробки інформації 6 (2014): 122-124.

3. Cybersecurity and Network Security / A. Guha et al. Wiley & Sons, Limited, John, 2022.

4. Staff J. f. A. Cybersecurity Log Book: Cybersecurity Log. Independently Published, 2017.

5. Local Network Security. Cybersecurity. Indianapolis, Indiana, 2018. P. 423–447.

УДК 004.056 https://doi.org/10.30837/IYF.PCEIP.2024.122

ХМАРНІ ОБЧИСЛЕННЯ ЯК РІШЕННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІКС

Мартиненко Я.А.
Проф., к.т.н., доц. Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: yana.martynenko@nure.ua

The disclosure of the relevance of this topic in the XXI century. The definition of cloud computing and the aim of using clouds in companies, their advantages above on-premise computing. The description of cloud computing functions, their brief description. The overview of two types of cloud: private and public, main features and key difference between them, their influence on information security. The overview of cloud computing components, their brief description. The consideration of three main kinds of cloud computing providers: Infrastructure as a Service (Iaas), Platform as a Service (PaaS), Software as a Service (SaaS).

Хмарні обчислення – це надання обчислювальних потужностей, баз даних, сховищ, додатків та інших IT-ресурсів на вимогу через Інтернет за допомогою платформи хмарних сервісів з оплатою лише за фактично використані ресурси.

Завдяки хмарним обчисленням немає необхідності у створенні великих інвестицій в апаратне забезпечення та їхнім управлінням. Замість цього хмарні сервіси надають конкретний тип і розмір обчислювальних ресурсів, який необхідний для реалізації у компанії. На відміну від локальних обчислень, які захищають комп'ютери користувачів, запобігають доступу шкідливих програм і керують знімними носіями, схема безпеки на основі хмарних обчислень повинна зосередитися на забезпеченні безпечного зв'язку з віддаленими системами.

Певні характеристики хмари є важливими для надання послуг, які дійсно представляють модель хмарних обчислень і задовольняють очікування споживачів, а хмарні пропозиції повинний мати можливість самообслуговування (робити запити, налаштовувати, оплачувати та користуватися послугами без втручання людини-оператора), враховувати використання (обирати необхідну кількість ресурсів), виставляти рахунок за використання (дає можливість коросткрокові оплати, що дозволяє користувачам звільнити ресурси, як тільки вони їм стануть не потрібними), а також бути гнучким (забезпечення ресурсами в будь-якій кількості в будь-який час) та кастомізованим (наявність привілейованого доступу до віртуального

серверів). Через низку зазначених функцій хмарні обчислення стають найкращим рішенням для розгортаннях систем у компаніях, а також дають можливість ефективно захищати інформацію.

Розрізняються два типи хмар: публічні та приватні. У публічній хмарі дані та програми зазвичай зберігаються в Центрі обробки даних ЦОД провайдера, які беруть на себе відповідальність за його управління та обслуговування. Крім того, у такій хмарі сховище буде спільним для кількох користувачів залежно від їхніх індивідуальних потреб або потреб бізнесу, що буде ставити під загрозу безпеку даних організації. Прикладами публічних хмарних сервісів є Google Print, Google Docs, Microsoft Office 365, Amazon EC2, та Amazon Cloud Player та інше. Всі вони мають спільну модель щомісячних операційних витрат і майже не мають авансових капітальних.

На відміну від публічної хмари приватна надає виділену інфраструктуру для однієї компанії, якою можна керувати самостійно або через стороннього постачальника послуг. Зазвичай, якщо компанія є власником приватної хмари, вона несе відповідальність за обслуговування та управління власним ЦОДом, що безсумнівно позитивно впливає на захист даних. Це дає можливість знизити ризики загрози внутрішніх атак на інфраструктуру, мати повний контроль над нею, а також знизити ризики несанкціонованого доступу до даних.

Хмарні обчислення надають розробникам та IT-відділам можливість зосередитися на тому, що має найбільше значення, і уникнути виконання однотипної роботи, такої як закупівлі, технічне обслуговування та планування потужностей. З ростом популярності хмарних обчислень з'явилося кілька різних моделей і стратегій розгортання, які допомагають задовольнити конкретні потреби різних користувачів. Кожен тип хмарного сервісу та метод розгортання надають різні рівні контролю, гнучкості та управління. Можна виокремити такі типи як:

– Інфраструктура як сервіс. Infrastructure as a Service (Iaas): містить структурні елементи хмарних IT і надає доступ до мережевих функцій, комп'ютерів та місця для зберігання даних. IaaS забезпечує найвищий рівень гнучкості та управлінського контролю над IT-ресурсами;

– Платформа як сервіс. Platform as a Service (PaaS): позбавляє організацію необхідності керувати базовою інфраструктурою і дозволяє зосередитися на розгортанні та управлінні додатками. Це допомагає бути більш ефективними, оскільки немає потреби турбуватися про закупівлю ресурсів, планування потужностей, обслуговування програмного забезпечення або встановлення виправлень;

– Програмне забезпечення як сервіс. Software as a Service (SaaS): надає готовий продукт, який запускається та управляється постачальник послуг. Поширеним прикладом програми SaaS є веб-пошта, яку можна використовувати для того, щоб надсилати та отримувати електронну пошту без необхідності керувати додаванням функцій до поштового продукту або обслуговувати сервери та операційні системи, які серверів та операційних систем, на яких працює поштова програма.

Таким чином, розглянувши хмарні обчислення, можна виділити суттєві переваги та недоліки. Серед переваг наявне підвищення гнучкості та швидкості, зниження витрат на експлуатацію та обслуговування ЦОД, а до недоліків відносяться обмежений контроль та залежність від Інтернету. Тож, хмарні обчислення відіграють важливу роль у забезпеченні доступу до обчислювальних ресурсів та послуг і дають можливість захищати дані на рівні з локальними обчисленнями.

Список використаних джерел:

1. John Wiley & Sons. Cloud Services For Dummies®, IBM Limited Edition. URL: https://www.ibm.com/cloud-computing/files/cloud-for-dummies.pdf (date of access: 03.03.2024).

2. Lysakov V., Sievierinov O., Taran I. ecurity of Web Applications Using AWS Cloud Provider. 2021: Fifth International Scientific and Technical Conference "COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES", Kharkiv, 2 March 2024. Харків, 2021

3. Ruparelia, Nayan. Cloud Computing. URL: https://s3.amazonaws.com/arena-attachments/911381/0ea8a9793158a95d9b91911e49240a43.pdf (date of access: 03.03.2024).

4. Wong Tsz Lai, Hoang Trancong, Steven Goh. Software Development Tools and Technologies.Ch1: Cloud Computing. URL: https://www.comp.nus.edu.sg/~seer/book/2e/Ch01.%20Cloud%20Computing.pdf (date of access: 02.03.2024).

5. Рудий С., Сєвєрінов О. ОСЛІДЖЕННЯ МОДЕЛІ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ ХМАРНИХ СЕРВІСІВ. Проблеми інформатизації : десята міжнародна науково-технічна конференція, м. Харків, 3 берез. 2024 р. Харків, 2022.

УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.125

ПРОТОКОЛ ДОСЯГНЕННЯ КОНСЕНСУСУ OUROBOROS ДЛЯ БЛОКЧЕЙН МЕРЕЖ

Набойщиков Б.Ю.
Науковий керівник – PhD, доцент Родінко М. Ю.
Харківський національний університет ім. В.Н. Каразіна, каф. МСіТ, м. Харків, Україна
naboishchykov2020ks13@student.karazin.ua

This work is dedicated to providing a general description of the Ouroboros protocol as the first developed Proof-of-Stake consensus protocol built on a secure blockchain, along with its formal rationale, as well as the concept of Verifiable Random Function, which is commonly used in the protocol.

Блокчейн протоколи на основі Proof of Work (PoW), такі як Bitcoin, розраховують на велику кількість ресурсів для генерації блоків в ланцюжках записів. І хоч на практиці це може й не бути проблемою для деяких компаній або користувачів – альтернативний протокол взаємодії з блокчейном все ж таки мав бути розроблений для потреб клієнтів з вимогами до ресурсів. Протокол на основі Proof of Stake (PoS) – «Ouroboros» запропонував свою концепцію роботи яка вирішувала проблеми протоколів PoW, гарантуючи такі ж стандарти безпеки.

До недавнього часу блокчейн протоколи PoW мали лідируючу позиції на ринку – але різкий перехід таких платформ як Ethereum на PoS – призвело до підвищеної зацікавленості в таких методах. Також, можливість блокчейну створювати децентралізовану, прозору та незмінну систему запису, що може ефективно взаємодіяти з різноманітними пристроями в мережі IoT розширює можливості використання PoS[1].

Proof-of-Stake (PoS) — широко поширений альтернативний механізм, який працює за принципом «підтвердження частки». Замість того, щоб покладатися на енергоємне обладнання для перевірки транзакцій, PoS використовує мережеві пристрої або вузли для перевірки та запису транзакцій, а також отримує винагороду у вигляді криптовалюти. Замість хешування даних процес перевірки в PoS в основному визначається випадковістю обчислень, при цьому вага участі вузла залежить від суми фінансової застави або частки, яку він вніс у мережу через ставку[2].

Алгоритми PoS використовують різні методи для вибору вузлів, які слугуватимуть валідаторами. Імовірність того, що вузол стане валідатором,

зростає з кількістю токенів, які він поставив, а також є більша ймовірність відбору для вузлів, які зберігають свої токени протягом більш тривалого періоду часу, не витрачаючи їх.

Хоча процес вибору валідатора в PoS надає перевагу учасникам з більшою часткою, цей протокол включає випадкові механізми для запобігання централізації, забезпечуючи справедливий і неупереджений відбір[3].

Ouroboros — це перший доведено безпечний протокол Proof-of-Stake і перший протокол блокчейну, заснований на рецензованих дослідженнях. Ouroboros поєднує унікальну технологію та математично перевірені механізми для забезпечення безпеки, стабільності та масштабованості блокчейнів, які його використовують.

Ouroboros використовує криптографію, комбінаторику та математичну теорію ігор для забезпечення цілісності, довговічності та продуктивності протоколу. Він забезпечує такий же рівень безпеки, як консенсус Proof-of-Work. Застосовуючи випадковий вибір лідера та вимагаючи, щоб принаймні 51% від загальної частки належало чесним учасникам, протокол гарантує безпеку. Крім того, він проходить постійний розвиток і ретельний аналіз безпеки. Управління мережею розподіляється між пулами розміщення, якими керують оператори вузлів із необхідною інфраструктурою для постійного та надійного з'єднання. Лідер слота обирає пул ставок для кожного слота, і пул отримує винагороду за додавання нового блоку до ланцюжка[4]. Стабільний консенсус в Ouroboros досягається завдяки використанню верифікованої випадкової функції(VRF).

У 1999 році група інформатиків і математиків, у тому числі Сільвіо Мікалі, Майкл Рабін і Саліл Вадхан, представили концепцію випадкової функції, що піддається перевірці (Verifiable Random Function, VFR) в опублікованій статті. З тих пір було зроблено прогрес для вдосконалення технології. У 2015 році Денніс Гофхайнц і Тібор Ягер використали криптографію еліптичної кривої для створення високозахищеного VRF. Пізніше, у 2019 році, Нір Бітанскі продемонстрував, що VRF можна побудувати за допомогою різних загальних примітивів, розширюючи можливості за межі алгебраїчних конструкцій. VRF, по суті, є генераторами випадкових чисел (RNG), які проходять криптографічну перевірку. Після його використання спеціалізований алгоритм забезпечує підтвердження VRF. Щоб кваліфікуватись як VRF, функція f має відповідати певним умовам.

Представлення f є компактним і неявним, що ускладнює ефективне обчислення. З іншого боку, існує компактне та явне представлення f, яке дозволяє «власнику» ефективно обчислювати його.

Таким чином, дану пару можна розглядати як відкритий ключ PKf та його відповідний секретний ключ SKf.

Більшість ГВЧ не генерують криптографічно перевірювані випадкові числа, що робить їх сприйнятливими до маніпуляцій, таким чином обмежуючи їх використання. Забезпечуючи безпеку випадкових чисел, VRF відкриває багато важливих застосувань, наприклад:

– Інтернет-безпека – VRF використовується для захисту повідомлень системи доменних імен (DNS);

– технологія нульового знання – VRF використовується для розробки протоколів захисту від нульового розголошення;

– неінтерактивна система лотерей – VRF забезпечує чесні та ефективні результати лотереї;

– блокчейн і смарт-контракти – VRF став важливою частиною децентралізованих протоколів і смарт-контрактів [5].

Таким чином, протокол консенсусу Ouroboros на основі Proof of Stake дозволяє досягти високого рівня безпеки за допомогою концепції VFR, при цьому, забезпечуючи значну швидкість обробки транзакцій та заощаджуючи енергоресурси системи.

Список використаних джерел

1. Просолов В. В. Використання блокчейн технології з машинним навчанням для безпечних IoT / В. В. Просолов, Г. З. Халімов // Проблеми інформатизації : тези доповідей одинадцятої міжнар. наук.-техн. конф., 16–17 листопада 2023 р. – Баку-Харків-Бельсько-Бяла, 2023. – Т. 2, секція 3,6. – С. 46. (дата звернення: 04.03.2024).

2. Blockchain Technologies: Probability of Double-Spend Attack on a Proof-of-Stake Consensus / Mikolaj Karpinski, Lyudmila Kovalchuk, Roman Kochan, Roman Oliynykov, Mariia Rodinko, Lukasz Wieclaw. Sensors. 2021. Vol. 21, no. 19. P. 6408. URL: https://doi.org/10.3390/s21196408. (дата звернення: 04.03.2024).

3. Blockchain Consensus Algorithms: A Survey. Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Mohammad A. Hoque, Alan Colman. 2020. 39 c. URL: https://www.researchgate.net/publication/338738073_Blockchain_Consensus_Algorithms_A_Survey. (дата звернення: 04.03.2024).

4. Roman Oliynykov, Aggelos Kiayias, Alexander Russell, Bernardo David. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. 2017. 67 c. URL: https://iohk.io/en/research/library/papers/ouroboros-a-provably-secure-proof-of-stake-blockchain-protocol/. (дата звернення: 02.03.2024).

5. Micali S., Rabin M., Vadhan S. Verifiable random functions. 40th annual symposium on foundations of computer science (17-19 січня 1999р.). New York, USA (date of access: 04.03.2024).

УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.128

ПРИНЦИПИ РОБОТИ ZKP ТА ПРОТОКОЛ ІДЕНТИФІКАЦІЇ ШНОРРА

Наконечний В.В.
Науковий керівник – к.т.н, доц. каф. ІУС Сердюк Н.М.
Харківський національний університет радіоелектроніки,
м.Харків, Україна
e-mail: volodymyr.nakonechnyi@nure.ua

Zero-Knowledge Proof is a cryptographic method used in digital authentication to verify information without revealing sensitive data. This allows the parties to confirm the accuracy of the information without revealing the details. This approach is valuable to governments and organizations seeking to protect data privacy while simultaneously verifying information. Zero-knowledge verification is used in a variety of digital contexts, including identity verification, authentication, anti-spam, secure payments, account management, and more.

У різних сферах діяльності часто виникають ситуації, коли необхідно підтвердити виконання роботи, залишаючи деталі виконання конфіденційними. Один із типових прикладів - передача важливих відомостей, де потрібно підтвердити певні характеристики без розголошення додаткової інформації. Сюди входять аутентифікація користувача, онлайн платежі, електронні вибори, боротьба зі спамом, управління акаунтами, та збереження анонімності.

Розуміння суті доказу нульового знання можна проілюструвати за допомогою ігрової колоди карт. Одна сторона може передати іншій карту, стверджуючи, що вона має певний колір, але з об'єктивних причин не надає докладні деталі. У таких випадках сторона, що передає карту, може взяти колоду і відокремити всі картки певного кольору, показуючи тим самим, що вона дійсно складається з карт одного кольору. Це демонструє, що передана карта відповідає вказаному кольору без розголошення додаткових деталей.

Протокол Ідентифікації Шнорра (Schnorr Identification Protocol) та нульзнання (Zero-Knowledge Proofs, ZKP) є важливими концепціями в області криптографії та інформаційної безпеки.

Протокол Ідентифікації Шнорра широко використовується в області криптовалют. Наприклад, у покращеному біткойн-протоколі “Тапрут” (Taproot), який спрямований на підвищення приватності та ефективності трансакцій. Ще однією перевагою протоколу Шнорра є його стійкість до підслуховування. Навіть якщо зловмисник прослуховує певну кількість підписаних повідомлень, важко вивести закритий ключ. Іноді протокол Ідентифікації Шнорра поєднується з кільцевими підписами (Ring Signatures) для досягнення більшої анонімності.

ZKP використовуються для розв'язання різноманітних завдань, таких як доказ володіння конкретною інформацією, відтворення доказів без розкриття деталей тощо.

В області криптовалют ZKP використовуються для забезпечення конфіденційності та приватності транзакцій. Наприклад, протокол zk-SNARK використовується у Zcash. ZKP можуть служити для забезпечення безпеки мульти партійних виборів, де кожен голосуючий може підтверджувати свій вибір, не розкриваючи його. Постійно відбуваються дослідження та розробки нових протоколів нуль-знання, що розширюють можливості застосування цих концепцій.

Обидва ці принципи визначають сучасні стандарти конфіденційності та безпеки в різних сферах, від криптовалют до кібербезпеки. їх комбінування та застосування можуть сприяти створенню ефективних та безпечних інформаційних систем.

Подана вище ситуація є наочним прикладом застосування доказів нульового знання у реальному житті. Проте, подібні випадки можуть виникати і в цифровому просторі, коли особі необхідно підтвердити певні відомості чи коректність даних, не розкриваючи деталей про виконану роботу. Для ефективного використання алгоритмів доказів нульового знання у цифровому середовищі, необхідно дотримуватися певних принципів [2]:

1. чесність сторін. Якщо твердження коректне, то чесна сторона, яка його доводить, зможе це довести іншій чесній стороні отримувачу;
2. обгрунтованість наведених доказів. Якщо твердження не коректне, то сторона доведення не може задовольнити сторону отримувача;
3. суть доказу нульового знання полягає в тому, що при наданні доказів особі абсолютно не має бути відомо додаткової інформації про твердження, крім того, що воно є правильним.

Також розрізняють різні схеми підтвердження доказу, а саме інтерактивна і не інтерактивна відповідно [2]:

— інтерактивна схема вимагає того, аби існувала сторона, що проводить підтвердження того, що твердження є вірним – верифікатор;

— не інтерактивна схема – передбачає, що створення доказу базується на загальних параметрах і що доказ може бути перевірений ким завгодно.

Прикладом роботи інтерактивної схеми є верифікація особистості у мобільному додатку «Дія» за допомогою сервісу BANKID. Використовуючи банківський додаток для верифікації в «Дія», можна підтвердити свою особистість без передачі чутливих даних.

Проте із не інтерактивною схемою коли немає верифікатора найкраще підходить не інтерактивний протокол ідентифікації Шнорра [1]. Він передбачає собою підтвердження того, що одна людина знає те, що і інша.

Протокол ідентифікації Шнорра реалізується за таким алгоритмом [3]:

1. Визначимо просте число p і g, а також секретний ключ x.
2. Обчислимо значення X за наступною формулою:

$$X = g^x mod\ p$$

3. Сторона, яка доводить генерує випадкове число y і обчислює значення Y:

$$Y = g^y mod\ p$$

4. Сторона, яка доводить надсилає стороні верифікатору значення Y.
5. сторона верифікатор генерує випадкове число c і надсилає його стороні, що доводить.
6. Сторона, яка доводить отримує c і обчислює значення z за формулою:

$$z = y + c * x$$

7. Сторона доведення надсилає стороні верифікатора значення z.
8. Сторона верифікатор проводить наступні операції по верифікації отриманих значень, а саме обчислює дві змінні v1 і v2:

$$v1 = g^z mod\ p$$

$$v2 = (Y * X^c) mod\ p$$

9. Верифікатор обчислює змінні v1 і v2 та перевіряє їх на рівність. Якщо вони рівні, значення вважається правильним, в іншому випадку - неправильним.
10. У процесі верифікації, якщо значення v1 і v2 однакові, це свідчить про те, що і верифікатор, і сторона, що доводить, знають, що значення, яке має сторона, що доводить, ідентичне значенню сторони верифікації.

Реалізація роботи алгоритму ідентифікації Шнорра наведена за посиланням: https://colab.research.google.com/drive/1-BR95Wz-ip5tLvhSE0Zk8PBKI2AdrFjh?usp=sharing.

Список використаних джерел

1. 8235. RFC. Official edition. Newcastle upon Tyne, 2017. 12 p. 4.
2. Computerphile. Zero Knowledge Proofs - Computerphile, 2017. *YouTube*. URL: https://www.youtube.com/watch?v=HUs1bH85X9I (date of access: 29.02.2024).
3. Schnorr Identification Scheme - GeeksforGeeks. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/schnorr-identification-scheme/ (date of access: 29.02.2024).

УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.131

МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ ВЕБ-ДОДАТКІВ

Неізвєсна М.Р.
Науковий керівник – к.т.н., доцент Балагура Д.С.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: mylana.neizviesna@nure.ua

This work is devoted to exploring methods and tools for detecting vulnerabilities in web applications, addressing the critical need for ensuring digital security. The detection and mitigation of vulnerabilities in web applications are paramount to safeguarding sensitive information and preventing unauthorized access or attacks. This study delves into diverse approaches such as active and passive scanning, code analysis, penetration testing, and fuzzing techniques, along with an overview of popular tools including Burp Suite, OWASP ZAP, Acunetix, Nessus, and Qualys.

У сучасному цифровому світі, вкрай залежному від мережі Інтернет, веб-додатки стають все більш невід'ємною частиною повсякденного життя: їх використовують для здійснення фінансових операцій, спілкування, роботи та багатьох інших цілей. Однак ця всеосяжна використовуваність веб-додатків також призводить до збільшення числа кіберзагроз, які спрямовані на них. Хакери та зловмисники постійно шукають вразливості веб-сайтів, щоб отримати несанкціонований доступ до конфіденційної інформації хосту або вчинити інші злочинні дії. Отже, виявлення та вирішення вразливостей сайтів стає надзвичайно важливим завданням для забезпечення цифрової безпеки.

Веб-додатки піддаються різного роду вразливостям, таким як кросс-сайт скриптінг (XSS), вразливості вводу, витік інформації, вразливості SQL-ін'єкцій та інші, що можуть призвести до компрометації безпеки сайту та даних користувачів. Методи перевірки вразливостей необхідні для виявлення та усунення слабких місць у програмному забезпеченні, мережах і системах [1]. Ось чотири поширені методи [2]:

1) Активне тестування передбачає активне дослідження та взаємодію з цільовою системою для виявлення вразливостей. Це може включати такі методи, як тестування нечіткості, тестування на проникнення та динамічне тестування безпеки додатків (DAST). Під час активного тестування тестувальники навмисно намагаються використовувати вразливості, щоб визначити їх серйозність і вплив.

2) Пасивне тестування передбачає моніторинг і аналіз мережевого трафіку, системних журналів та інших джерел даних без активної взаємодії з цільовою системою. Метод є менш нав’язливим і може надати інформацію про потенційні вразливості та слабкі місця безпеки. Методи пасивного тестування включають аналіз мережі, аналіз журналів і аналіз трафіку.

3) Тестування мережі зосереджується саме на оцінці безпеки мережевої інфраструктури, включаючи маршрутизатори, комутатори, брандмауери та

інші мережеві пристрої. Це може включати такі методи, як сканування вразливостей, сканування портів і відображення мережі для виявлення потенційних слабких місць і неправильних конфігурацій, якими можуть скористатися зловмисники.

4) Розподілене тестування передбачає використання кількох ресурсів тестування, таких як комп'ютери, сервери та мережі, для проведення комплексної оцінки вразливості. Метод дозволяє проводити більш масштабне та ефективне тестування, розподіляючи робоче навантаження між кількома системами. Розподілене тестування може допомогти виявити вразливості, які можуть бути неочевидними під час тестування з одного джерела.

Метою роботи є огляд методів та засобів виявлення вразливостей веб-додатків для забезпечення їхньої безпеки. В роботі розглядаються різноманітні інструменти, які допомагають ідентифікувати потенційні уразливості та запобігти можливим атакам, приділивши увагу саме пентестингу, або тестуванню на проникнення - процесі активного аналізу і випробування комп'ютерних систем, програмного забезпечення чи мереж для виявлення потенційних слабких місць, вразливостей та інших потенційних проблем з безпекою [3]. Пентестинг передбачає імітацію реальних атак для оцінки ризику, пов'язаного з можливими порушеннями безпеки. Під час пентесту (на відміну від оцінки вразливості) тестувальники не лише виявляють уразливості, якими можуть скористатися зловмисники, але й використовують уразливості, де це можливо, щоб оцінити, що зловмисники можуть отримати після успішного використання.

Інструменти для виявлення вразливостей розвиваються швидко. Вони можуть бути представлені як комерційними продуктами, так і вільно розповсюджуваними відкритими програмами. У доповіді розглядаються такі програми, як Burp Suite, OWASP ZAP, Acunetix, Nessus та Qualys.

Виявлення вразливостей веб-додатків є надзвичайно важливою складовою забезпечення їх безпеки в умовах постійно зростаючої кількості кіберзагроз. Використання різноманітних методів та інструментів для цієї мети є ключовим для забезпечення стійкості та надійності веб-додатків.

Список використаних джерел

1. Сєвєрінов О.В., Баклан Я.А. Аналіз рівня безпеки web-ресурсів. 2022.

2. Georgia Weidman, Penetration Testing A Hands-On Introduction to Hacking, 2014. 531 с.

3. Vulnerability Testing: Methods, Tools, and 10 Best Practices [Електронний ресурс] Режим доступу: https://brightsec.com/blog /vulnerability-testing-methods-tools-and-10-best-practices/

4. Лопатінський А. Розробка сканера виявлення вразливостей вебсайту на основі методів захисту від різних типів атак // Scientists and existing problems of human development: Abstracts of IX International Scientific and Practical Conference, 14–17 лист. 2023. p. Загреб, 2023. С. 380-388.

УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.133

ВІДПОВІДНІСТЬ НОРМАТИВНИХ ВИМОГ УКРАЇНИ ТА ЄС У СФЕРІ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ

Ободяк В.К.
Науковий керівник – к.т.н., доцент Снігуров А.В.
Харківський національний університет радіоелектроніки, каф. ІКІ імені В.В. Поповського, м. Харків, Україна
e-mail: viktor.obodiak@nure.ua

This work is devoted to the analysis and comparison of existing regulatory requirements in the field of cyber protection of personal data in Ukraine and the European Union. The aim is to develop recommendations for improving the regulatory regulation of cyber protection of personal data processed in the information and communication systems of Ukrainian state authorities, local self-government bodies, enterprises, institutions and organizations regardless of their form of ownership.

Інтернет дозволяє вести різну діяльність, спілкуватися в режимі онлайн де б ми не знаходились, проводити фінансові та бізнес операції, навчатися тощо. В зв’язку з цим виникають питання захисту цифрових активів компаній і організацій, а також персональних даних користувачів, які обробляються в інформаційно-комунікаційних системах (ІКС). Особливої уваги заслуговує той факт, що розвиток суспільних відносин в мережі та розвиток інформаційних систем відбувається швидше, ніж розвиток нормативно-правової бази. Враховуючи зазначене потрібне правове регулювання таких відносин. Особливо це стосується кіберзахисту персональних даних в інформаційно-комунікаційних системах.

До цього часу основну увагу більшості фахівців було зосереджено на питанні захисту саме персональних даних, а не на тому, що потрібно зробити в ІКС для захисту цих даних.

Основним нормативним документом ЄС в сфері захисту персональних даних є General Data Protection Regulation (GDPR) [1]. Даний документ регламентує порядок обробки персональних даних та встановлює вимоги до систем захисту в тих інформаційно-комунікаційних системах, в яких будуть оброблятись персональні дані. Проте даний документ більше фокусується на порядку та процедурах обробки персональних даних, питання кіберзахисту в чистому вигляді не розглядаються.

GDPR обов'язковий до виконання всіма суб'єктами господарювання, які знаходяться на території ЄС. Проте необхідно звернути увагу, що норми цього документу мають виконуватися і будь-яким іншим суб'єктом господарювання,

який обробляє персональні дані громадян ЄС, навіть якщо він знаходиться в країні, яка не є членом ЄС.

Положення GDPR зазвичай є стандартними для будь-яких систем кіберзахисту, за винятком «псевдонімізації» та концепції «конфіденційності за проектом» і «конфіденційності за замовчуванням». У GDPR «псевдонімізація» або «використання псевдонімів» – це обробка персональних даних у спосіб, який не дозволяє віднести персональні дані до конкретного суб'єкта без використання додаткової інформації. Концепція «конфіденційності за проектом» означає, що такі поняття, як «конфіденційність» та «безпека» повинні впроваджуватись в товари і послуги на самих ранніх етапах їх розробки та протягом всього життєвого циклу продукту. В свою чергу «конфіденційності за замовчуванням» – означає що в усіх продуктах і послугах повинні бути встановлені найвищі налаштування конфіденційності

В нормативно-правових актах України [2, 3] відсутні чіткі і однозначні вимоги до захисту персональних даних. Аналіз цих нормативних документів, дає можливість виділити наступні вимоги до побудови системи кібербезпеки в організаціях і суб'єктах господарювання:

1. Необхідність забезпечення конфіденційності, цілісності та доступності персональних даних (ст. 24 [3], п. 3.3, 3.13, 3.14 [2]).

2. Необхідність надання резервної копії персональних даних (ст. 24[3], п. 3.3 [2]).

Потрібно звернути увагу, що ці вимоги тільки випливають із тексту статей зазначених документів і не прописані явно.

Таким чином можна зробити висновок, що ні існуючі нормативно-правові акти України, ні основний нормативний документ Європейського Союзу GDPR щодо захисту персональних даних, не містять чітких вимог щодо забезпечення захисту цих даних в ІКС. При цьому вимоги загального регламенту про захист даних ЄС є ширшими порівняно із Законом України «Про захист персональних даних». Тому актуальною є необхідність імплементації норм GDPR в нормативні документи України щодо захисту персональних даних.

Список використаних джерел

1. Про захист фізичних осіб щодо обробки персональних даних і про вільний рух таких даних, а також про скасування Директиви 95/46 /ЕС : Регламент (ЄС) 2016/679 від 27.04.2016 р. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

2. Про затвердження документів у сфері захисту персональних даних : Наказ Уповноваж. Верхов. Ради України з прав людини від 08.01.2014 р. № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text.

3. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI: станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

УДК 004.056.5:004.056.56 https://doi.org/10.30837/IYF.PCEIP.2024.135

РОЗБІР ТА АНАЛІЗ ЗАГРОЗИ ІСНУЮЧИХ ВИДІВ DDOS-АТАК

Павлов О.А.
Науковий керівник – доц. Шаповалова А.С.
Харківський національний університет радіоелектроніки,
каф. інфокомунікаційної інженерії імені В.В. Поповського,
м. Харків, Україна
e-mail: Oleksii.pavlov2@nure.ua

The evolution of Denial of Service (DoS) attacks into sophisticated Distributed Denial of Service (DDoS) threats poses a severe risk to online entities. DDoS attacks, employing botnets, aim not to breach security but to deny authorized users access to websites. These attacks can serve as a smokescreen for other malicious activities and disrupt security measures. DDoS techniques vary, including volume-based, protocol, and application layer attacks. The constant evolution of attack methodologies, from basic scripts to distributed and adaptive strategies, requires advanced monitoring and defense mechanisms. The rise of "service malware" and the expanding attack surface through IoT devices underscore the critical need for scalable defenses against diverse DDoS threats.

Denial of Service (DoS) - це тип кібератак, до якого входять атаки Distributed Denial of Service (DDoS) як підтип. Під час DDoS-атак використовується численні підключені до Інтернету машини, що разом називаються "ботнетом", для максимального навантаження на веб-сайти зловмисним трафіком. Відмінно від інших атак, цей тип атак не спрямований на окремого користувача, а ціль є саме позбавлення користувачів можливості у доступу до ресурсів певних джерел, сайтів та подібного.

Атаки типу DDoS можуть відбуватись систематично, чи проходити в невеликих обсягах. Залежно від типу та кількості трафіку, вони можуть мати як тривалий ефект, так і одноразовий сплеск системи. Головна проблема подібного типу атак в тому, що вони можуть продовжуватись доволі значну кількість часу, що може призвести до краху всієї системи без можливості відновлення. Таким чином, DDoS-атаки можуть стати серйозною проблемою для будь-якої онлайн організації.

Усі DDoS-атаки можна поділити на 3 типи:

- атаки на основи об’єму – як правило використовують велику кількість зловмисного трафіку для того, що б перенавантажити сервер або веб-сайт. За приклад можна взяти feed flood, ICMP та UDP. Об’єм подібних атак вимірюється у бітах на секунду (BPS);
- атаки на протоколи – під час подібних атак на протоколи чи мережевий рівень відправляється велика кількість пакетів до цільової мережевої інфраструктури та інструментів управління. Прикладом подібних атак є SYN

flood та Smurf DDoS. Атаки подібного типу вимірюються в пакетах на секунду (PPS);

- атаки на рівень застосунків – атаки подібного типу передбачають собою використання програмних засобів для максимальної кількості запитів, призначених для перенавантаження серверів та застосунків. Подібні атаки вимірюються в запитах на секунду (RPS).

Кожна атака відрізняється та по своєму є небезпечною для онлайн-ресурсів. Подібні атаки мають дуже потужні наслідки для цілі, на яку вони направлені. Одні з головних наслідків DDoS-атак:

- втрата даних – здебільшого, саме подібного типу атаки призводять до втрати даних цілі, без можливості відновлення.
- повільне завантаження сторінок – здебільшого швидкість завантаження на сайті залежить від доступних серверних ресурсів, які при DDoS-атаках падають до мінімуму, або взагалі перестають бути доступними, що призводить до неможливості використовувати ресурс.
- підвищення уразливості до інших атак – в багатьох випадках подібного роду атаки використовують як прикриття для більш складніших атак, це дає змогу послабити захист та пройти складні частини захисту.
- колосальні втрати – DDoS-атаки змушують сторону захисту приймати міри розгортання більших серверів, що передбачає собою дуже великі суми. Крім того, якщо не виконувати подібних дій, можливість втрати всього ресурсу стає максимальною.

DDoS-атаки зросли за останні місяці, з якістю та частотою атак. Згідно з звітом Cloudflare [2], кількість DDoS-атак у другому кварталі 2023 року збільшилася на 15% порівняно з попереднім кварталом. Середній розмір DDoS-атак також збільшився, і найбільша атака досягла рекордних 2,3 терабайти в секунду.

Найпоширенішими цілями DDoS-атак є фінансові послуги, геймінг та технологічні галузі. Проте жодна галузь не є імунною до DDoS-атак. За останні місяці DDoS-атаки також були спрямовані проти медичних установ, урядових агентств та освітніх установ.

DDoS-атаки є серйозною загрозою для онлайн-сервісів та систем. Вони можуть викликати широкий спектр проблем, від втрати прибутку і збитків репутації до юридичних наслідків та порушень безпеки даних. Впровадження ефективних стратегій запобігання та пом'якшення DDoS-атак є важливим для захисту від цих небезпечних атак.

Список використаних джерел:

1. Takehiro K. DDOS Attack: What it is, and how to stop it.: A Cybersecurity guide for 2024 / K. Takehiro, V. Hayden., 2024. – 260 с.
2. Yoachimik O. DDoS threat report for 2023 Q3 [Електронний ресурс] / O. Yoachimik, J. Pacheco // cloudflare. – 2023. – Режим доступу до ресурсу: https://blog.cloudflare.com/ddos-threat-report-2023-q3.

УДК 004.896.2:006.3 https://doi.org/10.30837/IYF.PCEIP.2024.137

РОЗВИТОК ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРБЕЗПЕЦІ

Павлов О.А.
Науковий керівник – доц. Шаповалова А.С.
Харківський національний університет радіоелектроніки,
каф. інфокомунікаційної інженерії імені В.В. Поповського,
м. Харків, Україна
e-mail: Oleksii.pavlov2@nure.ua.

Artificial Intelligence (AI) is transforming cybersecurity, aiding in threat detection and response. This article explores AI's role in enhancing cybersecurity, utilizing machine learning to analyze vast data sets, identify patterns, and automate threat detection. While offering benefits like improved detection and real-time response, challenges include algorithm complexity and the potential misuse of AI by cybercriminals. Despite these challenges, the efficiency gains and evolving cyber threats highlight the indispensable role of AI in safeguarding digital assets.

Штучний інтелект останні роки отримав величезний розвиток в багатьох галузях, одним з основних направлень, та найважливіший є кібербезпека. В умовах постійного вдосконалення та зростання кількості та якості кібератак та загроз кібербезпеці штучний інтелект став одним з важливих інструментів для вдосконалення кібербезпеки.

Штучний інтелект у кібербезпеці передбачає саме використання алгоритмів машинного навчання та інших технологій для виявлення, реагування та запобігання кіберзагроз. Головним завданням штучного інтелекту є саме аналізування величезних обсягів даних, виявлення закономірностей та навчання на них, для того що б в подальшому виявляти потенційні загрози та аномалії. Кінцевою задачею є автоматизація процесу виявлення та реагування на загрози, що дозволяє команді кібербезпеки швидше реагувати на загрози та запобігати порушенням.

Моделі штучного інтелекту використовують методи машинного навчання як для аналізу поведінки самої мережі, так і для постійного виявлення аномалій. З часом моделі корегуються та проходять адаптацію, для того що б підвищити швидкість та точність виявлення як аномалій так і потенційних загроз безпеці. Саме здатність штучного інтелекту до самостійного корегування та адаптації забезпечує компаніям потужний та надійний захист у кібербезпеці, який здатний швидко та чітко реагувати на нові загрози.

Переваги використання штучного інтелекту для кібербезпеки:

1. Швидке та чітке виявлення загроз - традиційні та більш застарілі методи в кібербезпеці використовують підписи та конкретні правила для виявлення загроз. Одна штучний інтелект інтегрований в методи кібербезпеки

може виявляти нові та невідомі загрози, аналізувати з аномальною швидкістю великі обсяги даних і виявляти певні закономірності, які можуть ідентифікуватися як зловмисна активність.

2. Реагування в режимі реального часу на загрози - інструменти кібербезпеки на основі штучного інтелекту можуть реагувати на загрози набагато швидше, ніж традиційні методи, що дозволяє стороні безпеки вживати негайних заходів та запобігати порушенням.

3. Зменшення проценту хибних показників реагування - більш традиційні методи безпеки часто не вірно реагують на індикатори у системі, що призводить до підвищеної трати ресурсів та зниження ефективності.

4. Підвищення ефективності роботи - інструменти на основі штучного інтелекту можуть автоматизувати більшість процесів, пов’язаних з виявленням та реагуванням на загрози, дозволяючи командам зосередитись на більш важливих цілях.

Недоліки інтеграції штучного інтелекту в кібербезпеці:

1. Проблема прозорості - інструменти на основі штучного інтелекту здебільшого використовують складні алгоритми, що ускладнює розуміння та аналіз того, як саме робляться висновки. Така непрозорість у результатах ускладнює довіру до результатів, що у подальшому може призвести до хибних викликів та тривог.

2. Штучний інтелект як інструмент для злочинців - проблематика штучного інтелекту в тому, що його можуть використовувати злочинці для покращення кіберзлочинів, що призводить до більш складних та потенційно вдалих атак.

3. Конфіденційність даних - штучний інтелект для навчання потребує доступу до велики обсягів даних, які можуть містити конфіденційну інформацію компанії, тому важливо, що б інформація була надійно захищена.

Майбутнє в кібербезпеці напряму пов’язане зі штучного інтелекту, особливо з урахуванням прогресії зростання кількості та якості нових атак та потенційних загроз. Штучний інтелект може використовуватись в боротьбі з різними видами атак пов’язаних з соціальною інженерією, шкідливим програмним забезпеченням та інші.

Сила ШІ полягає в його здатності до безперервного навчання, що перевершує ручні методи виявлення, які використовуються людьми-експертами; його ефективність у запобіганні кібератакам не має собі рівних, оскільки моделі ШІ постійно адаптуються до нових загроз.

Список використаних джерел:

1. Parisi A. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies / Alessandro Parisi., 2019. – 342 с.

УДК 004.896.2:004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.139

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ЗАХИСТІ ТА ПРОТИДІЇ DDOS-АТАКАМ

Павлов О.А.
Науковий керівник – доц. Шаповалова А.С.
Харківський національний університет радіоелектроніки,
каф. інфокомунікаційної інженерії імені В.В. Поповського,
м. Харків, Україна
e-mail: Oleksii.pavlov2@nure.ua.

The article explores the evolving landscape of DDoS attacks within the realm of Artificial Intelligence (AI). Delving into the technological progress, it highlights how AI, particularly Machine Learning, is leveraged by attackers to craft sophisticated and adaptive DDoS strategies. The text emphasizes real-world instances where AI is employed in orchestrating attacks, posing challenges for traditional detection methods. While acknowledging the technical advantages, the article also underscores the challenges of integrating AI into cybersecurity, emphasizing the need for a delicate balance between accuracy and computational resources.

Тенденція розвитку сфери кіберпростору прогресивно зростає з кожним роком. Жертвами DDoS-атак стають критично важливі цілі, здебільшого це – онлайн-банкінг, платіжні шлюзи, урядові портали, оператори зв’язку. З переліченого зрозуміло, що це критично важливі інфраструктури як для звичайного користувача, так і для держави в цілому. Захист подібних цілей є найважливішим та першочерговим. У цій статті ми обговоримо як про важливість захисту від подібних атак, так і можливість інтеграції штучного інтелекту у вже існуючі методи захисту від DDoS-атак, що дасть змогу покращити їх.

Головною метою подібних атак є чітка кінцева ціль – відмова в обслуговуванні. Концепція подібних атак є дуже простою, зловмисники використовують таку кількість трафіку, що б він перевищував роздільну здатність пропускної спроможності цілі. Distributed Denial of Service attack - напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

Штучний інтелект дає можливість зловмисникам провести автоматизацію процесів створення та запуску DDoS-атак. Машинне навчання дає змогу атакам виявляти в системі жертви вразливості безпеки та швидко адаптуватись під потрібні методи. Це важливий аспект захисту, оскільки традиційні методи виявлення DDoS-атак стають не ефективними порівняно з сучасними, інтелектуальними атаками з використанням штучного інтелекту.

Вже є випадки, коли штучний інтелект використовувався для реалізації атак. Як приклад, атаки де використовувались ботнети на основі нейронної мережі для імітації поведінки реальних користувачів, вони стають все більш популярними методами атак. Для традиційних методів захисту подібні атаки стають критичними, а їх виявлення та блокування стає набагато складнішим завданням для команд кібербезпеки.

Головна проблематика інтеграції штучного інтелекту, є постійний баланс між швидкістю реагування та точністю дуже великим обсягом даних, які вони обробляють. Більшість сучасних систем штучного інтелекту мають потребу в дуже великих обчислювальних ресурсах, які забезпечити здебільшого складно.

Тенденція розвитку кіберзагроз, з використанням штучного інтелекту та машинного навчання у розробці DDoS-атак стає серйозним викликом для сучасних систем захисту. Порівнюючи технологічні переваги та проблематику інтеграції штучного інтелекту, можна зробити чіткі висновки, сторона безпеки повинна активно інтегрувати штучний інтелект у свої системи для забезпечення ефективної протидії більш новітнім та вдосконаленим атакам.

Системи безпеки, які інтегрують штучний інтелект для захисту від DDoS-атак, зменшують час виявлення атак з годин до хвилин, а іноді цей показник становить секунди.

Дивлячись на тенденції розвитку, можна спрогнозувати, що захист від DDoS-атак буде стрімко проходити інтеграцію зі штучним інтелектом. Розвиток квантових обчислень може дозволити створення нових, надзвичайно швидких алгоритмів для аналізу трафіку та ідентифікації атак, що відбуваються на ранніх етапах та під час самих атак.

Інновації в захисті від DDoS-атак, завдяки використанням штучного інтелекту, відкривають нові горизонти для захисту важливих онлайн ресурсів. Окрім цього, штучний інтелект посиле як чіткість реагування, так і швидкість, що дасть змогу в рази покращити кібербезепку. До всього, штучний інтелект постійно навчається, що в подальшому буде тільки покращувати кібербезпеку на автоматичному рівні.

Список використаних джерел:

1. Dhruba K. B. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance / K. B. Dhruba, K. K. Jugal., 2016. – 312 с. – (1st Edition).

2. Leslie F. Sikos. AI in Cybersecurity (Intelligent Systems Reference Library, 151) / Leslie F. Sikos., 2018. – 222 с. – (1st ed. 2019 Edition).

УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.141

МЕТОДИ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ КОРИСТУВАЧА В МЕРЕЖІ ІНТЕРНЕТ

Папазов К.О.
Науковий керівник – к.т.н., доц. Олешко І.В.
Харківський національний університет радіоелектроніки, каф. БІТ, м. Харків, Україна
e-mail: kyrylo.papazov@nure.ua

This paper examines the different methods of providing user anonymity in the Internet, including proxy servers, virtual private networks (VPN) and Onion routing. The paper evaluates and compares these methods according to the criteria of anonymity level, speed, cost and ease of use. The paper also discusses the advantages and disadvantages of each method, as well as the specific needs of users. The paper concludes that VPNs are the “golden mean” that offer a balance between anonymity, internet connection speed and technical complexity. However, the choice of a particular method depends on the user’s preferences and goals.

В епоху цифрової інформації, анонімність в Інтернеті стає все більш актуальною темою. Користувачі прагнуть залишатися анонімними, щоб захистити свою приватність, уникнути небажаного контенту та забезпечити свободу вираження своїх думок без страху переслідування.

Анонімність в Інтернеті – це стан, коли ідентичність користувача не відома або не може бути встановлена. Користувач, який залишається анонімним, може переглядати, завантажувати та використовувати Інтернет-ресурси, не розкриваючи свою особисту інформацію. Це може бути важливо для захисту приватності, свободи слова та уникнення цензури.

Одним з методів забезпечення анонімності є використання проксі-сервера. Проксі-сервер – проміжний сервер у комп’ютерних мережах, що виконує роль посередника між користувачем і цільовим сервером, що дозволяє клієнтам виконувати непрямі запити до інших мережних служб і отримувати відповіді. Простими словами, проксі-сервер ховає IP-адресу користувача і звертається до сайтів за допомогою іншої IP-адреси. Хоча проксі-сервери можуть забезпечити певний рівень анонімності, вони мають обмеження, наприклад, вони не шифрують трафік, що може стати проблемою, якщо користувач передає чутливу інформацію.

Віртуальна приватна мережа (VPN) – це доступне програмне забезпечення, яке забезпечує конфіденційність Інтернету. VPN створює зашифрований тунель між пристроєм користувача і всесвітньою мережею, щоб діяльність в Інтернеті була прихована від хакерів, Інтернет-провайдерів (ISP) та інших.

VPN з’єднують пристрій користувача та мережу, як правило, публічну, через зашифрований тунель. Тунель шифрує онлайн-активність користувача та

приховує його IP-адресу, замінюючи її IP-адресою приватного сервера, до якого користувач підключається. Більшість VPN використовує 256-бітне шифрування AES, яке є поточним стандартом у галузі. Щоб передати дані з пристрою на приватний сервер, мережі VPN використовують Інтернет-протоколи, які розміщують дані в пакетах і забезпечують їх надсилання в належному порядку. Якщо VPN виходить з ладу, більшість із них оснащена перемикачами, які закривають усі вікна чи програми з веб-трафіком, залишаючи користувача захищеним і конфіденційним у мережі.

Ще одним важливим та доволі потужним методом забезпечення анонімності в Інтернеті є Onion routing, який найбільш відомий завдяки мережі Tor. Tor – це мережа віртуальних тунелів, які дозволяють покращити приватність і безпеку в інтернеті. Архітектура Tor базується на принципі розподіленої мережі. Вона складається з тисяч волонтерських ретрансляторів по всьому світу, які передають трафік від одного до іншого. Кожен ретранслятор додає шар шифрування до даних, що забезпечує анонімність користувача. Коли дані досягають свого кінцевого пункту, кожен шар шифрування знімається, щоб відновити оригінальні дані. Це гарантує, що жоден окремий вузол в мережі Tor не знає і про джерело, і про призначення даних, що забезпечує високий рівень анонімності. Таким чином ті, хто зацікавлений особою користувача, бачитимуть підключення з мережі Tor замість справжньої IP-адреси, допоки користувач сам не залишить інформацію про себе в мережі.

Хоча Tor забезпечує високий рівень анонімності, він також має обмеження такі, як повільна швидкість, можливість стати ціллю для зловмисника, а також ризики, пов’язані з відвідуванням .onion сайтів.

Враховуючи те, що повна анонімність в Інтернеті є майже неможливою, в таблиці 1 наведено порівняння розглянутих методів за рівнем анонімності, впливом на швидкість інтернет з’єднання, вартістю впровадження та простотою використання. З таблиці можна зробити висновок, що кожен метод має свої сильні та слабкі сторони, які залежать від критеріїв порівняння. Проксі-сервери надають середній рівень анонімності, не впливають значно на швидкість інтернет з’єднання, але потребують впевненого вміння керувати пристроями. VPN забезпечують високий рівень анонімності, середній вплив на швидкість інтернет з’єднання, але коштують гроші. Onion routing надає максимальний рівень анонімності, але значно знижує швидкість інтернет з’єднання, а також має ризики, пов’язані з відвідуванням .onion сайтів. Вибір конкретного методу залежить від специфічних потреб користувача.

Враховуючи вищезазначене, можна зробити висновок, що анонімність в Інтернеті є важливим аспектом цифрової безпеки. Проксі-сервери, VPN та Onion routing надають різні рівні анонімності та мають свої переваги та недоліки. Віртуальні приватні мережі (VPN) вважаються “золотою серединою”, оскільки вони забезпечують баланс між анонімністю, швидкістю

інтернет-з’єднання та технічною складністю. Однак вибір конкретного методу залежить від специфічних потреб користувача. Незважаючи на те, що повна анонімність в Інтернеті є майже неможливою, використання цих методів поодинці або в поєднанні може значно підвищити приватність користувача в мережі.

Таблиця 1 – Порівняння методів забезпечення анонімності в мережі інтернет

Критерії порівняння	Проксі-сервери	VPN	Onion routing
Рівень анонімності	Середній	Високий	Максимальний
Вплив на швидкість інтернет з’єднання	Не значний, в залежності від навантаження серверів та відстані до них	Середній вплив, в залежності від навантаження серверів та відстані до них	Значний
Вартість	Від 0.80$ в місяць; є безкоштовні, але зі значними обмеженнями	Надійні сервіси від 5$ в місяць; є безкоштовні, але зі значними обмеженнями	Безкоштовно
Простота використання	Потребує впевненого вміння керувати пристроями	Потребує вміння встановлювати додатки на пристрої	Потребує вміння встановлювати додатки на пристрої

Список використаних джерел

1. A 2024 Guide to VPNs : вебсайт. URL: https://www.security.org/vpn/ (дата звернення 04.03.2024).

2. How can we help? | Tor Project | Support : вебсайт. URL: https://support.torproject.org/ (дата звернення 04.03.2024).

3. Proxy server : вебсайт. URL: https://en.wikipedia.org/wiki/Proxy_server (дата звернення 04.03.2024).

4. Сердюков Д. В., Сєвєрінов О. В., Сидоренко З. М. Безпечне підключення мобільних пристроїв до корпоративної мережі з використанням тунелю VPN. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. 2023. Т. 1, С. 70.

УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.144

ВРАЗЛИВОСТІ МЕСЕНДЖЕРІВ «TELEGRAM», «WHATSAP», «VIBER»

Пашнєва О.Р.
Науковий керівник – Євгеньєв А.М.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: olha.pashnieva@gmail.com

The proliferation of messaging applications such as Telegram, WhatsApp, and Viber has revolutionized communication, but it has also introduced a myriad of security concerns. This paper provides a analysis of the vulnerabilities present in the messengers Telegram, WhatsApp and Viber, with a particular focus on the threat of phishing attacks. As these platforms handle sensitive personal and professional information, they are increasingly becoming prime targets for attackers who seek to exploit unsuspecting users through deceptive tactics. The relevance of this research is due to the increasing use of these messengers for communication in various domains, including business, personal, and government.

У червні 2016-го року «International Journal of Electrical and Computer Engineering» було опубліковано роботу, що дослідила вже популярні на той час «Telegram», «Whatsap» та «Viber» за багатьма критеріями, щоб обрати серед них найбільш зручний і захищений [1]. Висновком стало: «Viber є найбільш функціональним месенджером, але якщо основною проблемою є безпека спілкування, то розумніше обрати Telegram. Telegram пропонує можливість синхронізації, надшвидкий сервіс, надійне резервне копіювання та кращі функції безпеки.» З плином часу й розвитком систем безпеки, нині всі найвідоміші месенджери використовуюсь двофакторну аутентифікацію та наскрізне шифрування. Це передбачає, що ключі дешифрування до чатів та дзвінків зберігаються лише на пристроях користувачів: повідомлення неможливо перехопити й прочитати, а розшифровуються вони тільки на пристроях співрозмовників. Будь-які інші особи, навіть співробітники месенджеру, не мають доступу до цих ключів, тому дзвінки та повідомлення можуть бути прочитані, чи прослухані лише учасниками діалогу.

Коли розшифрування перехопленого повідомлення стало невигідним, популярність отримали інші види атак [2]. Кіберзлочинці можуть маскуватися. Вони можуть зв'язатися із законним користувачем, видаючи себе за іншу фізичну або юридичну особу, щоб отримати конфіденційні дані (особисті дані, паролі, номери кредитних карток) або розгорнути шкідливе ПЗ (шкідливе програмне забезпечення, що отримує несанкціонований доступ до будь-якої системи). Атаки такого типу називають фішингом. За даними компанії Vesta,

що є платформою наскрізної гарантії транзакцій для онлайн-покупок, 2021 року фішингові схеми стали другою найімовірнішою причиною витоку даних і коштували підприємствам у середньому 4,65 мільйона доларів. Того самого року група аналізу загроз Google повідомила про блокування близько 800 мільйонів фішингових листів, пов'язаних із COVID-19, на день.

Соціальні мережі дали можливість кіберзлочинцям не тільки автоматизувати процес, використовуючи ботів для розсилки, але й для реклами різних послуг – від продажу наборів для фішингу до допомоги в налаштуванні користувацьких фішингових кампаній – усім, хто готовий платити. Крім того, не потрібно застосовувати великих зусиль, щоб знайти безкоштовний контент, або посібники, які шахраї так охоче поширюють серед своєї аудиторії Telegram. Це слугує своєрідною приманкою для менш досвідчених фішерів. Новачки дізнаються, на що здатні фішингові інструменти, здійснять свою першу аферу і бажають більшого, і саме тоді їм буде запропоновано платний контент. Інша причина розміщення подібних матеріалів – набір неоплачуваної робочої сили. Щоб залучити ширшу аудиторію, шахраї рекламують свої послуги, обіцяючи навчити інших фішингу за серйозні гроші. Таким чином основною небезпекою є навіть не самі атаки, а розповсюдження вказівок і ресурсів, завдяки яким кількість злочинців тільки зростає.

Враховуючі, що більшість кіберзлочинців не є професіоналами, їх методи можна назвати лінійними й обійти небезпеку стає простою задачею, коли знаєш на що звертати увагу. Одна з найпоширеніших хитрощів, які використовують шахраї під час фішингових атак – створення фейкової офіційної сторінки відомого бренду. Зловмисники схильні копіювати елементи дизайну з реального сайту, тому користувачам складно відрізнити підроблені сторінки від офіційних. Навіть доменне ім'я фішингової сторінки часто може виглядати як реальна веб-адреса певного бренду, оскільки кіберзлочинці додають до URL-адреси назву компанії або послуги, під якою вони видають себе. Цей трюк відомий як комбосквотинг. Злочинці, як правило, використовують зламані офіційні веб-сайти для розміщення сторінок, створених за допомогою фішингових наборів, або покладаються на компанії, що пропонують безкоштовний веб-хостинг. Останні постійно працюють над боротьбою з фішингом і блокують фейкові сторінки, хоча фішингові сайти часто за короткий період своєї діяльності встигають виконати поставлене завдання – зібрати та надіслати злочинцям персональні дані жертв. Посилання на таку сторінку звичайний користувач може отримати через розсилку бота, або групи. Як приклад, боти «Telegram» використовують обробку природної мови і штучний інтелект для ведення реалістичної розмови, що ускладнює визначення того, що вас обманюють. В одній із нещодавніх версій шахрайства хакери використовували бота, відомого як «SMSRanger», видаючи себе за

представників банків і компаній, таких як «PayPal», «Apple Pay», «Google Pay» і широко використовуваних операторів мобільного зв'язку. Щойно хакери вводять номер телефону користувача Telegram, бот дзвонить і переконує користувача надати особисту інформацію, логіни банківських рахунків, паролі і навіть коди двофакторної аутентифікації. Небезпека такого роду демонструє типові попереджувальні ознаки фішингового шахрайства, зокрема можна виділити наступні сім:

Використовує владу для завоювання довіри. Інтернет-шахраї використовують організації та імена, яким ви довіряєте, щоб послабити вашу пильність. Остерігайтеся тих, хто несподівано пише вам і стверджує, що він з IRS, уряду або відомої компанії.

Створює відчуття терміновості. Кіберзлочинцям потрібно, щоб ви діяли швидко, перш ніж ви зрозумієте, що вони задумали. Вони часто винаходять відчуття терміновості, щоб завадити вам спочатку перевірити їхні твердження.

Зв'язується з вами несподівано. Один із найпростіших способів виявити шахрая – це якщо він першим зв'яжеться з вами. Якщо ви отримали будь-яке повідомлення, телефонний дзвінок або електронний лист від когось, кого ви не знаєте, переконайтеся, що він той, за кого говорить, безпосередньо зв'язавшись з його агентством або компанією.

Запитує конфіденційну інформацію. Шахраї видають себе за ваш банк і запитують ваш PIN-код або онлайн-паролі, щоб «захистити» обліковий запис. Але законні фінансові установи ніколи не зроблять цього [3].

Надмірні обіцянки щодо того, що вони можуть виконати. Якщо щось або хтось здається «занадто хорошим, щоб бути правдою», велика ймовірність, що вас намагаються обдурити.

Намагається бути представницьким. Кіберзлочинці прикидаються другом або членом сім'ї, щоб швидко завоювати вашу довіру. Але це не так. Не довіряйте повідомленню тільки тому, що воно прийшло від знайомого вам облікового запису.

Змушує використовувати незвичайні способи оплати. Більшість варіантів онлайн-платежів захищають від шахраїв. Якщо хтось змушує вас заплатити йому невідстежуваним або незворотнім способом, це може бути шахрайством. Сюди входять банківські перекази, подарункові картки та криптовалюта.

Список використаних джерел

1. «WhatsApp, Viber and Telegram which is Best for Instant Messaging?», International Journal of Electrical and Computer Engineering (IJECE), June 2016.

2. Сєвєрінов, О.В., Шевцов В.О., Сокол-Кутиловська А.С. Аналіз сучасних методів атак на електронні ресурси органів управління // Системи озброєння і військова техніка, 2017. – С. 65-68.

3. Арчакова А.І., Сєвєрінов О.В. Аналіз забезпечення конфіденційності інформації в сучасних мессенджерах. Комп’ютерні та інформаційні системи і технології (2019).

УДК 004.056 https://doi.org/10.30837/IYF.PCEIP.2024.147

ТАКТИЧНА РОЗВІДКА ЗАГРОЗ В УМОВАХ КІБЕР ВІЙНИ

Пічієнко М. Г.
Науковий керівник – проф. Радівілова Т.А.
Харківський національний університет радіоелектроніки, Харків, Україна
e-mail: mariia.pichiienko@nure.ua, +380961690863

The thesis discusses the effective protection of organisations against digital threats, in particular in the context of cyber warfare and cyber threats affecting Ukrainian companies. The document emphasises the importance of tac-tical threat intelligence and a system of general threat intelligence to prevent and mitigate cyber attacks. The document also discusses the low level of threat intelligence use in Ukrainian organisations due to low awareness, lack of maturity, lack of a comprehensive approach and insufficient community interaction.

Ефективний захист активів організації від цифрових загроз складається з низки задач, серед яких є як аналіз внутрішньої інфраструктури з метою виявлення можливих точок вразливості, так і розуміння потенційних загроз. У останньому випадку команді інформаційної безпеки необхідно мати більш глибоке уявлення, ніж просто поверхнева ідентифікація. Для передбачення та послаблення наслідків від кібератак вони потребують тактичної розвідки загроз — конкретної інформації про тактику, яку цифрові супротивники можуть використовувати для проникнення в систему захисту. [1]

Особливої актуальності розвідка загроз набуває для українських організацій, які є постійними цілями з боку російських APT в умовах російсько-української кібервійни. З 2014 року Україна стала полігоном для випробування кіберпотужностей росії, надаючи можливість іншим спостерігати і дізнаватися про їхню тактику і методи. Російські групи спрямовують свої атаки з метою викрадення інформації, припинення нормального функціонування ресурсів, а також завдання репутаційної шкоди. [2] На даному етапі можна стверджувати, що кібервійна не має кордонів, адже від неї значною мірою потерпають і країни Європи. [3]

Поняття тактичної розвідки загроз вписується в ширшу систему розвідки загроз, в якій різні види інформації про цифрові ризики збираються, аналізуються і передаються зацікавленим сторонам. Ця система включає чотири види розвідки загроз - стратегічну, тактичну, оперативну і технічну - з чіткими відмінностями між ними.

1. Стратегічна розвідка загроз має справу з інформацією високого рівня про мінливий ландшафт цифрових ризиків і про те, як ці зміни можуть вплинути на стан кібербезпеки організації та її готовність до них. Стратегічна розвідка зосереджується на новітніх типах загроз і супротивників, які можуть

становити ризик для організації. Вона найчастіше надається керівництву з метою прийняття стратегічних рішень.

2. Тактична розвідка загроз обробляє конкретну інформацію про новітні тактики, техніки, методи і процедури, які використовують цифрові супротивники для досягнення своїх цілей. Тактична розвідка загроз найчастіше надається керівникам SOC, оскільки вона дозволяє їм впроваджувати відповідні заходи протидії новим моделям атак.

3. Оперативна розвідка загроз є ще більш специфічною, ніж тактична, оскільки вона зосереджена на наданні практичної інформації про ідентифіковану атаку на організацію. Оперативна розвідка найчастіше надається керівникам з мережевої безпеки та їхнім командам, які можуть негайно використовувати цю інформацію в процесі реагування на інциденти.

4. Технічна розвідка загроз фокусується на конкретних індикаторах загроз або індикаторах компрометації (IoC), які сигналізують про зловмисну активність в мережі або системі. Дані про технічні загрози зазвичай передаються групам безпеки, які можуть розпочати розслідування, щоб визначити, чи відбулася атака.

Зазвичай джерелами даних тактичної розвідки загроз виступають:

- обмін інформацією про інформаційну безпеку серед спільноти;
- бази даних про загрози і відкриті джерела (MITRE ATT&CK, публічні threat intelligence feeds, оголошення та попередження про загрози від урядових організацій, таких як CERT-UA в Україні і CISA у США);
- розвідка у DarkNet (аналіз як і скомпроментованих даних організації, так і можливе отримання інформації про майбутні кібератаки у специфічних форумах, каналах, чатах);
- моніторинг публічної площини атак за допомогою спеціалізованих рішень з threat intelligence. [1]

Для українських організацій напрямок розвідки загроз не є широко розвинутим, хоча його актуальність є беззаперечною. Відповідальним за роботу в цьому напрямку на державному рівні є CERT-UA при Державній службі спеціального зв’язку і захистом інформації, в основні задачі якого входить реагування на кіберінциденти, накопичення та проведення аналізу даних про кіберзагрози, а також міжнародна співпраця за наведеними напрямками. CERT-UA регулярно публікує дані про відомі їм атаки разом з IoC і випускає аналітичні звіти з дослідження російсько-української кібервійни.

Однак проведена робота не може бути ефективною без правильної обробки отриманої інформації всередині самих організацій. Наразі загальний рівень threat intelligence в українських організаціях залишається незадовільним через низку чинників.

1. Низький рівень обізнаності. Для багатьох представників організацій threat intelligence обмежується збиранням threat intelligence feeds без їх

подальшої обробки. Розвідка загроз завершується підписанням на розсилки від CERT-UA і переглядом тематичних груп у Telegram у вільний час. Немає уявлення щодо можливості використання даних про загрози у планах стратегічного розвитку і їх інтеграції в системи захисту.

2. Низький рівень зрілості. Використання threat intelligence – це метод проактивного захисту, на той час як більшість українських організацій використовують скоріш реактивний підхід, тобто займаються усунення недоліків інформаційної безпеки вже після того, як відбувся інцидент.

3. Відсутність комплексного підходу. Використання тактичної розвідки про загрози вимагає побудованих процесів у напрямках моніторингу і реагування на інциденти. У найкращому варіанті це має бути повноцінний SOC, який наразі є у великих комерційних компаніях. Йдуть процеси щодо створення окремих галузевих SOCів для низки організацій критичної інфраструктури, але ситуація для державного сектору залишається незадовільною.

4. Низький рівень спілкування. В Україні все ще відбувається процес налагодження культури обміну інформації у сфері кібербезпеки. На жаль, багато організацій продовжують замовчування інцидентів безпеки через боязнь подальших ускладнень, можливих збільшень перевірок з боку регулятора, тощо. Через це багато даних про атаки залишаються невідомими для спільноти.

Отже, ефективний захист активів організації від цифрових загроз є комплексною задачею, в яку повинно входити використання даних про кіберзагрози. В умовах кібервійни це стає все більш актуальним не лише для України, але й країн-партнерів. Побудова налагоджених процесів з обміну даних і проактивний підхід до кіберзагроз є критичним у протистоянні агресії. Українським організаціям необхідно буде підвищувати рівень обізнаності, розвивати використання threat intelligence, впроваджувати комплексний підхід до захисту, а також сприяти обміну інформацією в галузі кібербезпеки. Тільки таким чином можна ефективно стояти на захисті в умовах постійно зростаючого ризику цифрових загроз.

Список використаних джерел

1. What is Tactical Threat Intelligence / Zerofox, 2022. URL: https://www.zerofox.com/blog/what-is-tactical-threat-intelligence/(дата звернення: 24.02.2022)

2. Russia’s Cyber Tactics: Lessons Learned in 2022 / State Service of Special Communication and Information Protection of Ukraine, 2022. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53466 (дата звернення: 24.02.2022)

3. 2022-2023: A year of Cyber Conflict in Ukraine / Thales, 2023. URL: https://bo-cyberthreat.thalesgroup.com/sites/default/files/2023-03/A%20year%20of%20Cyber%20Conflit%20in%20Ukraine_CTI-2023.pdf (дата звернення: 24.02.2022)

УДК 004.056 https://doi.org/10.30837/IYF.PCEIP.2024.150

АНАЛІЗ МОДЕРНІЗАЦІЇ ОСНОВНИХ ЗАГРОЗ В УМОВАХ КІБЕРВІЙНИ

Пічієнко М. Г.
Науковий керівник – проф. Радівілова Т.А.
Харківський національний університет радіоелектроніки, Харків, Україна
e-mail: mariia.pichiienko@nure.ua, +380961690863

The issue of destructive and devastating cyber-attacks by Russia before the invasion of our country demonstrates that cyber-attacks play an important and strategic role in the modern world and warfare, regardless of public awareness. This threat to us is constant and evolving. Cyber-attacks pose significant challenges to our system and infrastructure with paradoxical consequences. Ukraine's security significantly depends on ensuring cyber security. It is not only worth emphasizing attention to this, but also putting in maximum effort. The thesis provides a brief overview of cyber warfare from its beginning to the present, identifies the main current threats and highlights the trends in cyber threats that are relevant to Ukrainian organisations today.

Поняття російсько-українська кібервійни з’явилося значно раніше початку повномасштабного вторгнення Російської Федерації 24 лютого 2022 року. Вважається, що кібервійна відбувається на фоні військового конфлікту між Україною та Російською Федерацією з 2014 року. Цей конфлікт спричинив значну активізацію кібератак і кібероперацій з обох сторін. Російські хакерські групи, а також групи, які зв'язують з російськими інтересами, були звинувачені у проведенні кібератак на українські урядові, військові та критичні інфраструктурні системи. Серед них ураження вірусом BlackEnergy української електроенергетичної системи у 2015 році і поширення вірусу NotPetya у 2017.

Ще до початку військових дій, росіяни почали синхронізувати атаки в кіберпросторі з інформаційними вкиданнями, фейковими новинами та іншими операціями впливу. Наприклад, масова успішна кібератака на більше 70 веб-ресурсів державних органів влади, що відбулася в січні 2022 року, є лише однією з численних інцидентів, які передували повномасштабному вторгненню. [1]

Інформаційні операції та кібератаки в перші дні вторгнення мали на меті локалізувати та паралізувати опір українців. У першу чергу росіяни націлилися

на системи зв’язку, проте більшість атак були відбиті. Суттєвою втратою став злам супутника компанії Viasat, який надавав українцям швидкісний інтернет.

Основні категорії атак під час гібридної війни можна визначити наступним чином:

1. Кібератаки, направлені на порушення доступності сервісів:
- масове ураження державних та комерційних сайтів;
- шкідливе програмне забезпечення Wiper;
- DDoS-атаки;
- атаки на об'єкти критичної інфраструктури та військову інфраструктуру;
2. Кібершпигунство:
- хакерські атаки з метою викрадення конфіденційних даних;
- шкідливе програмне забезпечення для викрадення інформації;
- захоплення облікових записів;
3. Інформаційна війна:
- ферми ботів, що поширюють фейкові новини та пропаганду;
- фейкові акаунти, що видають себе за публічних осіб чи посадовців;
4. Кіберзлочинність з корисливих мотивів:
- шахрайство на військовій тематиці.

З початку повномасштабного вторгнення залежно від виду атаки, їх кількість збільшилася від 3 до 10-12 разів. Експерти стикнулися з чотирма основними видами подій під час кібервійни порівняно з мирним періодом: кібершпигунство, руйнівні атаки на системи критичної інфраструктури, які часто відбувалися разом з військовими операціями, інформаційна війна – розповсюдження фейків, пропаганда, психологічний тиск, та напади кіберзлочинців як зі сторони міжнародних кримінальних угруповань, так і з боку початківців-хакерів. Більшість фізичних атак на цивільну інфраструктуру супроводжувалася атакою у кіберпросторі. [2]

Наразі вже можна спостерігати зміни в кіберпросторі порівняно з початком війни, коли більшість кібератак спланована російською федерацією і мала чітку мету. З третього кварталу 2022 року кіберконфлікт значною мірою пов'язаний з операціями з боку хактивістів, які пов'язані між собою, хоча й не обов'язково спонсоруються. На ці операції припадає 75% інцидентів, зафіксованих з початку конфлікту, і вони включають хвилі DDoS-атак, здійснених групами, які здебільшого були сформовані після початку конфлікту. Деструктивні кібервійськові операції становлять лише 2% від загальної кількості інцидентів і переважно спрямовані проти українських організацій державного сектору.

Серед поточних трендів кіберзагроз можна виділити наступні.

1. Кількість кіберінцидентів продовжує збільшуватись.
2. Цивільний і правоохоронний сектори, Сили безпеки і оборони України залишаються основними цілями атаки з метою викрадення конфіденційних даних.
3. При виявленні більшості атак з'ясовується, що первинний доступ до систем був отриманний зловмисниками заздалегідь (рік та більше).
4. Тенденція до повторних атак тих об’єктів, що вже були уражені.
5. Атаки через ланцюжок постачання і застосування легітимного ПЗ для зловмисних дій у хакнутій системі.

Російсько-українська кібервійна відображає загальний тренд в сучасних конфліктах, де кіберпростір стає важливим полем боротьби між державами та некерованими суб'єктами. Кібератаки можуть мати серйозні наслідки для економіки, інфраструктури та безпеки країн, тому відповідна кібербезпека стає важливим елементом національної безпеки кожної країни

Список використаних джерел

1. Lessons from Russia’s cyber-war in Ukraine / The Economist, 2022. URL: https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine (дата звернення: 24.02.2022).
2. Про кібербезпеку в Україні. Як бізнес зараз вирішує питання кіберзахисту? // KPMG в Україні. URL: https://kpmg.com/ua/uk/home/media/press-releases/2023/08/pro-kiberbezpeku-v-ukrayini.html (дата звернення: 24.02.2022).
3. Російські кібероперації. Аналітика за перше півріччя 2023 року: звіт Державної служби спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=60201 (дата звернення: 24.02.2022).
4. 2022-2023 : A year of Cyber Conflict in Ukraine: Summary of extensive analysis from the Thales Cyber Threat Intelligence Team. URL: https://bo-cyberthreat.thalesgroup.com/sites/default/files/2023-03/A%20year%20of%20Cyber%20Conflit%20in%20Ukraine_CTI-2023.pdf (дата звернення: 24.02.2022).

004.056.5:004.722 https://doi.org/10.30837/IYF.PCEIP.2024.153

ЗАХИСТ ДАНИХ ЗА ДОПОМОГОЮ БЛОКЧЕЙНУ ТА ШТУЧНОГО ІНТЕЛЕКТУ

Просолов В.В.
д.т.н. проф. Халімов Г.З.
Харківський національний університет радіоелектроніки, Харків, Україна
e-mail: vladyslav.prosolov@nure.ua

In this article, we will analyze SecNet, an architecture that can provide secure data storage, computation, and sharing in a large-scale Internet environment, aiming for a more secure cyberspace with true big data and thus advanced AI with a large number of data sources, through the integration of three key components: blockchain-based data sharing with a guarantee of ownership; a secure computing platform based on artificial intelligence; a trusted value exchange mechanism for purchasing a security service.

У доповіді розглядається можливість захистити дані шляхом поєднання блокчейну та штучного інтелекту, а також дослідити архітектуру захищеної мережі, щоб значно підвищити безпеку обміну даними та всієї мережі [1].

Щоб використовувати штучний інтелект (ШІ) і блокчейн для вирішення проблеми зловживання даними, а також розширити можливості штучного інтелекту за допомогою блокчейну для довіреного керування даними в недовіреному середовищі, пропонуємо SecNet, яка є новою мережевою парадигмою, зосередженою на безпечному зберіганню даних, обмін та обчислення замість спілкування.

SecNet гарантує право власності на дані за допомогою технологій блокчейну та безпечної обчислювальної платформи на основі ШІ, а також механізму стимулювання на основі блокчейну, пропонуючи парадигму та стимули для об’єднання даних і більш потужний ШІ для досягнення кращої безпеки мережі. Крім того, ми обговорюємо типовий сценарій використання SecNet у системі медичного обслуговування та надаємо альтернативні способи використання функції зберігання SecNet. Також, ми оцінюємо його покращення щодо вразливості мережі під час протидії DDoS-атакам і аналізуємо винахідницький аспект щодо заохочення користувачів до спільного використання правил безпеки для більш безпечної мережі.

Дані дуже важливі для їх власника, і різні типи даних можна створювати, змінюючи необроблені дані відповідно до різних вимог і сценаріїв. Наприклад, інформацію про здоров’я користувача, яка зберігається в PDC, можна витягти та реорганізувати, щоб стати структурованими медичними даними, що дуже зручно для покупців із лікарень, науково-дослідних інститутів і розробників програм [2].

Усі дані об’єкта в кіберпросторі зберігаються в PDC, тому їх безпека має велике значення для власника, оскільки дані фактично є цифровим клоном

об’єкта в реальному світі. Для захисту даних SecNet впроваджує компонент ASC в OSS у кожному PDC.

AI є однією з основних можливостей, інтегрованих у PDC. Для різних штучних інтелектів було винайдено різні методи машинного навчання, наприклад, зіставлення шаблонів, комп’ютерний зір і самостійне керування. Наразі досліджуються різні методи ШІ для обробки різних типів даних. Ці специфічні для даних функції штучного інтелекту можна розглядати як великий набір «острівців рішень»: наукові кола та індустрія створили численні ізольовані програмні компоненти та механізми, які мають справу з різними частинами інтелекту окремо. PDC працює як операційна платформа штучного інтелекту, об’єднуючи окремі компоненти штучного інтелекту в узгоджену інтелектуальну систему ширшого характеру. Різні функції штучного інтелекту взаємодіють одна з одною в PDC і діють як інтелектуальна система.

Для захищених обчислень на самому початковому етапі ASC може інтегрувати модуль Generative Adversarial Network (GAN) для генерації більш потужних правил безпеки, що розвиваються, і ввімкнення безпечного та інтелектуального OSS для PDC.

Модуль GAN ASC може вивчати поточні правила безпеки PDC, а потім генерувати зловмисні, але «схожі на законні» запити на доступ до деяких особистих даних, щоб заплутати OSS PDC, щоб змусити OSS втратити здатність класифікувати запит на доступ є незаконним чи ні. Після тривалого раунду генерації та класифікації за допомогою модуля GAN OSS PDC стане набагато розумнішим і потужнішим, а фальшиві запити доступу до даних матимуть мало шансів конкурувати з таким безпечним і інтелектуальним OSS цього PDC.

SecNet забезпечить величезну кількість додатків завдяки вбудованому штучному інтелекту та блокчейну. Одним із типових випадків розгортання та застосування SecNet є довірчий обмін медичними даними між недовіреними різними сторонами для підтримки інтелектуальної та безпечної екосистеми керування медичними даними, яка є ключем до глобальної системи охорони здоров’я.

У майбутній роботі ми дослідимо, як використовувати блокчейн для авторизації доступу до запитів на дані, а також розробимо безпечні та детальні смарт-контракти для обміну даними та обчислювальної служби на основі ШІ в SecNet. Крім того, ми змоделюємо SecNet і проаналізуємо його продуктивність за допомогою масштабних експериментів на основі передових платформ.

Список використаних джерел

1. H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu and J. Xing, "Hyperconnected network: A decentralized trusted computing and networking paradigm", IEEE Netw., vol. 32, pp. 112-117, Jan./Feb. 2018.

2. Y.-A. de Montjoye, E. Shmueli, S. S. Wang and A. S. Pentland, "openPDS: Protecting the privacy of metadata through SafeAnswers", PLoS ONE, vol. 9, no. 7, 2014.

УДК 004.056.53:355.451]:004.7 https://doi.org/10.30837/IYF.PCEIP.2024.155

ДОСЛІДЖЕННЯ ТА АНАЛІЗ МЕХАНІЗМІВ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АТАКАМ ТИПУ DDOS НА СЕРВЕРИ

Топіха Т.Б.
Науковий керівник – ст. викладач В'юхін Д.О.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: tymofii.topikha@nure.ua

The first DDoS attacks appeared in 1996. However, this phenomenon attracted special attention in 1999, when the world's giants - Amazon, Yahoo, CNN, eBay, and E-Trade - were put out of working condition. And to take urgent measures to solve the problem began only in 2000, when again were committed impact on the servers of important companies. Also at this moment russia is using DDoS attacks to undermine the performance of important structures in Ukraine. And even though the attack has existed for more than 20 years, due to the modernization of the attack algorithm it is possible to inflict quite severe damage to the target of the attack

Атака DoS (відмова в обслуговуванні) є методом, в якому атакуючий намагається перешкодити нормальному функціонуванню системи чи сервісу, завантажуючи його надмірною кількістю запитів або шкідливими діями. DDoS (розподілена атака з відмовою в обслуговуванні) використовує багато атакуючих пристроїв для збільшення навантаження на цільовий сервер, збільшуючи ймовірність його відмови в обслуговуванні.

Призначеним для атаки можуть бути будь-які пристрої, які мають доступ до мережі Інтернет, і можуть надсилати запити, такі як комп'ютери, смартфони або побутова техніка. Проте організувати атаку з використанням великої кількості пристроїв може бути складно, тому зазвичай атакуючий використовує комп'ютери, що підкорені вірусами або іншим шкідливим програмним забезпеченням, без відома їх власників [1].

Простий трафік - це HTTP-запити. Основа запиту - HTTP-заголовок. Запитуюча сторона може використовувати стільки заголовків, скільки потрібно, надаючи їм необхідні властивості. Зловмисники, які здійснюють DDoS, можуть змінювати ці заголовки, тому їх важко розпізнати як атаку [2, 3].

HTTP(S) GET-запит - спосіб, яким дані запитуються на сервері. Цей запит може "попросити" сервер передати який-небудь файл, зображення, сторінку або скрипт для відображення у веб-браузері.

HTTP(S) GET-флуд - DDoS атака прикладного рівня (7) моделі OSI. Зловмисник відправляє потужний потік запитів на сервер для переповнення його ресурсів. У цьому випадку сервер перестає відповідати на запити реальних відвідувачів.

HTTP(S) POST-запит - метод, суть якого полягає в тому, що дані поміщаються у тіло запиту для подальшої обробки на сервері. HTTP POST-запит кодує передавану інформацію і поміщає на форму, а потім відправляє

цей вміст на сервер. Цей метод використовується, коли потрібно передавати великі обсяги даних.

HTTP(S) POST-флуд - тип DDoS-атаки, при якому кількість POST-запитів переповнюють сервер, в результаті чого він не може відповісти на них. Це призводить до аварійного зупинення сервера з наступними наслідками.

Всі перераховані запити також передаються по HTTPS, передавані дані в такому випадку шифруються. І подібний захист грає на користь хакерам. Адже, щоб виявити такий запит, сервер повинен спочатку розшифрувати його. А розшифрувати потік запитів під час такої атаки дуже складно і це створює додаткове навантаження на сервер.

ICMP-флуд (або атака Smurf). Досить небезпечний тип атаки. Хакер відправляє підроблений ICMP-пакет, в якому адреса атакуючого змінюється на адресу жертви. Усі вузли надсилають відповідь на цей пінг-запит. Для цього у більшості випадків використовують велику мережу, щоб у комп'ютера-жертви не було жодних шансів.

UDP флуд (або атака Fraggle): Цей тип атаки аналогічний ICMP флуду, проте використовуються UDP пакети. Через перевантаження пропускної здатності сервера жертви відбувається відмова в обслуговуванні.

SYN-флуд: Основою цієї атаки є запуск великої кількості одночасних TCP-з'єднань за допомогою відправлення SYN-пакета з неправильною зворотною адресою.

Відправка "важких пакетів": У цьому типі атаки зловмисник відправляє серверу пакети, які не перевантажують пропускну здатність, але витрачають його процесорний час. Це призводить до збою в системі, і користувачі не можуть отримати свої ресурси.

Для ефективного протидії атакам DDoS важливо вжити комплекс заходів. По-перше, використання захисних пристроїв і програмного забезпечення, таких як файрволи та системи виявлення вторгнень, дозволяє виявляти та блокувати шкідливий трафік. Другим важливим кроком є постійний моніторинг трафіку, щоб вчасно виявляти аномальну активність, яка може свідчити про атаку. Фільтрація трафіку на рівні мережевих пристроїв дозволяє блокувати шкідливі запити перед тим, як вони досягнуть цільового сервера.

Додатково, використання спеціалізованих служб DDoS-захисту може надати ще один рівень захисту, фільтруючи трафік на віддалених вузлах мережі. Резервні мережні канали можуть допомогти розподілити трафік у випадку атаки, що зберігає доступність сервісів. Нарешті, оптимізація програмного забезпечення та конфігурація серверів можуть зменшити вразливість до DDoS-атак шляхом оптимізації ресурсів та обмеження навантаження на сервери.

Список використаних джерел

1. Сєвєрінов О.В., Шевцов В.О., Сокол-Кутиловська А.С. Аналіз сучасних методів атак на електронні ресурси органів управління // Системи озброєння і військова техніка 1 (2017): 65-68.

2. Shin D. How to defend against amplified reflection ddos attacks. URL: https://www.a10networks.com/resources/articles/how-defend-against-amplifiedreflection-ddos-attacks.

3. Виявлення DDoS атак статистичними методами / Т. А. Радівілова та ін. COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES. 2019. URL: https://openarchive.nure.ua/server/api/core/bitstreams/7b8e7f34-ca47-4632-80a2-e527f27e81c1/content.

УДК 004.056:355.451

СТВОРЕННЯ БЕЗПЕЧНИХ ЛОКАЛЬНИХ МЕРЕЖА З ВИКОРИСТАННЯМ ЕЛЕМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ

Тяптя А.В.
Науковий керівник – ст. викл. В'юхін Д.О.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: anastasiia.tiaptia@nure.ua

An analysis of the principles of creating secure local networks using advanced information security technologies was carried out. The key directions in the field of security technologies of local networks are considered. Correct use of encryption technologies, network firewalls, identification and authentication systems, but care must be taken to ensure that the cost of security does not exceed reasonable limits.

У сучасному цифровому світі, де відбувається постійний розвиток технологій, безпека локальних мереж є надзвичайно актуальною проблемою. Зростаюча кількість кіберзагроз та інцидентів з порушенням безпеки мереж підкреслює необхідність удосконалення методів захисту [1].

Мета роботи - дослідження та аналіз принципів створення безпечних локальних мереж з використанням передових технологій інформаційної безпеки.

Зважаючи на швидкі та постійні зміни в кіберзагрозах, розвиток технологій інформаційної безпеки також є невпинним. Ключові напрямки у сфері технологій безпеки локальних мереж:

1. Розширене шифрування даних. Шифрування даних є однією з найважливіших технологій для захисту конфіденційності. Розширені методи шифрування, такі як AES-256, дозволяють забезпечити високий рівень безпеки для пересилання даних через мережу, а також для зберігання інформації на пристроях та серверах [2].

2. Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS). Ці системи виявляють та блокують незвичайну або підозрілу активність у мережі. Вони дозволяють вчасно реагувати на потенційні загрози та вторгнення, запобігаючи їхньому успішному завершенню [3].

3. Методи автентифікації користувачів [4]. Для забезпечення безпеки мережі важливо правильно ідентифікувати та автентифікувати користувачів. Парольні системи, біометричні технології (відбитки пальців, розпізнавання обличчя), а також механізми двофакторної автентифікації надають додатковий рівень безпеки.

4. Інтеграція штучного інтелекту (AI) та машинного навчання (ML). Технології штучного інтелекту та машинного навчання стають все більш важливими в сфері кібербезпеки. Вони дозволяють автоматизувати процес виявлення та аналізу загроз у реальному часі, а також вдосконалювати системи захисту за допомогою аналізу великих обсягів даних.

5. Blockchain технології для захисту даних. Blockchain технології дозволяють створювати розподілені та незмінні записи даних, що робить їх вкрай важливими для забезпечення цілісності та захисту даних у локальних мережах.

Для вирішення вищеназваних проблем існує багато різних способів їх вирішення: використовувати технології AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), SHA (Secure Hash Algorithm), IPsec (Internet Protocol Security).

За допомогою суміщення технологій IDS, IPS та AI можна зробити паралельне машинне навчання та первинну безпеку від вторгнень. Для навчання AI потрібно буде використати достатньо немало коштів, але з часом , для використання його в довгострокову перспективу, кіберзахист буде виконуватись автоматично та реакція між дією та реакцією буде мінімальною. Залишається тільки додати журнал користувачів і щоб AI запам'ятовував їх поведінку.

За допомогою особливостей Blockchain технології - можна створювати розподілену систему записів користвачів. Одним з важливих методів захисту інформації при використанні цієї технології є автоматичне застосування хешування інформації за допомогою хешування. Таким чином ми будемо використовувати найновітніші засоби захисту на базі технологій SHA.

Створення безпечних локальних мереж з використанням передових технологій інформаційної безпеки вимагає системного підходу та поєднання різноманітних заходів захисту [5]. Правильне використання технологій шифрування, мережевих брандмауерів, систем ідентифікації та автентифікації, але треба слідкувати за тим щоб вартість безпеки не перевищувала розумні кордони.

Список використаних джерел

1. Голубничий Д.Ю. et al. Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації, 2021.
2. William Stallings. Cryptography and Network Security: Principles and Practice.: Pearson. 2016 p. 752c.
3. Сєвєрінов О.В., Хрєнов А.Г. Аналіз сучасних систем виявлення вторгнень. // Системи обробки інформації 6 (2014): 122-124.
4. Кліпоносова В.С., Сєвєрінов О.В. Сучасні методи біометричної ідентифікації та автентифікації користувачів. // ВА ЗС АР; НТУ" ХПІ"; НАУ, ДП" ПДПРОНДІАВІАПРОМ"; УмЖ, 2021.
5. Michael E. Whitman, Herbert J. Mattord. Principles of Information Security. Cengage Learning. 2018 p. 656 c.

УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.159

СТРАТЕГІЇ АДАПТАЦІЇ CIS CONTROLS ДО СПЕЦИФІКИ СЕКТОРУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Уманець М.С.
Науковий керівник – Євгеньєв А.М.
Харківський національний університет радіоелектроніки
61166, Харків,просп.Науки,14, каф. БІТ
e-mail:mariia.umanets@nure.ua

This paper presents the main steps to start implementing CIS CONTROLS for any system or organization, both private and public sector. The key stages are considered, the observance of which will contribute to the increase of the level of cybersecurity of information systems, reduction of the risks of cyberattacks and their consequences, and effective use of CIS Controls to protect information systems.

Сучасні стандарти та законодавство вимагають від організацій впровадження специфічних заходів безпеки та більш точного та адаптованого контролю. Керування CIS Controls - це пріоритетний набір дій, розроблений світовою IT-спільнотою з метою підвищення рівня безпеки інформаційних систем та даних [1]. CIS Controls визначають ключові кроки, які організації повинні вживати для захисту від загроз, включаючи кібератаки, витоки даних та зловживання привілеями. Адаптація цих контролів до конкретних потреб сектору інформаційної безпеки дозволяє забезпечити ефективний захист, враховуючи специфіку діяльності та ризики даного сектору.

Для ефективного впровадження та адаптації CIS Controls до певної інформаційної системи необхідно дотримуватися певної стратегії, яку поділено на кроки [2].

Першим рекомендованим кроком є «Проведення інвентаризації активів». Важливо з самого початку розуміти, що саме підлягає захисту, цей крок відповідає Критичним контролям безпеки 1 і 2:

- CSC 1. Інвентаризація та контроль апаратних засобів. (Активне керування всіма апаратними пристроями в мережі так, щоб доступ до них мали лише авторизовані пристрої.)
- CSC 2: Інвентаризація та контроль програмних активів. (Активне керування усім програмним забезпеченням у мережі, щоб лише дозволене програмне забезпечення було встановлене та могло виконуватися.)

На другому етапі необхідно провести «Вимірювання засобів контролю активів», який включає безперервне управління вразливостями, контрольоване використання адміністративних привілеїв, безпечну конфігурацію апаратного та програмного забезпечення на мобільних пристроях, ноутбуках, робочих станціях та серверах, захист електронної пошти та веб-браузерів, захист від

шкідливого програмного забезпечення, можливість відновлення та захист даних.

Третій крок – це захист зовнішнього контуру мережі. На цьому кроці необхідно забезпечити обмеження та контроль мережевих портів, протоколів і служб. Створити та активно керувати конфігурацією безпеки пристроїв мережевої інфраструктури, використовуючи суворий процес управління конфігурацією та контролю змін, щоб запобігти використанню зловмисниками вразливих сервісів та налаштувань, а також забезпечити контроль бездротового доступу.

Крок чотири. Виявлення та реагування на інциденти [3]. Невід'ємною частиною впровадження контролю є розробка інфраструктури моніторингу, аналізу та реагування на інциденти для швидкого виявлення атаки, а потім ефективного обмеження збитків, усунення присутності зловмисника та відновлення цілісності мережі та систем.

П’ятий крок це навчання та контроль користувачів, так як люди є найслабшою ланкою в ланцюгу безпеки. Плануючи та впроваджуючи навчання та моніторинг користувачів рекомендовано звернути увагу на такі ключові моменти як: захист електронної пошти та веб-браузерів, контрольоване використання адміністративних привілеїв, впровадження програми підвищення обізнаності та навчання з питань безпеки.

Фінальним, шостим кроком розглянутої стратегії є тестування. Після впровадження засобів контролю доцільно використовувати такі інструменти, як тестування на проникнення, щоб переконатися, проведена робота виконана успішно. Це необхідно робити на регулярній основі, з метою перевірки загальної сили захисту організації імітуючи цілі та дії зловмисника.

CIS Controls - це базові засоби контролю безпеки, які суб’єкти як приватного так і публічного сектору можуть використовувати для вдосконалення своєї програми кібербезпеки. Вони дають чітке уявлення про те, чого не вистачає у запезпечені безпеки, і можуть бути використані як дорожня карта, навіть впровадження перших 4-5 наборів засобів контролю може значно підвищити стійкість компанії. CIS Controls зосереджені не лише на впровадженні, але й на забезпеченні гарантій за допомогою реалізації, вимірювання, автоматизації та звітності.

Список використаних джерел

1. CIS controls v8. Official edition.

2. Marotta L. 8 steps to successfully implement the CIS top 20 controls | rapid7 blog. *Rapid7*. URL: https://www.rapid7.com/blog/post/2020/04/07/8-steps-to-successfully-implement-the-cis-top-20-controls-in-your-organization/ (дата звернення: 01.03.2024).

3. Ушатов В., Сєвєрінов О.В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. – Харків: ХНУРЕ, 2019. - С. 104–105.

УДК 005.94

АНАЛІЗ МЕТОДУ ЛІНІЙНОГО КРИПТОАНАЛІЗУ

Д.Д. Федірко
Науковий керівник – ст. викладач кафедри БІТ Данилов А.Д.
Харківський національний університет радіоелектроніки, м. Харків, Україна
dmytro.fedirko@nure.ua

The article is devoted to the consideration of the main methods of cryptanalysis of string and block encryption systems. As an example, the article analyzes the most well-known methods of cryptanalysis - for linear codes: the method of full key search, side attacks, for block codes: full (total) key search, the method of meeting in the middle, differential cryptanalysis. Particular attention is paid to the method of linear cryptanalysis. After the analysis of open sources of information, an overview of the chosen method, its essence, advantages, disadvantages and scope of application was carried out.

У сучасному світі з кожним днем все більше розвиваються комп'ютерні технології, методи передачі та обробки інформації. На жаль, разом з цим прогресом з'являються і нові види загроз, вразливостей та атак, через які дані користувачів можуть бути втрачені, розкриті або модифіковані. Для захисту інформації в комп'ютерних системах використовуються криптографічні алгоритми, що уберігають користувачів від інформаційних загроз.

Атакуючи алгоритм шифрування, зловмисник зазвичай має дві основні цілі: знайти секретний ключ або знайти відкритий текст, що відповідає зашифрованому. Тому актуальним є проведення досліджень методів криптоаналізу для оцінки стійкості існуючих криптографічних алгоритмів.

Криптоаналіз – це наука про методи здобуття вихідного значення зашифрованої інформації, не маючи доступу до секретної інформації (ключа), необхідної для цього [1].

Найпоширеніші методи криптоаналізу наведені на рисунку 1 [2].

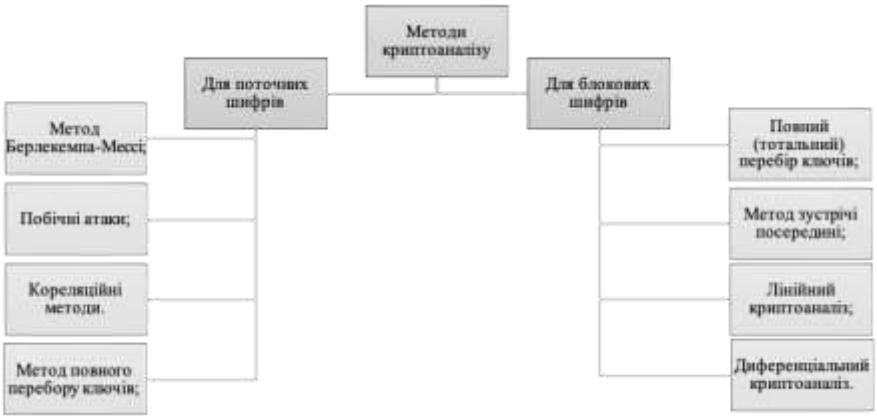


Рисунок 1 − Методи криптоаналізу.

Існує багато методів криптоаналізу, але в роботі детально розглянемо саме лінійний криптоаналіз. Лінійний криптоаналіз є ефективним для аналізу блочних шифрів, оскільки він дозволяє виявити статистичні залежності між вхідними і вихідними бітами шифру. Це допомагає знаходити ключі шифрування та розкривати секретну інформацію.

Лінійний криптоаналіз був винайдений японським криптологом Міцуру Мацуї (Mitsuru Matsui). Даний метод використовує лінійні наближення перетворень, що виконуються алгоритмом шифрування. Цей метод дозволяє знайти ключ, маючи досить велику кількість пар (незашифрований текст, зашифрований текст)[3].

Розглянемо основні принципи, на яких базується лінійний криптоаналіз. Лінійний криптоаналіз базується на тому, що існує можливість замінити нелінійну функцію на її лінійний аналог.

Метою лінійного криптоаналізу є пошук лінійного рівняння виду $P_{i1} \oplus P_{i2} \oplus \dots P_{ia} \oplus C_{j1} \oplus C_{j2} \oplus \dots \oplus C_{jb} = K_{k1} \oplus K_{k2} \oplus \dots \oplus K_{kc} (1)$, де P_n, C_n і K_n - n-і біти відкритого тексту, шифротекста й ключа відповідно.

Для випадково обраних частин відкритого тексту, шифротекста і ключа ймовірність того, що такі біти відповідають один одному, становить приблизно 1/2. Якщо криптоаналітику вдається виявити біти, де ймовірність P відрізняється від 1/2, це співвідношення можна використовувати для розкриття алгоритму.

Це рівняння означає, що при виконанні операції XOR над певними бітами незашифрованого повідомлення і певними бітами зашифрованого повідомлення отримується біт, який є результатом XOR певних бітів ключа. Цей процес відомий як лінійне наближення, яке може бути вірним з ймовірністю P.

Рівняння формуються таким чином: значення лівої частини обчислюються для значної кількості пар відповідних фрагментів незашифрованого та зашифрованого блоків. Якщо результат дорівнює нулю у більш ніж половині випадків, то вважають, що $K_{k1} \oplus K_{k2} \oplus \dots \oplus K_{kc} = 0$. Якщо в більшості випадків виходить $1 - K_{k1} \oplus K_{k2} \oplus \dots \oplus K_{kc} = 1$. Таким чином формується система рівнянь, рішенням якої є ключ. Подібно до диференціального криптоаналізу, результати лінійного криптоаналізу повинні враховуватися при розробці алгоритмів симетричного криптоаналізу.

Лінійний криптоаналіз часто використовується в поєднанні з атакою методом "грубої сили" – певні біти ключа виявляються за допомогою лінійного криптоаналізу, після чого здійснюється вичерпний пошук за можливими значеннями інших бітів.

Лінійний криптоаналіз має одну досить корисну властивість: за певних умов співвідношення (1) може бути перетворене до наступного:

$$C_{j1} \oplus C_{j2} \oplus \ldots \oplus C_{jb} = K_{k1} \oplus K_{k2} \oplus \ldots \oplus K_{kc}.$$

У даному випадку відсутні будь-які біти відкритого тексту у зазначеному співвідношенні, що означає можливість побудови атаки лише на основі шифротексту за допомогою лінійного криптоаналізу. Це ще більше розширює сферу застосування лінійного криптоаналізу, оскільки атака, яка вимагає лише перехопленого шифротексту, є найбільш практичною.

У даний час, існує багато методів криптоаналізу як для поточних шифрів, так і для блокових. Кожен метод криптоаналізу призводить до перегляду безпеки шифрів, до яких він застосовується. Лінійний криптоаналіз − це метод атаки на шифри, який базується на виявленні лінійних зв'язків між вхідними та вихідними бітами шифрувального алгоритму. Незважаючи на свою ефективність у деяких випадках, він має свої недоліки.

По-перше, для успішної реалізації атаки потрібно мати значну кількість пар тексту − шифротексту, що може бути важким завданням, особливо якщо доступ до таких даних обмежений.

По-друге, ефективність атаки може значно залежати від точності вибору початкових умов, тобто визначення правильного вихідного пункту для проведення аналізу.

Незважаючи на ці обмеження, лінійний криптоаналіз широко використовується в криптографії для атак на різні шифри, які використовують лінійні перетворення, такі як DES і AES, а також у дослідженнях нових криптографічних алгоритмів для оцінки їхньої стійкості. Наприклад, метод був успішно використаний для злому DES. У 1994 році, Matsui зміг зламати DES, використовуючи атаку лінійним криптоаналізом, використовуючи близько 2^43 пар тексту-шифротексту.

Таким чином метод лінійного криптоаналізу є доволі розповсюдженим та ефективним методом захисту інформації та може бути успішно використаний для захисту інформаційних активів організації.

Список використаних джерел:

1. Криптоаналіз. Криптографічні протоколи: веб сайт. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/36273 (дата звернення: 27.02.2024).

2. Cryptanalysis in Cybersecurity: веб сайт. URL: https://www.zenarmor.com/docs/network-security-tutorials/what-is-cryptanalysis (дата звернення: 27.02.2024).

3. Криптоаналіз: веб сайт. URL: https://www.wikidata.uk-ua.nina.az/Криптоаналіз.html (дата звернення: 28.02.2024).

УДК 004.056.5

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЙНИХ ДАНИХ КОРИСТУВАЧІВ В СФЕРІ VOICE OVER IP

Черкашинов Т.К.
Науковий керівник - старший викладач В'юхін Д.О.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail:tymur.cherkashynov@nure.ua

Voice over IP telephony, which is replacing telecommunications and is becoming more common every day among companies that deal with telephone communications. Since VoIP is an Internet protocol, it has several vulnerabilities that depend on the use of data transfer protocols from VoIP service providers. He is also susceptible to many attacks (DoS, man-in-the-middle attack). The transition to VoIP has not created the opportunity for such attacks, but it may make them easier to execute. The main objective of this work will be to analyze the VoIP system and its data transmission protocols, consider potential risks for attacks and apply preventive measures to complicate or eliminate the possibility of attacks. Another important task is to ensure confidentiality for VoIP users.

Оскільки з часом поширеність використання VoIP сервісів тільки зростає, відповідно зростає попит користувачів та увага зловмисників до цього сервісу. Потреба в захисті особистих даних користувачів, а також в захисті постачальників від перевантаження мережі зростає з кожним днем, тому для забезпечення стабільної роботи VoIP сервісів та конфіденційності особистої інформації користувачів виникає потреба в аналізі, впровадженні та удосконалені систем та методів захисту як під час передачі трафіку, так і під час збереження інформації (історія та записи дзвінків, тарифікація клієнтів, історія змін тощо).

В сучасному світі існує безліч компаній, які так чи інакше пов'язані з Voice over IP (VoIP): це можуть бути компанії, які займаються налаштуванням цього трафіку, або компанії, чиї співробітники безпосередньо користуються Voice over IP трафіком. Безпека даного методу зв'язку дуже актуальна в наш час: через Voice over IP передається багато особистої інформації– починаючи від одноразових кодів аутентифікації через СМС та закінчуючи бесідами співробітників компанії на теми, оприлюднення яких може стати перевагою для компанії-конкурента.

Головною метою цієї роботи є розглядання, аналіз та пошук способів удосконалення для найпоширеніших методів захисту в сфері Voice over IP трафіку. Для розгляду ми охопимо усі розділи VoIP трафіку:

1. Протоколи передачі даних(SIP, TCP тощо): будуть розглянуті переваги та недоліки найбільш актуальних на даний момент часу протоколів, їхнє призначення та методи захисту від потенційних атак;

2. Сервери, які займаються структуруванням та збором даних; тарифікації услуг, обробкою платежів та виставленням платежів абонентам– білінги: без існування білінгу дуже важко уявити собі будь-якого оператора зв'язку. Оскільки білінг-сервери у більшості випадків є серверами з базами даних, які зберігають велику кількість даних(дані о дзвінках чи СМС, тарифи та дані про операторів дзвінків) та є найбільш пріоритетними через велику кількість конфіденціальної інформації, захист білінг-серверів є однією із найголовніших задач під час аналізу безпеки VoIP-мережі;

3. Сервери, які безпосередньо займаються передачею трафіку(наприклад, RTP-сервери): Захисту цих серверів також повинно приділятися багато уваги, оскільки саме через ці сервери йде трафік у реальному часі. Тож перевантаження цього серверу буде нести великі збитки для компанії, тому що це буде означати, що живий трафік, який надходить від клієнтів, не буде оброблятися через перевантаженість серверу.

Окрім указаних вище методів ми розглянемо та проаналізуємо найпоширеніші види загроз та атак на VoIP мережі, такі як:

1. Атаки типу чоловік посередині(man-in-the-middle attack, MITM attack): атака, яка спрямована на перехоплення трафіку, методологією якого є підключення до вже існуючих каналів зв'язку. Використовується для прослуховування та отримання конфіденційної інформації, або зміни переданої інформації з метою отримання потрібних відповідей від учасників розмови;

2. Атаки типу відмова в обслуговуванні(Denial of service attacks): мета такого типу атак– зробити сервіс недоступним для користувачів. Для VoIP методами таких атак є відмовлення сервісу через флуд дзвінків/СМС;

3. Шкідливе ПЗ та вірусі: оскільки VoIP є інтернет сервісом, існує вірогідність зараження шкідливим ПЗ(сніфери, черв'яки, шкідливі макроси тощо).

Метою розглядання атак на Voice over IP є їх аналіз та приведення заходів для мінімізації фактору ризику виникнення таких атак, або виконання заходів, які унеможливлюють їх проведення. Перш за все ми повинні розглядати можливість та основні ознаки певної атаки:

1. Man-in-the-middle attack: найбільш очевидною ознакою цієї атаки розриви у часі відповіді – під час розмови двох сторін дії двох користувачів можуть займати різну кількість часу під час виконання однакової дії з двох сторін. Така прірва у часі обробки запиту може позначати перехоплення та/або зміну даних зловмисником, що прослуховує дану розмову. Методи захисту від цих атак різні. Наприклад, користувачі та оператор мають користуватися захищеними протоколами HTTPS, оскільки під час користування протоколом HTTP зловмисник має змогу зробити підміну сайту. HTTPS протоколи мають свій SSL-сертифікат, що не дає змоги зловмиснику зробити підміну сертифікату, оскільки ліцензіати одразу фіксують підозрілу активність сайту та можуть заблокувати сертифікат тому що дорожать власною репутацією. Також

важливим кроком забезпечення безпеки є використання багатофакторної аутентифікації. Однак найбільш ефективним та важливим рішенням буде моніторинг мережі на ознаку підозрілої активності: це можуть бути сліди зламу, або виявлення третьої сторони з дампу дзвінка.

2. DoS: характерними ознаками для цієї атаки є перевантаження мережі великою кількістю запитів. Одним з рішень для захисту від такої атаки є обмеження кількості запитів від одного користувача(чудовим прикладом є використання rate функції веб серверу Nginx) а також аналіз цих запитів із виявленням IP, який намагається перевантажити сервіс. Після виявлення IP з якого зловмисник надсилає велику кількість запитів(наприклад, навантаження 600 запитами у секунду нашого RTP-серверу, який здатен підтримувати до 700 одночасних дзвінків).

3. Шкідливе ПЗ: ознак для даного пункту існує безліч: від навантаження серверу при відсутності запитів до видалення важливих для системи компонентів. Засоби захисту в цьому пункті повинні застосовуватися майже завжди: на серверному обладнанні повинно бути встановлено підтримувальні та регулярно оновлюванні версії ОС з метою мінімізації зламу через вразливості старих операційних систем. Також дуже важливе правильне налаштування фаерволу серверу, яке буде блокувати підключення з неавторизованих IP адрес. Дані для доступу до серверу повинні ретельно охоронятися, а співробітник компанії мають бути уважними під час роботи: не допускається з’єднання по небезпечним протоколам(тільки HTTPS) а також поширення конфіденційної інформації незнайомим користувачам, або тим, хто видає себе за авторизованих спіробітників/клієнтів.

Також важливою метою буде дотримання балансу між затратами на забезпечення безпеки та вірогідністю проведення атаки.

Список використаних джерел

1. «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу». 2021. https://duikt.edu.ua/ua/lib/1/category/742/view/2173#page=51

2. Detection of Intruders and Flooding in VoIP using IDS, Jacobson Fast and Hellinger Distance Algorithms. 2020. https://www.researchgate.net/publication/3301407_Detecting_VoIP_Floods_Using_the_Hellinger_Distance

3. Involved Security Solution in Voice over IP Networks. 2023. https://www.ajrt.dz/index.php/ajrt/article/view/110

4. «Защита информации В IP-телефонии». А. А. Замула, Ю. С. Павленко. с.191–194. 2001. https://openarchive.nure.ua/handle/document/17305

УДК 004.056.5

КЛЮЧОВІ ПРОБЛЕМИ БЕЗПЕКИ У ТЕХНОЛОГІЯХ БЕЗДРОТОВОГО ЗВ'ЯЗКУ 5G

Чибізов І. О.
Науковий керівник- старший викладач В’юхін Д.О.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: ihor.chybizov@nure.ua

5G is the fifth generation of mobile communications that offers significantly higher speed, bandwidth and reliability compared to 4G. The growing use of 5G in various industries, such as the Internet of Things (IoT), autonomous vehicles, and telemedicine, makes the issue of 5G communication security extremely important. Previous generations of mobile networks had the primary goal of providing fast and reliable data services to users. However, 5G extends this concept by offering a wide range of wireless services through different access platforms and multi-layer networks. It is through services that the main issues of technology security will be considered in this work.

5G – це п'яте покоління мобільного зв'язку, яке пропонує значно більшу швидкість, пропускну здатність та надійність, порівняно з 4G. Зростаюче використання 5G у різних галузях, таких як Інтернет речей (IoT), автономні транспортні засоби та телемедицина, робить питання безпеки зв'язку 5G надзвичайно важливим [1].

Попередні покоління мобільних мереж мали основну мету у наданні швидких і надійних послуг передачі даних для користувачів. Однак 5G розширює цю концепцію, пропонуючи широкий спектр бездротових послуг через різні платформи доступу та багаторівневі мережі [2].

Архітектура 5G створює динамічну, узгоджену та гнучку структуру для підтримки різноманітних програм. Вона використовує більш інтелектуальну систему з мережами радіодоступу (RAN), які вже не обмежені лише базовими станціями чи складною інфраструктурою. Замість цього, 5G впроваджує дезагреговану, гнучку та віртуальну RAN з новими інтерфейсами, що створюють додаткові точки доступу до даних.

Для 5G існують два варіанти розгортання:

1. Архітектура "Неавтономна" (NSA), де мережа радіодоступу 5G (AN) та інтерфейс New Radio (NR) використовуються разом з існуючою базовою мережею інфраструктури LTE та EPC (відповідно до 4G Radio та 4G Core), що дозволяє використовувати технологію NR без необхідності заміни мережі. У цій конфігурації підтримуються лише послуги 4G, але вони використовують можливості, що пропонує 5G New Radio (зокрема, менша затримка). NSA також відомий як "E-UTRA-NR Dual Connectivity (EN-DC)" або "Архітектурний варіант 3" (рисунок 1).

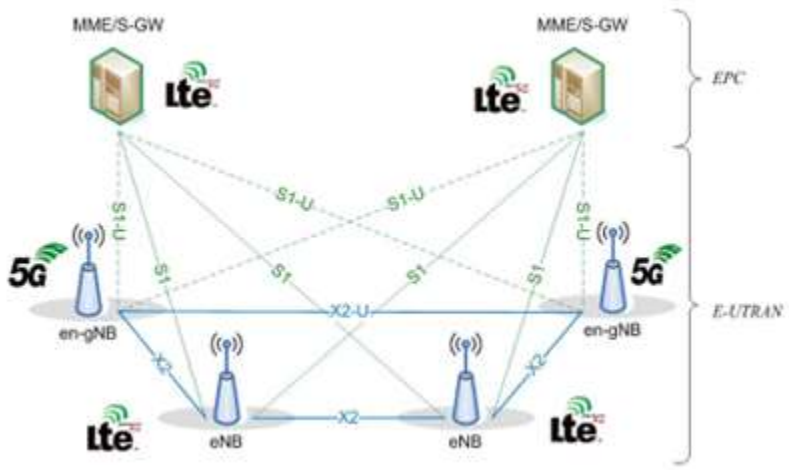


Рисунок 1 – Архітектура неавтономного доступу до мережі 5G

2. Архітектура "Автономна" (SA), де NR підключений до 5G CN. Тільки в цій конфігурації підтримується повний набір послуг 5G Phase 1 (рисунок 2).

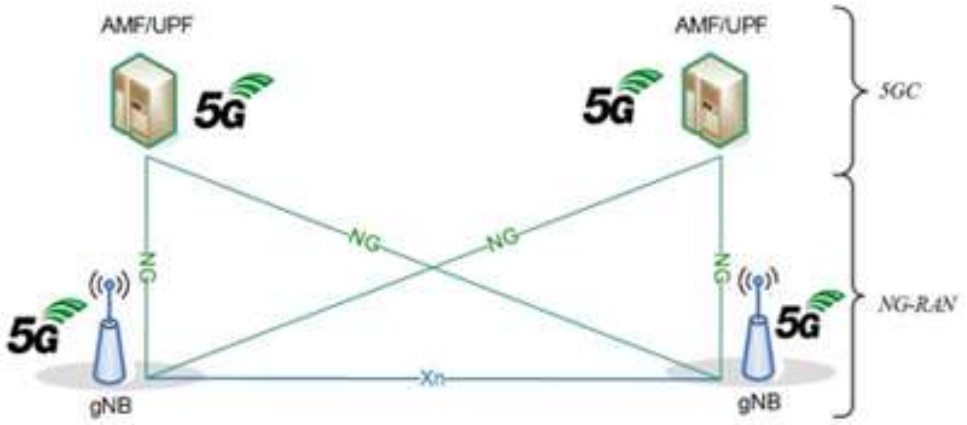


Рисунок 2 – Архітектура автономного доступу до мережі 5G

Впровадження технології 5G пов'язане з рядом викликів в галузі безпеки, які потребують уваги та вирішення. Одним із головних аспектів є безпека критичної інфраструктури, яка стає більш вразливою через збільшення кількості підключених пристроїв та IoT. Порушення безпеки в таких системах може мати катастрофічні наслідки для суспільства. Крім того, забезпечення безпеки радіоінтерфейсів важливе для запобігання доступу до конфіденційної інформації через незахищені канали [3].

Розробка ефективних стратегій та рішень для вирішення цих викликів є критичною для забезпечення безпеки та надійності мереж 5G. Співробітництво між виробниками обладнання, операторами мереж та регуляторними органами може допомогти розробити стандарти та протоколи, які забезпечать безпеку мереж 5G на високому рівні [3].

Деякі з ключових викликів, визначених Mobile Networks Next Generation (NGMN) включають такі:

1. Флеш-мережевий трафік: Збільшена кількість підключених пристроїв та IoT може призвести до перевантаження мережі, що може вплинути на безпеку та стабільність системи.
2. Безпека радіоінтерфейсів: Використання незахищених каналів для передачі ключів шифрування може зробити мережу вразливою перед атаками.
3. Цілісність площини користувача: Відсутність криптографічного захисту цілісності даних користувача може призвести до ризику несанкціонованого доступу до чутливої інформації.
4. Безпека роумінгу: Недостатня оновлення параметрів безпеки під час роумінгу між мережами операторів може призвести до ризику компрометації безпеки.
5. Атаки типу "відмова в обслуговуванні" (DoS): Напади на інфраструктуру мережі, такі як DoS, можуть призвести до переривання послуг та зниження якості обслуговування.
6. Сигнальні шторми: Неспроможність розподілених систем керування координувати свою діяльність може призвести до ситуацій, коли рівень сигналізації перевищує потреби мережі, що може вплинути на її ефективність.
7. DoS-атаки на пристрої кінцевих користувачів: Відсутність адекватних заходів безпеки на пристроях кінцевих користувачів може зробити їх вразливими перед атаками та незаконним доступом до особистих даних.

Як можна побачити з виявлених вище проблем то основна їх частина походить від збільшення кількості підключень до базових станцій на які можуть бути здійснені DoS-атаки через ці пристрої за допомогою слабозахищених каналів передачі даних. Ще існує ймовірність неуважного користувача мобільного зв'язку і якщо всі фактори складуться, то втрата особистих даних, грошових коштів тощо стає постійною загрозою безпеці.

Вирішенням виявлених загроз можна зробити обмеженням пристроїв на одну базову станцію, автоматичним оновленням протоколів безпеки і якщо це корпоративна мережа вести облік користувачів мережі та активних пристроїв.

Список використаних джерел

1. 5G NR: технологія бездротового доступу нового покоління. Ерік Дальман, Стефан Парквалл, Йохан Скольд. Академ. вид.: 2020 р.. 548 с.
2. Тимошенко, Д. В. Публікація: Вплив розвитку 5G технологій на майбутнє телекомунікаційного сектору 2023р.
https://openarchive.nure.ua/handle/document/25365
3. Базові мережі 5G: посилення цифровізації. Стефан Роммер, Пітер Хедман, Магнус Олссон, Ларс Фрід, Шабнам Султана. Академічна преса: 2019 р., 476 с.

АЛФАВІТНИЙ ПОКАЗЧИК

А

Ахмедзянова О. А. 53

Б

Бабаєва К. Г. гизи 88
Блінна В. С. 91
Боровик П. К. 5

В

Веселовський О. Г. 94
Воронін Р. А. 7

Г

Гаража Р. Ю. 96
Герасимчук Д. В. 9
Гунько М. А. 11
Гузенко Н. В. 99

Д

Дараган Д. М. 13
Дорофєєва К. І. 101

Є

Єрьомін Д. А. 15

Ж

Жигалкін Є. В. 17
Жук М. В. 19, 63

З

Заброда І. С. 21
Зюнд Б. В. 23

І

Івашов В. А. 103
Ілляшенко І. Б. 25

К

Кайдалов В. Д. 105
Кравченко А. А. 108
Кузнєцов Д. О. 27

Л

Леонова А. О. 111
Лісняк Д. С. 113
Лось Д. І. 115
Ляшко М. С. 117

М

Малахова А. А. 120
Мартиненко Я. А. 122
Мельніченко Ф. О. 29
Мідіна С. С. 32
Міхаль О. П. 50
Міхнов Є. Д. 34
Мякшин А. С. 38

Н

Набойщиков Б. Ю. 125
Наконечний В. В. 128
Неізвєсна М. Р. 131

О

Ободяк В. К. 133
Осипов Д. О. 41

П

Павлов О. А. 135, 137, 139
Папазов К. О. 141
Пашнєва О. Р. 144
Піглюк І. М. 43
Пічієнко М. Г. 147, 150

Погорєлова Л. А. 45
Потопа В. О. 48
Просолов В. В. 153

Р

Радченко В. О. 50
Радченко О. П. 53
Рибалов О. О. 56

С

Савченко Є. Ю. 58
Свергун В. А. 61
Сергородцев І. Д. 19
63
Сердюк С. С. 66
Снігур А. Р. 68

Т

Топіха Т. Б. 155
Тяптя А. В. 157

У

Уманець М. С. 159

Ф

Федірко Д. Д. 161
Фролов Д. Є. 11

Х

Хрустальов Є. К. 70

Ц

Ціпковський В. О. 73

Ч

Чепурна І. С. 76
Чередниченко І. С. 79
Черкашинов Т. К. 164
Чіві Я. В. 81
Чибізов І. О. 167

Ш

Швиденко А. О. 83
Штонда О. А. 85

ЗМІСТ

КОМП’ЮТЕРНА ІНЖЕНЕРІЯ: СУЧАСНІ ТЕХНОЛОГІЇ РОЗРОБКИ ТА ПРОГРАМУВАННЯ КОМП’ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ ….4

ЗАХИСТ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ РЕСУРСІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ (ІКС) 87

АЛФАВІТНИЙ ПОКАЗЧИК 170

«РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ В XXI СТОЛІТТІ»

Матеріали 28-го Міжнародного молодіжного форуму

Відповідальні за випуск: О.С. Ляшенко

Комп’ютерна верстка: О.А. Єрошенко

Матеріали збірника публікуються в авторському варіанті

без редагування

Матеріали XXVIII Міжнародного молодіжного форуму

«Радіоелектроніка та молодь у XXI столітті»

Харківський національний університет радіоелектроніки