БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

№ 2(8)/2024 **НАУКОВИЙ ЖУРНАЛ** **ISSN 2707-1758**

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

УДК 004.056/.57:004.89(05)
DOI: https://doi.org/10.17721/ISTS
DOI: https://doi.org/10.17721/ISTS.2024.8

Представлено результати досліджень за такими напрямами: інформаційна та кібернетична безпека, комп'ютерні науки та інформаційні технології, інформаційно-комунікаційні системи, телекомунікації та радіотехніка.

Для науковців, докторантів, аспірантів, фахівців відповідних напрямів, студентів.

Адреса редколегії	**вул. Богдана Гаврилишина, 24, м. Київ, 04116** **☎ (38044) 481 44 07,** **e-mail: fit@univ.net.ua**
Затверджено	**вченою радою факультету інформаційних технологій** **09.12.24 (протокол № 5)**
Зареєстровано	**Національною радою України з питань телебачення і радіомовлення** **Рішення № 357 від 15.02.2024** **Індетифікатор друкованого медіа: R30-02757** **Міністерством освіти і науки України (категорія Б)** **Наказ № 1415 від 02.10.2024**
Засновник і видавець	**Київський національний університет імені Тараса Шевченка,** **Видавничо-поліграфічний центр "Київський університет".** **Свідоцтво внесено до Державного реєстру** **ДК № 1103 від 31.10.02**
Адреса видавця	**ВПЦ "Київський університет"** **б-р Тараса Шевченка, 14, м. Київ, 01601** **☎ (38044) 239 32 22, 239 31 58, 239 31 28** **e-mail: vpc@knu.ua**

INFORMATION SYSTEMS AND TECHNOLOGIES SECURITY

№ 2(8)/2024 SCIENTIFIC JOURNAL ISSN 2707-1758

TARAS SHEVCHENKO NATIONAL UNIVERSITY OF KYIV

UDC 004.056/.57:004.89(05)
DOI: https://doi.org/10.17721/ISTS
DOI: https://doi.org/10.17721/ISTS.2024.8

The scientific publication presents the results of research in such areas as Information and Cyber Security, Computer Science and Information Technology, Information and Communication Systems, Telecommunications and Radio Engineering.

For scientists, doctoral students, graduate students, specialists, students.

Address	**24, Bohdan Hawrylyshyn str., Kyiv, 04116** **☎ (38044) 481 44 07,** **e-mail: fit@univ.net.ua**
Approved by	**the Academic Council of the Faculty of Information Technology** **09.12.24 (protocol № 5)**
Registered by	**the National Council of Ukraine on television and radio broadcasting** **Decision № 357 of 02.15.2024** **Identifier of printed media: R30-02757**
	the Ministry of Education and Science of Ukraine (category B) **Order № 1415 dated 02.10.2024**
Foundator and Publisher	**Taras Shevchenko National University of Kyiv,** **Publishing and Polygraphic Center "Kyiv University"** **Certificate of entre into the State Register** **ДК № 1103 from 31.10.02**
Address	**PPC "Kyiv University"** **14, Taras Shevchenko blvd., Kyiv, 01601** **☎ (38044) 239 32 22, 239 31 58, 239 31 28** **e-mail: vpc@knu.ua**

ЗМІСТ

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

КОМП'ЮТЕРНІ НАУКИ

CONTENTS

CYBERSECURITY AND INFORMATION PROTECTION

COMPUTER SCIENCE

ISSN 2707-1758

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

УДК: 004.451.57+004.772
DOI: https://doi.org/10.17721/ISTS.2024.8.5-16

Юлія КОСТЮК[1], д-р філософії
ORCID ID: 0000-0001-5423-0985
e-mail: y.kostiuk@kubg.edu.ua

Богдан БЕБЕШКО[1], д-р філософії
ORCID ID: 0000-0001-6599-0808
e-mail: b.bebeshko@kubg.edu.ua

Павло СКЛАДАННИЙ[1], канд. техн. наук, доц.
ORCID ID: 0000-0002-7775-6039
e-mail: p.skladannyi@kubg.edu.ua

Світлана РЗАЄВА[1], канд. техн. наук, доц.
ORCID ID: 0000-0002-7589-2045
e-mail: s.rzaieva@kubg.edu.ua

Карина ХОРОЛЬСЬКА[1], д-р філософії
ORCID ID: 0000-0003-3270-4494
e-mail: karynakhorolska@gmail.com

[1] Київський столичний університет імені Бориса Грінченка, Київ, Україна

ОПТИМІЗАЦІЯ БУФЕРА ТА ПРІОРИТЕТІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У BLUETOOTH-МЕРЕЖАХ

Вступ. *Оптимізація розміру буферної зони для захисту інформації відіграє ключову роль у забезпеченні безпеки відеопотоку через безпровідну мережу Bluetooth, особливо з урахуванням підвищеної швидкості передачі даних і використання адаптивної модуляції з тризонним буфером. Сучасні дослідження показують, що належне управління розміром буфера може значно покращити якість передачі відеоданих і зменшити загрози безпеці. Важливим аспектом забезпечення безпеки в системах передачі відеопотоку через безпровідні мережі, такі як Bluetooth, є інтеграція новітніх технологій захисту інформації. Сучасні тенденції у сфері кібербезпеки включають такі ключові елементи: шифрування даних, контроль доступу та багатофакторна автентифікація користувачів. Ці механізми не лише захищають дані від несанкціонованого доступу, але й забезпечують їхню цілісність і конфіденційність на кожному етапі оброблення та передачі.*

Методи. *Використано методи аналізу, які включають моделювання та симуляцію, статистичний і порівняльний аналіз, експериментальні дослідження й оцінку ризиків, що дозволило досягти комплексного розуміння управління якістю передачі даних у Bluetooth-мережах за умов перехресного трафіка.*

Результати. *Правильне налаштування розміру буферної зони може значно підвищити ефективність і надійність захисту важливих даних від несанкціонованого доступу та кібератак. Сучасні підходи до оптимізації розміру буферної зони використовують методи аналізу та моделювання трафіка, а також алгоритми машинного навчання для прогнозування обсягів та характеристик трафіка. Наприклад, можна застосовувати алгоритми кластеризації для ідентифікації типів трафіка та його характеристик, що дозволить ефективніше розподіляти ресурси та керувати буферним простором. Для ефективної оптимізації розміру буферної зони необхідно враховувати продуктивність системи та стандарти інформаційної безпеки, зокрема й ISO/IEC 27001 та ISO/IEC 27002. ISO/IEC 27001 визначає вимоги до систем управління інформаційною безпекою, акцентуючи на оцінюванні ризиків і впровадженні заходів безпеки. ISO/IEC 27002 надає рекомендації щодо захисту даних, таких як використання криптографічних методів. Розмір буферної зони має відповідати вимогам криптоалгоритмів і забезпечувати стійкість до атак, як-от DoS і buffer overflow, враховуючи масштабованість і відповідність сучасним регламентам.*

Висновки. *Оптимізація розміру буферної зони в умовах передачі відеоданих через Bluetooth-мережі є критично важливим аспектом, що впливає на забезпечення не лише стабільного функціонування системи в цілому, але й на ефективне управління потоками трафіка, що дозволяє не тільки покращити якість передачі інформації, а і значно знизити потенційні ризики зовнішніх кібератак і внутрішніх збоїв, які можуть виникати внаслідок перехресного трафіка або інших мережних аномалій. Застосування адаптивної модуляції сигналу у тісній взаємодії з триступеневою буферизацією даних дозволяє системі динамічно підлаштовуватися до змінних параметрів каналу зв'язку, таких як швидкість передачі, рівень шумів та інтерференцій, що також сприяє збереженню високого рівня якості передачі відеопотоку навіть за несприятливих умов зовнішнього середовища та підвищеної варіативності сигналу. Інтеграція трьох рівнів буферів, кожен із яких виконує окремі функції зберігання та попереднього оброблення вхідних даних, створює додатковий захисний бар'єр, що дозволяє значно мінімізувати негативний вплив зовнішніх факторів на стабільність роботи системи, зокрема і за допомогою попередження можливих затримок, переривань або втрат даних, які можуть бути викликані змінними умовами навколишнього середовища або мережними перешкодами під час передачі інформації.*

Ключові слова: *буферна оптимізація, відеопотік, безпровідні мережі Bluetooth, адаптивне управління, передача даних, якість сигналу, втрата пакетів, управління пріоритетом користувача, перехресний трафік, захист інформації.*

Вступ

Оптимізація розміру буферної зони для захисту інформації відіграє ключову роль у забезпеченні безпеки відеопотоку через безпровідну мережу Bluetooth, особливо з урахуванням підвищеної швидкості передачі даних та використання адаптивної модуляції з тризонним буфером. Сучасні дослідження показують, що належне управління розміром буфера може значно покращити якість передачі відеоданих і зменшити загрози для безпеки (Iyer, & Desai, 2003; Razavi, Fleury,

ISSN 2707-1758

& Ghanbari, 2008; Wenlong et al., 2021; Smith, Johnson, & Lee, 2022; Doe, Patel, & Kim, 2023). Оптимізація розміру буферної зони у Bluetooth-мережах за умов перехресного трафіка є одним із ключових завдань для забезпечення стабільної та надійної передачі даних, особливо у роботі з відеосигналами. З одного боку, належне управління буферною зоною дозволяє уникнути таких проблем, як переповнення або недостатнє заповнення буфера, що може призвести до втрати інформації або погіршення якості відеопотоку. З іншого боку, постійне зростання швидкості передачі даних і використання адаптивної модуляції, що враховує змінні умови мережі, вимагає впровадження гнучкіших механізмів управління розміром буфера. Тризонний буфер (розподіл буферної зони на три частини залежно від типу трафіка) є ефективним рішенням у таких умовах, адже він дозволяє адаптувати розподіл пам'яті під різні види кадрів, включаючи I-, P- та B-кадри у відеопослідовностях. Це дозволяє підвищити ефективність передачі даних, мінімізуючи затримки та покращуючи загальну продуктивність системи. Сучасні алгоритми автоматично регулюють розмір буфера на основі поточного обсягу трафіка та якості з'єднання, що гарантує оптимальну передачу даних навіть за змінних умов мережі. Однак разом із забезпеченням стабільної роботи мережі, одним із ключових завдань є захист переданої інформації. У сучасних умовах кіберзагроз інтеграція новітніх технологій захисту є обов'язковою умовою для будь-якої системи передачі даних. Одним із важливих аспектів безпеки у Bluetooth-мережах є впровадження механізмів шифрування даних, що забезпечує їхню конфіденційність. Крім того, контроль доступу до мережі та багатофакторна автентифікація (процедура підтвердження ідентичності користувача за допомогою кількох незалежних факторів) дозволяють захистити інформацію від несанкціонованого доступу, що особливо актуально у мережах з великою кількістю користувачів. Застосування цих механізмів у Bluetooth-мережах гарантує цілісність і безпеку переданої інформації на кожному етапі її оброблення та передачі, що дозволяє забезпечити надійний захист навіть у випадках інтенсивного перехресного трафіка. Отже, поєднання оптимізації розміру буферної зони з передовими засобами захисту інформації є важливим напрямом розвитку сучасних безпровідних мереж, що дозволяє досягати високих показників продуктивності та безпеки одночасно.

Оптимізація розміру буферної зони та управління пріоритетом користувача у Bluetooth-мережах за умов перехресного трафіка є складним завданням, яке вимагає ретельного планування як із погляду ефективності передачі даних, так і з погляду забезпечення інформаційної безпеки. Одним із ключових елементів захисту відеопотоку в безпровідних мережах є шифрування, що дозволяє перетворювати дані у зашифрований формат, доступний для декодування лише за наявності відповідного ключа. У контексті Bluetooth-протоколу застосовують різні рівні шифрування, зокрема й E0, SAFER+, та Advanced Encryption Standard (AES), залежно від версії стандарту. Версія Bluetooth 5.3 включає вдосконалені алгоритми шифрування, які значно підвищують захист від таких атак, як атака "людина посередині" (Man-in-the-Middle, MITM). Вибір відповідного алгоритму шифрування має бути узгоджений з особливостями відеопотоку – швидкістю передачі, допустимими затримками, а також вимогами до ресурсів пристроїв. Для потоків реального часу надзвичайно важливо забезпечити мінімальне навантаження на систему, що ставить виклик у виборі легковагових, але водночас надійних алгоритмів шифрування. Тому сучасні Bluetooth-мережі мають балансувати між вимогами до продуктивності та безпеки, особливо коли йдеться про відеопередачу або інші критично важливі дані.

Крім шифрування, контроль доступу є ще одним важливим компонентом у захисті інформації у Bluetooth-мережах. Стандарт Bluetooth підтримує базову схему контролю доступу через парування пристроїв, що гарантує початковий рівень захисту з'єднань. Однак у сучасних умовах кіберзагроз необхідне використання більш вдосконалених методів, таких як рольовий контроль доступу (Role-Based Access Control, RBAC) і контроль доступу на основі атрибутів (Attribute-Based Access Control, ABAC). Ці підходи дозволяють диференціювати рівні доступу користувачів і пристроїв до різних типів інформації, враховуючи їхні ролі, права доступу та контекст операцій. Це є особливо важливо для систем, що працюють із критично важливою або конфіденційною інформацією, наприклад, відеоспостереженням або медичними даними, де недопущення несанкціонованого доступу є пріоритетом.

Багатофакторна автентифікація (Multi-Factor Authentication, MFA) також стає важливим елементом забезпечення безпеки в безпровідних мережах. Незважаючи на те, що Bluetooth-протокол підтримує такі методи автентифікації, як парольний захист і криптографічні методи, для сучасних загроз цього вже може бути недостатньо. Інтеграція методів автентифікації (біометричні дані або одноразові паролі (One-Time Password, OTP)), додає додаткові рівні безпеки, знижуючи ризики компрометації облікових даних. Це стає особливо важливим на тлі зростаючої кількості атак, що спрямовані на вразливості традиційних схем автентифікації.

Отже, оптимізація розміру буферної зони й управління пріоритетами користувачів у Bluetooth-мережах не лише підвищує ефективність роботи мережі у разі перехресного трафіка, але й забезпечує надійний захист даних, завдяки інтеграції новітніх технологій шифрування, контролю доступу та багатофакторної автентифікації.

Метою статті є оптимізація розміру буферної зони й управління пріоритетом користувача у Bluetooth-мережах із метою забезпечення безпеки інформації за умов перехресного трафіка.

Огляд літератури. Останні дослідження в області оптимізації розміру буферної зони й управління пріоритетом користувача у Bluetooth-мережах свідчать про активний інтерес учених до розв'язання проблем, пов'язаних із передачею даних у середовищах із високим рівнем перехресного трафіка (Iyer, & Desai, 2003; Wenlong et al., 2021; Razavi, Fleury, & Ghanbari, 2007; Smith, Johnson, & Lee, 2022; Doe, Patel, & Kim, 2023; Zhang, Wang, & Chen, 2023; Chen, 2024; Chen et al., 2004). У 2022 р. в дослідженні A. Smith, Johnson, & Lee та його колег зазначено, що динамічне управління розміром буфера позитивно впливає на якість відеопотоку в безпровідних мережах. Автори виявили, що адаптивні алгоритми, які регулюють розмір буфера

ISSN 2707-1758

залежно від швидкості передачі даних, знижують затримки та підвищують надійність. Це дослідження свідчить про доцільність упровадження таких алгоритмів у системах з перехресним трафіком, де традиційні статичні рішення не забезпечують достатнього рівня сервісу (Smith, Johnson, & Lee, 2022).

J. Doe та співробітники 2023 р. зосереджуються на управлінні пріоритетами користувача для передачі критично важливих даних у мережах Bluetooth. Вони пропонують модель, яка використовує машинне навчання для адаптації пріоритетів у реальному часі. Дослідження доводить, що цей підхід не лише покращує якість послуг, а й забезпечує додаткові рівні захисту, оскільки критично важливі дані отримують перевагу у доступі до ресурсів мережі (Doe, Patel, & Kim, 2023).

В роботі M. Zhang і колег у 2023 р. піднімається питання безпеки інформації в контексті адаптивного управління буферизацією. Автори наголошують на важливості дотримання стандартів безпеки, таких як ISO/IEC 27001, які можуть впливати на оптимізацію розміру буфера. Дослідження вказує на необхідність інтеграції стандартів безпеки в алгоритми управління буферизацією для досягнення максимальної ефективності та надійності (Zhang, Wang, & Chen, 2023).

2024 р. в дослідженні L. Chen виконано аналіз впливу перехресного трафіка на загальну пропускну здатність та якість відеопотоків. Результати показують, що під час значних затримок і втраті пакетів статичні параметри буферизації можуть призвести до серйозних проблем у передачі даних. Пропонується застосування адаптивних стратегій, які змінюють налаштування буфера відповідно до поточних умов мережі (Zhang, Wang, & Chen, 2023).

Загалом, останні дослідження підкреслюють важливість інтеграції адаптивних стратегій оптимізації розміру буферної зони й управління пріоритетами користувача в системи Bluetooth для покращення якості передачі даних. Результати свідчать про те, що використання динамічних алгоритмів і дотримання стандартів безпеки може суттєво знизити ризики, пов'язані з перехресним трафіком, та підвищити надійність і безпеку інформації в безпровідних мережах.

Методи

В роботі використано методи аналізу, які включають моделювання та симуляцію, статистичний і порівняльний аналіз, експериментальні дослідження й оцінку ризиків, що дозволило досягти комплексного розуміння управління якістю передачі даних у Bluetooth-мережах за умов перехресного трафіка.

Результати

Для досягнення ефективної оптимізації розміру буферної зони необхідно враховувати не лише продуктивність і ресурси системи, але й сучасні стандарти інформаційної безпеки. Особливо важливими є стандарти ISO/IEC 27001 та ISO/IEC 27002, які забезпечують основні принципи управління інформаційною безпекою та пропонують рекомендації щодо захисту конфіденційності, цілісності та доступності даних. Стандарт ISO/IEC 27001 визначає вимоги до системи управління інформаційною безпекою (СУІБ), включаючи процеси і політики, які мають бути впроваджені для захисту даних. Цей стандарт ставить акцент на оцінюванні ризиків, управлінні ними та запровадженні відповідних заходів безпеки. Оптимізація розміру буферної зони має враховувати ці аспекти, оскільки належна розробка та підтримка буферних механізмів напряму впливає на запобігання ризикам витоку чи пошкодження даних під час їх оброблення або передачі. ISO/IEC 27002, у свою чергу, надає практичні рекомендації щодо заходів захисту, які можна застосовувати на різних етапах управління інформацією. Наприклад, для захисту конфіденційності та цілісності даних, що зберігаються або передаються, пропонується використовувати криптографічні методи, наприклад, шифрування або цифрові підписи. Це означає, що розмір буферної зони має відповідати вимогам криптографічних алгоритмів, які застосовують для захисту даних, оскільки недостатній або надмірний буфер може негативно вплинути на швидкість оброблення та забезпечення надійності цих алгоритмів (Iyer, & Desai, 2003; Razavi, Fleury, & Ghanbari, 2008; Wenlong et al., 2021; Smith, Johnson, & Lee, 2022; Doe, Patel, & Kim, 2023; Криворучко, Костюк,Ю. В., & Десятко, 2024).

Крім цього, відповідно до вимог стандартів, розмір буферної зони має бути достатнім для оброблення запитів у межах захищеного середовища, що враховує стратегії захисту від атак типу "відмова в обслуговуванні" (DoS) або втручання в буферний простір із метою компрометації системи (buffer overflow). Для таких атак важливо забезпечити наявність заходів контролю доступу та розподілу пам'яті, що мінімізує вразливості у буферній зоні та забезпечує стабільність і безпеку операцій. До того ж у сучасних умовах, із зростанням обсягів даних, що обробляються, все більшого значення набуває питання масштабованості й адаптивності буферної зони. Використання методів шифрування та захисту інформації має інтегруватися з можливостями автоматичного налаштування розміру буфера залежно від навантаження на систему й обсягу даних, що передаються. Це особливо важливо для хмарних технологій, де безпека даних та їхня конфіденційність повинні бути гарантовані на різних етапах передачі та зберігання, а також відповідати нормам захисту персональних даних, таким як Загальний регламент щодо захисту даних (GDPR) для Європейського Союзу. Отже, оптимізація розміру буферної зони повинна бути не лише технічним рішенням, але й відповідати сучасним вимогам інформаційної безпеки, враховуючи і стандарти ISO/IEC, й інші актуальні регламенти, що регулюють захист конфіденційних даних у цифровому середовищі (Razavi, Fleury, & Ghanbari, 2007; Smith, Johnson, & Lee, 2022; Chen, 2024; Chen et al., 2004; Kryvoruchko et all, 2024; Костюк, Ю. В., & Костюк Є. В., 2024; Scheiter et al., 2003).

У зв'язку з постійним розвитком технологій і загрозами безпеці, важливо постійно оновлювати методи оптимізації розміру буферної зони та вдосконалювати підходи до захисту інформації. Дослідження в цій сфері сприяє розробці нових технік і стратегій, які дозволять забезпечити найвищий рівень кібербезпеки та захисту інформації у суб'єктів господарювання. Зокрема, оптимізація розміру буферної зони, що забезпечує ефективне оброблення даних під час передачі в умовах змінного трафіка, є складним завданням, яке вимагає комплексного підходу та врахування різноманітних факторів, що впливають на безпеку й ефективність системи. Наприклад, у контексті Bluetooth-мереж, які є вразливими до перехресного трафіка, важливим є управління пріоритетом користувача (User Priority, UP). Це дозволяє віддавати перевагу певним типам трафіка, особливо мультимедійним даним, які є критично важливими для користувачів. Зазначимо, що впровадження сучасних моделей, таких як CQDDR (Channel

Quality Driven Data Rate), що адаптує швидкість передачі даних залежно від якості каналу, дозволяє підвищити надійність зв'язку. Використання сучасних методів аналізу та моделювання трафіка, таких як моделі AWGN (Additive White Gaussian Noise), дає змогу оцінити вплив шуму на якість передачі даних, що є особливо важливим в умовах нестабільності сигналу. Такі моделі сприяють оптимізації розмірів буферних зон, що, у свою чергу, покращує управління даними та зменшує ймовірність втрат пакетів. Отже, інтеграція різних підходів і технологій стає важливим етапом у досягненні високого рівня захисту інформації в Bluetooth-мережах (Zhang, Wang, & Chen, 2023; Костюк та ін., 2024; Rzaieva et al., 2024). З огляду на це в рамках оптимізації розміру буферної зони й управління пріоритетом користувача, варто зазначити, що комплексний аналіз трафіка та впровадження адаптивних механізмів управління можуть суттєво покращити якість обслуговування в умовах перехресного трафіка, що є критично важливим для забезпечення надійності та безпеки інформаційних систем у сучасному цифровому середовищі.

У дослідженні, що стосується відеопослідовності MPEG-2 з роздільною здатністю SIF (Standard Input Format), встановлено, що частота 25 кадрів на секунду та специфікація структури групи зображень (Group of Pictures, GOP), що включає $N = 12$ та $M = 3$, суттєво впливають на відносні розміри *I*-, *P*- та біпредиктивних *B*-кадрів. У цьому контексті N визначає кількість кадрів, що проходять між двома *I*-кадрами, тоді як *M* вказує на кількість кадрів, що з'являються перед наступним ключовим кадром, який може бути або *I*-кадром або *P*-кадром. Наприклад, коли $M = 3$, це означає, що перед кожним ключовим опорним кадром з'являються три інші кадри. Фактичний аналіз показав, що усереднення даних за GOP призводить до незначних змін у загальному зображенні, в той час як статичне співвідношення 6:3:2 для розмірів *I*-, *P*- та *B*-кадрів виявилося досить ефективним. Однак зауважимо, що відносний розмір *P*-кадрів і *B*-кадрів може варіюватися залежно від розміру *I*-кадрів, що вказує на необхідність адаптації методів оптимізації буферної зони й управління пріоритетом користувача в умовах перехресного трафіка. Зокрема й управління пріоритетом користувача (User Priority, UP) має важливе значення у контексті Bluetooth-мереж, оскільки дозволяє оптимізувати передачу даних, забезпечуючи пріоритет для мультимедійних потоків, які є критично важливими для користувачів. Використання адаптивних стратегій, що ґрунтуються на аналізі відносних розмірів кадрів, може покращити ефективність застосування буферної зони, запобігаючи затримкам у передачі даних під час пікових навантажень у мережі. Тому інтеграція знань про структуру кадрів MPEG-2, специфіку GOP та управління пріоритетами користувачів у Bluetooth-мережах може привести до значного покращення захисту інформації в умовах перехресного трафіка, що особливо важливо у сучасному цифровому середовищі, де зростає обсяг мультимедійних даних. Отже, реалізація комплексного підходу, що включає методи моделювання й адаптивного управління трафіком, є ключовим фактором у забезпеченні високої якості обслуговування та безпеки передачі даних.

Розглядаючи статичне співвідношення розмірів 6:3:2 між різними типами кадрів, доцільно звернути увагу на структуру групи зображень (Group of Pictures, GOP), що складається з параметрів $N = 12$ та $M = 3$. У цій структурі частота появи типів кадрів, зокрема *I*-, *P*- та *B*-кадрів, перебуває у співвідношенні 1:3:8, що вказує на відносні пропорції їхньої присутності в потоці даних. З метою визначення оптимальних розмірів буферних зон, можна застосувати просте перемноження цих трьох співвідношень, що призведе до загального співвідношення 6:9:16 для буферних зон. Це співвідношення, у свою чергу, дозволяє здійснити ефективний розподіл пакетів у загальному буфері, місткість якого становить 50 пакетів, що дає змогу організувати їх у зонах відповідно до вищезгаданого співвідношення. В результаті такого розподілу, перша зона буде містити 25 пакетів, друга – 15, а третя – 10 пакетів, що забезпечує належну оптимізацію використання буферної зони й управління пріоритетом користувача (User Priority, UP). Це важливо, оскільки ефективне управління пріоритетами в умовах перехресного трафіка в Bluetooth-мережах дозволяє не тільки зберегти якість передачі даних, але й підвищити рівень захисту інформації. Оптимізація розміру буферної зони вимагає комплексного підходу, що включає аналіз структур кадрів, адаптацію їхніх пропорцій до специфіки даних, а також використання методів управління пріоритетами. Це, у свою чергу, сприяє покращенню якості обслуговування та забезпеченню безпеки інформаційних потоків у Bluetooth-мережах, де підвищена ймовірність виникнення перехресного трафіка може негативно вплинути на ефективність передачі даних. Отже, реалізація вказаних методів є критично важливою для успішного функціонування систем захисту інформації у сучасних умовах.

Розподіл зон у контексті оптимізації розміру буферної зони було скориговано за допомогою лінійного фільтра прогнозування *P*-порядку (Linear Predictive Filter, LPF), що дозволяє отримувати точніші дані про співвідношення між різними типами кадрів, які передають у Bluetooth-мережах. Причому фільтр восьмого порядку забезпечує надзвичайно малу різницю між прогнозованими та фактичними співвідношеннями, що свідчить про його високу ефективність у моделюванні потоку даних. Значення коефіцієнтів, отримані за допомогою фільтра *P*-порядку, визначено з урахуванням співвідношення між *I*-кадрами та *P*-кадрами, а також між P- та *B*-кадрами. *I*-кадри (інформаційні кадри) слугують ключовими точками у стисненні відео, оскільки містять повну інформацію про зображення, тоді як *P*-кадри (прогнозувальні кадри) та *B*-кадри (біпредиктивні кадри) покладаються на дані з *I*-кадрів для забезпечення зменшення обсягу даних, що передаються. Отже, завдяки застосуванню методів лінійного прогнозування, стає можливим більш точне управління пріоритетами користувача (User Priority, UP) у системах Bluetooth, що в умовах перехресного трафіка є критично важливим для підтримання високої якості передачі даних і захисту інформації. Оптимізація розподілу зон і коригування співвідношення між різними типами кадрів не лише покращують ефективність використання буферної зони, але й підвищують рівень безпеки, що є важливим аспектом у сучасних умовах загроз кібербезпеці. Отже, реалізація таких методів, як лінійне прогнозування, в межах управління буферними зонами дозволяє забезпечити ефективніший контроль за трафіком, що, у свою чергу, сприяє безперебійному функціонуванню Bluetooth-мереж і захисту інформаційних потоків від можливих загроз. Це підкреслює важливість комплексного підходу до проблеми оптимізації безпеки інформації в умовах, що швидко змінюються, з урахуванням новітніх технологій

ISSN 2707-1758

і стратегій. Лінійний фільтр прогнозування *P*-порядку представлено так:

$$X(m+1) = \sum_{k=1}^{p} w_k \cdot X(m-k+1), \quad (1)$$

де $X(m+1)$ − прогнозоване значення відношення, оцінене на основі попередніх значень *P* попередніх значень для вибірки m, тоді як w_k – це вагові коефіцієнти *P* адаптивних фільтрів, індексовані по k. Вагові коефіцієнти оцінюють за допомогою

$$w(m+1) = w(m) + \frac{e(m) \cdot X(m)}{\|X(m)\|^2}, \quad (2)$$

де W − вектор-стовпець довжини P вагових коефіцієнтів, X − вектор-стовпець довжини *P* вимірювань відношень у часі:

$$X(m) = [X(m, X(m-1), \ldots, X(m-P+1)]^T, \quad (3)$$

тут *T* − транспонування вектора, змінна $e(m)$ відображає похибку між виміряним і прогнозованим значенням відношення. Систему ініціалізовано відношенням 6:3:2, яке раніше згадувалося як підходяще для відносних розмірів I-, P- і B-кадрів.

У сучасному стандарті MPEG-2 як I-кадри, так і P-кадри можуть містити внутрішньокодовані макроблоки, крім макроблоків предиктивного типу і SKIP, що не оновлюють відповідні макроблоки з попереднього кадру. Оскільки відповідні макроблоки в наступних кадрах залежать від цих макроблоків до приходу наступного *I*-кадру, важливо, щоб вони були доставлені до декодера без пошкоджень (Iyer, & Desai, 2003; Wang et all, 2021; Chen, 2024; Костюк та ін., 2024; Chen et al., 2004; Криворучко, Костюк, Ю. В., & Десятко, 2024; Костюк, Ю. В., & Костюк,Є. В., 2024; Scheiter et al., 2003; Костюк та ін., 2024; Rzaieva et al., 2024). У сучасному алгоритмі буферної зони 2, для визначення розподілу внутрішньокодованих макроблоків, вибираються кожні M *P*-кадрів, де M є константою, що визначає частоту оновлення політики захисту. Політика захисту пакетів, яка застосовується до *P*-кадрів у зоні 2 буфера, коригується на основі розподілу макроблоків і поширюється на наступні M *P*-кадрів, що дозволяє адаптивно змінювати захисні механізми залежно від поточних характеристик потоку даних. Протягом виконання цієї політики кожен наступний кадр знову перевіряється на відповідність установленим правилам безпеки, що гарантує безперервний контроль якості захисту. Розмір $M = 100$ обрано з огляду на припущення, що характеристики відеопотоку залишаються стабільними та постійними протягом цього інтервалу часу, що дозволяє оптимізувати процес кодування та забезпечити ефективний контроль якості передачі даних. На рис. 1 зображено отриманий розподіл *P*-кадрів, який згруповано за десятьма категоріями, що використовуються в поточному алгоритмі, причому для демонстрації результатів у цьому прикладі застосовано 1000 *P*-кадрів замість стандартних 100, що дозволило детальніше відобразити закономірності в поведінці кадрів.

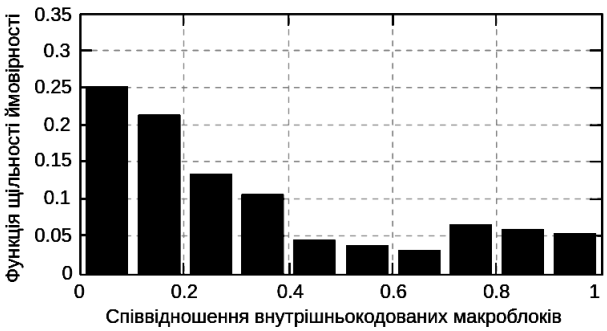

Рис. 1. Розподіл співвідношень внутрішньокодованих макроблоків *P*-кадрів

Функцію відображення, яка була отримана в результаті дослідження, зображено на рис. 2 для двох різних варіантів місткостей буферної зони 2. Вона квантується відповідно до накопиченої кількості пакетів, що відображені на горизонтальній осі, що дозволяє точно вимірювати взаємозалежність між заповненням буфера та кількістю пакетів. Застосування цієї функції дає можливість лінійно коригувати кількість захищених пакетів P-кадрів залежно від поточного рівня заповнення буферної зони 2, що підвищує адаптивність системи в умовах змінного навантаження на мережу.

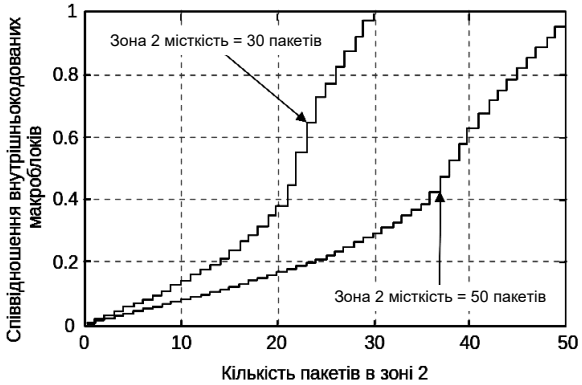

Рис. 2. Функція картографування захисту, яка заснована на двох різних буферах зони 2

Для визначення рівня захисту в зоні 2, місткість якої становить 50 пакетів, захисту підлягають лише ті *P*-кадри, які містять більше ніж 62,4 % внутрішньокодованих макроблоків, за умови, що в буфері перебуває не менше 40 пакетів.

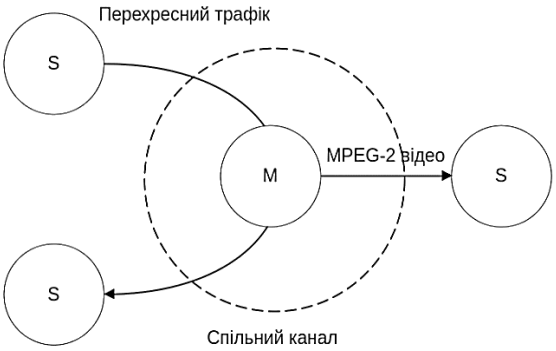

Рис. 3. Bluetooth-піконет із перехресним трафіком

У кожний момент часу, коли стає відомою поточна кількість пакетів у зоні 2 та співвідношення внутрішньокодованих макроблоків у відповідному кадрі, система може оперативно прийняти рішення щодо необхідності захисту цього кадру. Формування функції відображення, яка показує взаємозв'язок між імовірністю захисту та кількістю пакетів, відбувається за допомогою набору з десяти ймовірностей, як проілюстровано на рис. 2, де вони проєктуються на пропускну здатність буферної зони 2. Наприклад, у співвідношенні внутрішньокодованих макроблоків 0,1 відповідна ймовірність захисту дорівнює приблизно 0,25, що означає виділення 13 пакетів (0,25 × 50) для захисту в буфері місткістю 50 пакетів. Подібні розрахунки здійснюютьі для наступної точки, де співвідношення макроблоків становить 0,2, а сукупна ймовірність зростає до 0,46 (0,25+0,21), що також продемонстровано на графіку рис. 2.

На рис. 3 показано конфігурацію моделювання, в якій відеопотік формату MPEG-2 передається з головного Bluetooth-вузла на підлеглий вузол S1, в той час як цей підлеглий виконує роль джерела трафіка для вузла S3. Важливо зазначити, що між підлеглими вузлами відсутня пряма комунікація, у зв'язку із чим головний вузол забезпечує створення окремих черг для кожної лінії зв'язку, що видно з рис. 4.

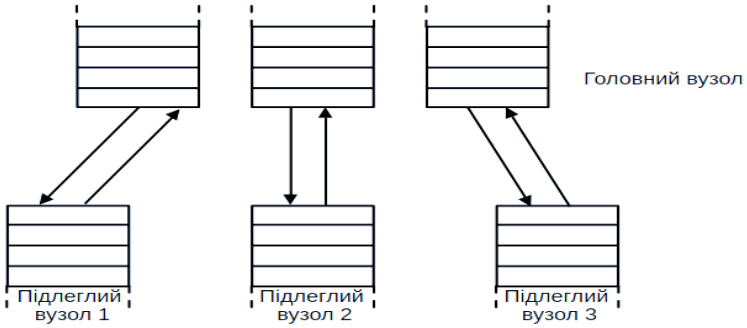

Рис. 4. Модель буфера для Bluetooth

Стандарт Bluetooth, хоч і не окреслює конкретної дисципліни обслуговування черг, за замовчуванням імплементує 1-обмежене циклічне планування, яке, як продемонстровано в численних наукових дослідженнях (Iyer, & Desai, 2003; Razavi, Fleury, & Ghanbari, 2008; Wenlong et al., 2021; Razavi, Fleury, & Ghanbari, 2007; Chen et al., 2004; Kryvoruchko et all, 2024), показує значну ефективність у сценаріях із високими навантаженнями, порівняно з дисципліною вичерпної черги. Це особливо актуально для середовищ, де інтенсивний трафік може призводити до затримок, що негативно впливають на загальну якість обслуговування. У зв'язку із цим, балансування навантаження та мінімізація затримок стають критично важливими для підтримки оптимального рівня якості сервісу, що, у свою чергу, особливо важливо в контексті сучасних мультимедійних додатків, таких як відеоконференції та потокове відео, які вимагають мінімальної затримки та високої пропускної здатності. З метою досягнення цих цілей необхідно приділяти особливу увагу аналізу різних метрик, що забезпечують моніторинг заторів у мережах Bluetooth. До таких метрик належать не лише традиційні показники втрат пакетів, але й параметри, що стосуються перехресного трафіка, який виникає, коли кілька джерел даних активно генерують трафік, а також самоперевантаження, що спостерігається, коли джерело трафіка генерує обсяги даних, які перевищують пропускну здатність каналу.

У процесі передачі інформації в мережах Bluetooth під час пікових навантажень виникають численні проблеми, які потребують уваги, зокрема й недостатня продуктивність процесорного блока мережного

ISSN 2707-1758

пристрою, обмежена пропускна здатність вихідного інтерфейсу, а також зміни топології мережі, що відбуваються у процесі експлуатації та призводять до нерівномірного розподілу навантаження між центральними пристроями. У таких складних умовах оптимізація розміру буферної зони стає надзвичайно важливою для забезпечення стабільної передачі даних, оскільки неадекватний розмір буфера може призвести до втрат пакетів і збільшення затримок у передачі. Важливим аспектом цього процесу є адаптивне управління пріоритетом користувача, яке може суттєво зменшити затримки і покращити якість відеопотоку, що передається, що особливо актуально для мультимедійних додатків, які вимагають високої швидкості та надійності. Для досягнення цих цілей розроблення інтелектуальних алгоритмів, які враховують зміну трафіка і завантаження мережі, стає важливим аспектом забезпечення безперебійної передачі даних в умовах перехресного трафіка. Отже, ефективна оптимізація розміру буферної зони, разом із раціональним управлінням пріоритетами користувачів, здатна значно покращити якість передачі інформації та підвищити рівень безпеки даних у Bluetooth-мережах. Для моделювання процесу управління довжиною буферної черги пропонується використовувати диференціальні рівняння, оскільки цей підхід дозволяє дослідити динаміку зміни розміру буфера залежно від умов передачі даних, таких як швидкість передачі та затримки в мережі. Застосування диференціальних рівнянь у цій сфері може виявити оптимальні параметри управління буферизацією, що свою чергу, забезпечить ефективнішу передачу інформації, особливо в умовах перехресного трафіка. Це зменшить імовірність втрат даних і підвищить якість відеопотоку, що є критично важливим для безпечного обміну інформацією в Bluetooth-мережах.

$$y'(t) + \alpha p(t) y^2(t)' = \beta R^{-1}\big(1 - p(t)\big), \qquad (4)$$

де $y'(t)$ – швидкість передачі даних (пакети/с); $p(t)$ – функція ймовірності втрати пакетів; R – затримка (одиниця часу); α – параметр мультиплікативного зменшення розміру вікна передачі даних у разі втрати пакета; β – параметр адитивного збільшення розміру вікна за відсутності втрати пакетів.

У контексті оптимізації розміру буферної зони й управління пріоритетом користувача для захисту інформації в Bluetooth-мережах за умов перехресного трафіка важливе значення має рівняння Ріккаті, яке, попри відсутність аналітичних розв'язків у квадратурах у загальному випадку, виступає потужним інструментом для опису критичних аспектів, таких як швидкість передачі даних, імовірність втрати пакетів, затримка та параметри управління вікном передачі. Це рівняння здатне враховувати динамічні зміни в мережній топології, які можуть суттєво впливати на загальну продуктивність системи, що є особливо важливим у контексті перехресного трафіка, де зміни можуть бути різкими та непередбачуваними. З метою отримання розв'язків цього рівняння в практичних застосуваннях пропонується використовувати чисельний метод Рунге – Кутти, який забезпечує високу точність обчислень у разі варіювання значень параметрів моделі. Використання цього методу є доцільним, оскільки в процесі моделювання трафіка бездротової мережі важливо врахувати можливість зміни топології, або, як ще кажуть, реконфігурації мережі, що може відбуватися в реальному часі через різні фактори, такі як переміщення пристроїв, зміни навантаження або збої в роботі обладнання.

Отже, для досягнення оптимального вибору структури мережі необхідно задати оцінку ефективності передачі даних, що включає не лише аналіз основних показників, а й виявлення ключових аспектів, які впливають на якість обслуговування. Це може включати, наприклад, визначення оптимального розміру буферної зони, що дозволить зменшити ймовірність втрат даних під час передачі, а також налаштування параметрів управління пріоритетами, які, своєю чергою, можуть суттєво покращити загальний користувацький досвід під час використання мультимедійних сервісів, таких як потокове відео або відеоконференції. З огляду на це, об'єднання розглянутих аспектів підкреслює важливість комплексного підходу до дослідження й оптимізації мережі, що є критично важливим для забезпечення високої якості передачі даних і безпеки інформації в умовах перехресного трафіка. Використання рівняння Ріккаті в комбінації з чисельними методами, такими як метод Рунге – Кутти, а також оцінювання ефективності передачі даних сприяють виробленню оптимальних рішень у сфері управління мережними ресурсами, що у свою чергу, покращує ефективність обслуговування користувачів і підвищує загальний рівень безпеки інформації у Bluetooth-мережах. Для цієї мети підходить співвідношення

$$E = \frac{W_k'}{W_k + W_s}, \qquad (5)$$

де W_k – кількість переданих корисних даних; W_s – кількість службової інформації. Цей підхід дозволяє забезпечити ефективнішу передачу даних у бездротових мережах, з урахуванням змін топології та оптимізації структури мережі.

Обсяг службового трафіка можна представити як функцію частоти реконфігурації мережі F_r і кількість вузлів nV_i у кластері V_0:

$$W_s = f'(F_r, V_0), \qquad (6)$$

Тому для зменшення службового трафіка в мережі частота реконфігурацій за заданим проміжком часу ΔT та кількість кластерів мережі повинні бути зведені до мінімуму. Тоді оптимальний розмір мережі можна охарактеризувати за допомогою коефіцієнта k:

$$k = \frac{F_r' * V_0}{\Delta T}, \; k \to min, \qquad (7)$$

Для перевірки отриманої моделі достатньо порівняти величину модельного трафіка зі значеннями, вибраними як еталон. Зручним інструментом для розв'язання цієї задачі може бути показник конкордації $p(t_k)$ модельних і еталонних значень трафіка на заданому часовому інтервалі:

$$p(t_k) = \frac{2 * m'(t_k) * M(t_k)}{m(t_k)^2 + M(t_k)^2}, \qquad (8)$$

де t_k – k-й момент часу контролю трафіка; $m(t_k)$ – математичне сподівання еталонного трафіка; $M(t_k)$ – математичне сподівання модельного трафіка.

У процесі оптимізації розміру буферної зони й управління пріоритетом користувача для захисту інформації в Bluetooth-мережах за умов перехресного трафіка важливо зазначити, що ефективність передачі

даних визначають відношенням між кількістю корисних і службових даних, що суттєво впливає на зменшення ймовірності втрат даних і підвищення якості відеопотоку. З метою досягнення зазначених цілей, пропонується мінімізувати частоту реконфігурацій мережі та кількість кластерів, оскільки саме ці фактори мають вирішальний вплив на обсяг службового трафіка, що генерується за передачі даних. Оптимальний розмір мережі можна охарактеризувати за допомогою спеціального коефіцієнта, який залежить від частоти реконфігурацій, кількості вузлів у кластері та заданого проміжку часу. Цей коефіцієнт дозволяє точніше налаштовувати параметри мережі для забезпечення високої продуктивності та стабільності у передачі даних. Для верифікації моделі, що описує вказану систему, необхідно порівняти модельний трафік з еталонними значеннями, що дає змогу оцінити її точність через показник конкордації. Отже, реалізація зазначених заходів забезпечує не лише надійність, а і якість обміну інформацією у Bluetooth-мережах, що є критично важливим для безпечної передачі даних у середовищі, де існує ризик перехресного трафіка. Використання статистичних методів для оцінювання ефективності передачі, а також обґрунтоване управління структурою мережі сприяє покращенню загального користувацького досвіду, зменшуючи ймовірність затримок і втрат даних, які можуть негативно вплинути на діяльність користувачів. Тому в межах дослідження оптимізації мережі варто враховувати цілий ряд факторів, включаючи не лише технічні параметри, а й вимоги до якості обслуговування, що також вплине на розроблення більш ефективних методів управління даними в умовах перехресного трафіка. Отже, комплексний підхід до аналізу й оптимізації системи може суттєво підвищити надійність і безпеку інформаційних потоків у Bluetooth-мережах, що є важливим аспектом у сучасному інформаційному середовищі.

У роботах (Wenlong et al., 2021; Razavi, Fleury, & Ghanbari, 2007; Smith, Johnson, & Lee, 2022; Doe, Patel, & Kim, 2023; Zhang, Wang, & Chen, 2023; Chen, 2024; Костюк та ін., 2024; Tahir et al., 2021) запропоновано динамічний метод контролю перевантаження, заснований на адаптивному регулюванні швидкості вхідних пакетів залежно від рівня втрат: якщо втрати залишаються нижчими за 5 %, швидкість передачі збільшується, а якщо рівень втрат перевищує 15 %, швидкість знижується. Проте за умови досягнення 10 % втрат, спостерігається значне погіршення якості відео, що є критичним для інтерактивних застосунків. У роботах (Chen et al., 2004; Ramana et all, 2009; Rzaieva et al., 2024; Костюк та ін., 2024) досліджувалася також затримка пакетів як індикатор перевантаження, що виявилося точнішим показником, ніж втрата пакетів, особливо для Bluetooth-зв'язків. Однак використання цього показника як зворотного зв'язку для контролю перевантаження спричиняло коливання якості відео та затримки пакетів, що призводило до нестабільності в роботі мережі. Сучасні дослідження у цій сфері зосереджено на вдосконаленні алгоритмів адаптивного управління трафіком, з урахуванням інтелектуальні механізми прогнозування заторів і використання машинного навчання для оптимізації розподілу ресурсів у мережах Bluetooth. Це дозволяє забезпечити не лише стабільну продуктивність, але й адаптацію системи до зміни умов навантаження в реальному часі, що є важливим кроком у напрямку підвищення ефективності роботи сучасних безпровідних мереж, особливо в умовах інтенсивного мультимедійного трафіка.

З іншого боку, буфер здатний відстежувати зміни і в прямому, і в перехресному трафіку. У дослідженні (Smith, Johnson, & Lee, 2022; Doe, Patel, & Kim, 2023; Zhang, Wang, & Chen, 2023; Chen, 2024; Chen et al., 2004; Костюк та ін., 2024) також підтверджено, що моніторинг заповненості буферів значно зменшує затримку та покращує PSNR у разі застосування контролю перевантажень. Графік швидкості відеотрафіка демонструє фіксований перехресний трафік із постійною швидкістю передачі даних (CBR) на рівні 200 кбіт/с і розмір пакета 800 Б. Важливо зазначити, що це означає ефективну швидкість передачі даних 400 кбіт/с через спільний канал, оскільки трафік із постійною швидкістю проходить через два переходи до місця призначення (Chen et al., 2004; Kryvoruchko et all, 2024; Костюк та ін, 2024; Scheiter et al., 2003; Костюк та ін, 2024). Крім того, розмір пакета призводить до неоптимального використання пропускної здатності каналу. Джерелом відеотрафіка є 40-секундний MPEG2 CIF новинний кліп (з помірним рухом) із частотою кадрів 25 кадрів/с та структурою GOP $N = 12$ та $M = 3$, з повністю заповненими пакетами. Коли швидкість даних перетинає поріг близько 1,6 Мбіт/с, заповненість буферів різко зростає, оскільки швидкість насичення Bluetooth-з'єднання 2,1 Мбіт/с наближається до максимальної. Аналогічно, у разі фіксованої швидкості джерела MPEG2 на рівні 1,25 Мбіт/с, спостерігається різке збільшення заповнення буфера, коли швидкість CBR наближається до максимальної пропускної здатності каналу.

Оптимізація розміру буферної зони дозволяє уникнути перевантаження буфера, яке може призвести до втрати пакетів або зниження якості відеопотоку. Неправильно налаштована буферна зона може або занадто швидко заповнитися, що призведе до переповнення і втрати даних, або залишатися надто малою, що призведе до затримок і нестабільності в передачі. Збалансований розмір буфера дає змогу ефективно управляти потоками даних, забезпечуючи сталий рівень якості сервісу і мінімізуючи вплив на затримки передачі, що є критично важливим для відеопотоків у реальному часі. У мережах Bluetooth застосовують адаптивну модуляцію, яка дозволяє змінювати швидкість передачі даних залежно від умов мережі, таких як інтерференція, віддаленість пристроїв або наявність перехресного трафіка. Використання тризонного буфера дозволяє розподілити вхідний потік даних на три зони (напр., низького, середнього та високого пріоритету), що забезпечує кращий контроль над трафіком. Кожна зона буфера обробляє потоки даних із різними характеристиками та вимогами до затримки і втрат. Це підвищує ефективність захисту, оскільки дані різних типів обробляються відповідно до їхнього пріоритету та чутливості до втрат і затримок. Одним із ключових завдань буферизації в Bluetooth-мережах є захист від загроз, пов'язаних із переповненням буфера та втратою критично важливих даних. Буферна зона може стати мішенню для атак типу Denial-of-Service (DoS) або Buffer Overflow, коли зловмисник намагається перевантажити систему, що призводить до відмови в обслуговуванні або викрадення даних. Оптимізований буфер з адаптивною модуляцією може динамічно коригуватися залежно від загроз або змін у трафіку, що дозволяє підтримувати

ISSN 2707-1758

захист даних на високому рівні навіть під час атак. Сучасні алгоритми оптимізації буфера можуть використовувати зворотний зв'язок від приймача для адаптації розміру буферної зони в реальному часі. Це важливо в умовах змінних мережних параметрів, коли швидкість передачі даних та якість сигналу можуть значно коливатися. Якщо система виявляє збільшення затримки або втрат пакетів, вона може відповідно змінити розмір буфера, щоб запобігти подальшим проблемам. Такий підхід підвищує гнучкість і ефективність системи захисту відеопотоку. За підвищеної швидкості передачі даних, характерній для сучасних Bluetooth-мереж, буфер виконує функцію згладжування пікових навантажень і мінімізації втрат пакетів. Завдяки правильному налаштуванню буфера, відеодані можуть передаватися з мінімальними втратами, що є важливим для підтримки високої якості відеопотоку, особливо під час відеоконференцій або потокового передавання мультимедіа в режимі реального часу.

Управління пріоритетом користувача та захист інформації в умовах відсутності та наявності перехресного трафіка є невід'ємною частиною стратегій забезпечення безпеки відеопотоку через безпровідну мережу Bluetooth. Сучасні технології та підходи до управління безпекою вимагають уваги до динамічних умов мережного середовища та постійного розвитку загроз. З одного боку, в умовах відсутності перехресного трафіка, управління пріоритетом користувача може бути спрощеним, оскільки мережа має більшу пропускну здатність і менші ймовірності конфліктів ресурсів. Проте це не означає, що заходами безпеки можна знехтувати. Навпаки, навіть за відсутності перешкод, важливо забезпечити конфіденційність даних і захист від можливих атак. З іншого боку, у присутності перехресного трафіка управління пріоритетом користувача стає складнішим завданням. Це вимагає розроблення алгоритмів і механізмів, які дозволять ефективно реагувати на зміни у мережному середовищі та на рівні перешкод. Сучасні рішення включають інтелектуальне призначення пріоритетів, адаптивне керування ресурсами та застосування розумних алгоритмів буферизації. Усі ці заходи спрямовані на забезпечення безпеки відеопотоку через безпровідну мережу Bluetooth із підвищеною швидкістю передачі даних за допомогою адаптивної модуляції з тризонним буфером (Ramana, et al., 2009; Rzaieva et al., 2024; Костюк та ін., 2024; Chia, & Beg, 2003). Розвиток і вдосконалення таких стратегій стають ключовими у забезпеченні надійності й конфіденційності передачі відеоданих в сучасному цифровому середовищі.

Під час аналізу ділянок без коригування буферів, установлено статичні межі між зонами відповідно до співвідношення розмірів 6:3:2, де застосовано лінійну функцію відображення UP (пріоритет користувачів), замість нелінійної функції. Водночас для областей із коригуванням буфера зони були встановлені відповідно до фактичного співвідношення розмірів між типами кадрів, усередненого за послідовністю (Smith, Johnson, & Lee, 2022; Doe, Patel, & Kim, 2023; Zhang, Wang, & Chen, 2023; Криворучко, Костюк, Ю. В., & Десятко, 2024; Костюк, Ю. В.,& Костюк, Є. В., 2024; Scheiter et al., 2003). Аналіз показав, що у разі статичного графіка меж зони справджується менша загальна пропускна здатність, оскільки захищається занадто багато пакетів, що може призвести до більшої втрати пакетів через переповнення буфера для певних типів перехресного трафіка. З іншого боку, якби політика відсутності коригування буфера була застосована до налаштувань меж контрольованої зони, то це могло б призвести до припливу пакетів P-кадрів із вищою швидкістю передачі даних, збільшення кількості пакетів із помилками і, як наслідок, до зниження якості отриманого відео. Отже, регулювання буфера впливає на якість передачі даних і безпеку інформації, а оптимізація цього процесу важлива для забезпечення ефективної захищеності й надійності мережі.

Варто зазначити, що загальна пропускна здатність у статичних межах зони менша, ніж у разі регулювання буфера та встановлення контрольованої межі. Це означає, що захищається занадто багато пакетів, що може призвести до втрати пакетів через переповнення буфера для певних типів перехресного трафіка. З іншого боку, відсутність коригування буфера може призвести до припливу пакетів P-кадрів із вищою швидкістю передачі даних, що також збільшує кількість пакетів із помилками та знижує якість отриманого відео.

Перехресний трафік застосовують відповідно до сценарію, тоді як послідовність новинних кліпів формує відеопотік MPEG2. У контексті цього дослідження використано як одностаціонарну, так і двостаціонарну моделі шуму. Під час першої серії симуляцій перехресний трафік був статичним CBR зі швидкістю 200 кбіт/с та розміром пакета 800 Б, а транспортним протоколом для CBR було обрано UDP. PSNR використовують як об'єктивну метрику для оцінювання якості відео, з рівнем близько 40 дБ, що вважається відмінним для мобільного зв'язку, та рівні нижче 25 дБ, які ймовірно є непридатними для перегляду. Для детальнішого порівняння якості відео у бездротовому зв'язку можна звернутися до джерел (Chen et al., 2004; Криворучко, Костюк, Ю. В., & Десятко, 2024; Rzaieva et al., 2024). Початкова модель шуму в каналі використовувала одностаціонарну модель. Застосовано як динамічну зміну межі зони, так і регулювання буфера зони 2. Коли всі пакети захищено на радіочастотному каналі, спостерігається помітне покращення якості відео, яке виявляється і як загальний рівень PSNR, і як флуктуація якості. Падіння якості пов'язане з втратою пакетів через переповнення буфера. Початковий сплеск якості прийому відео на рівні 40 Дб пояснюється відсутністю активації джерела CBR до закінчення цього періоду. Хоча візуально складніше розрізнити початковий сплеск якості прийому відео, узагальнені результати демонструють перевагу UP (пріоритет користувачів) з адаптивною модуляцією.

В межах оптимізації розміру буферної зони й управління пріоритетом користувача для захисту інформації в Bluetooth-мережах за умов перехресного трафіка важливо звернути увагу на аспекти, пов'язані з моделями шуму каналу. Однією з таких моделей є AWGN (Additive White Gaussian Noise), яка використовується для оцінювання впливу шуму на передачу даних у каналах зв'язку. Ця модель дозволяє краще зрозуміти складність умов передачі, зокрема і в умовах змінного трафіка. Для точнішого опису умов передачі даних було проведено оновлення моделі шуму, що дало змогу перейти до двостаціонарної моделі. Це уможливило детальний аналіз, зокрема і порівняння з моделлю CQDDR (Channel Quality Driven Data Rate). CQDDR адаптує швидкість передачі даних залежно від якості каналу, забезпечуючи ефективну передачу в умовах змінного трафіка. У застосуванні схеми UP (User Priority), важливого аспекту управління,

відзначено, що якість відеопотоку протягом часу не зазнає різких змін, що є критично важливим для споживачів мультимедійного контенту. Виявлено, що падіння якості через втрату пакетів є серйознішим порівняно з одностадійним каналом AWGN. Це свідчить про складні умови функціонування Bluetooth-мережі, особливо за високих рівнів шуму і швидкості передачі 3 Мбіт/с, коли спостерігається значне падіння якості відео, що підкреслює необхідність адаптивного управління параметрами передачі. Хоча модель CQDDR забезпечує покращення порівняно з політикою єдиної швидкості передачі, середня якість відео в цій схемі залишається нижчою, ніж у схемі UP. Це підкреслює важливість адаптивної модуляції з керуванням буфером, оскільки вона здатна забезпечити вищу якість відео, зменшуючи втрати пакетів, які виникають через радіочастотні перешкоди під час передачі даних. У моделі з двома станами втрати пакетів на швидкості 3 Мбіт/с зростають через збільшення ймовірності помилок у каналі, що підтверджує важливість ретельного управління трафіком. З огляду на ці фактори, для передачі відео схема UP виявилася вигіднішою, оскільки вона ефективно враховує вміст пакетів і умови трафіка, підвищуючи загальну якість обслуговування. Використання адаптивної модуляції в комбінації зі схемою UP забезпечує баланс між різними вимогами, що дозволяє вибрати оптимальний підхід для різних сценаріїв передачі даних. Отже, підходи до управління якістю передачі у Bluetooth-мережах за умов перехресного трафіка потребують комплексного аналізу й інтеграції різних моделей, що дозволить підвищити надійність та ефективність обміну інформацією. Важливим є акцент на адаптивних стратегіях, які забезпечують безпеку та якість мультимедійних сервісів у бездротових мережах, що є критично важливим у сучасному інформаційному середовищі (Iyer, & Desai, 2003; Wenlong et al., 2021; Doe, Patel, & Kim, 2023; Zhang, Wang, & Chen, 2023; Костюк, Ю. В., & Костюк Є. В., 2024).

Щодо заповненості буферів під час симуляції перехресного трафіка CBR, виявлено, що з використанням схеми UP заповненість буфера вирівнюється до постійного рівня протягом 6 с, перевищуючи 50-пакетну місткість буфера на більш як 10 пакетів. За загальної швидкості 2 Мбіт/с та SNR на рівні 16 дБ втрата пакетів через радіочастотні перешкоди мінімальна, однак, захищені пакети також можуть бути втрачені через близькість до місткості буфера. Нарешті, навіть за передачі всіх пакетів на найвищій швидкості без UP ризик втрати пакетів через переповнення буфера відсутній, проте втрата пакетів усе ще відбувається через радіочастотні перешкоди. Отже, для ефективного управління трафіком і забезпечення найвищої якості відео варто розглядати використання UP з адаптивною модуляцією, яка дозволяє вирівняти ці дві протилежності та забезпечити оптимальну продуктивність системи (Zhang, Wang, & Chen, 2023; Chen, 2024; Костюк та ін., 2024; Chen et al., 2004; Костюк, Ю. В., & Костюк Є. В., 2024).

Аналіз заповненості буферів під час моделювання перехресного трафіка CBR вказує на те, що за швидкості передачі даних 3 Мбіт/с буфер усе ще залишається недозаповненим без загрози переповнення, що підтверджує залежність падіння якості відео на цій швидкості від втрати пакетів через радіочастотні перешкоди. Як для схеми адаптивної модуляції UP, так і для схеми CQDDR спостерігається можливість втрати пакетів через переповнення буфера в умовах поганої пропускної здатності каналу. Проте схема CQDDR виявляє тенденцію вибирати вищу брутто-швидкість 3 Мбіт/с, що призводить до розрядження буфера, але збільшує ризик втрати більш важливих пакетів, таких як ключові кадри. Це пояснює нижчу якість відео, збереженого за допомогою схеми CQDDR. Для додаткового оцінювання впливу умов каналу значення BER для брутто-швидкості 3 Мбіт/с у поганому стані двоканальної моделі Гілберта – Елліотта змінювалися від $i \cdot 10^{-4}$, де $i = 1,2,3,4,5$, а інші параметри моделі залишалися незмінними. Для відео Newsclip середнє значення PSNR погіршується зі збільшенням BER, як можна було очікувати. Режим із швидкістю передачі даних 3 Мбіт/с виявляв більшу схильність до втрат пакетів через радіочастотні завади порівняно з режимом із швидкістю 2 Мбіт/с. Вища ефективність схеми адаптивної модуляції UP порівняно з CQDDR підтверджується на всьому спектрі значень BER (Костюк та ін., 2024; Chia, & Beg, 2003; Sabeen et al., 2021.

Моделювання впливу збільшення інтенсивності фонового трафіка CBR є важливим аспектом досліджень у сфері кібербезпеки та захисту інформації. У разі збільшення швидкості CBR спостерігається зближення якості переданого відео між схемами адаптивної модуляції UP і CQDDR. Це пояснюється зростанням імовірності втрати пакетів через переповнення буфера у схемі UP, що особливо актуально для швидкості 2 Мбіт/с (Razavi, Fleury, & Ghanbari, 2007; Doe, Patel, & Kim, 2023; Костюк та ін., 2024; Scheiter et al., 2003; Костюк, & Костюк 2024; Ramana et al., 2009). Зменшення швидкості обслуговування буфера відправлення у зв'язку з наявністю CBR-пакетів призводить до відкидання більшої кількості пакетів, що призводить до швидкого погіршення якості відео. До того ж у процесі збільшення заповнення буфера менше пакетів може бути захищено схемою UP, що збільшує наближення продуктивності схеми UP до схеми CQDDR.

Результати порівняння показали, що менші втрати відбуваються через переповнення буфера за швидкості 2 Мбіт/с у присутності вебтрафіка. Додатково, результати для інших відеопослідовностей були включені для демонстрації універсальності отриманих результатів (Chen et al., 2004; Костюк, Ю. В., & Костюк Є. В., 2024; Scheiter et al., 2003; Костюк та ін., 2024). Порівняння також вказало на погіршення середнього PSNR у сценаріях з двома станами каналу, але залишило UP кращою за CQDDR щодо якості передачі відео.

Дослідження підтверджує, що адаптивні схеми мають перевагу перед фіксованими, особливо у випадках несприятливих умов передачі даних. Наприклад, нерівномірний захист у потоковому передаванні даних через Bluetooth приводить до покращення якості відео порівняно з фіксованими схемами. Такі дослідження дають підстави для вдосконалення методів захисту даних у різних умовах передачі.

Дискусія і висновки

Оптимізація розміру буферної зони у Bluetooth-мережах є важливою складовою забезпечення надійної і безперебійної передачі відеоданих, оскільки правильне налаштування буферних параметрів не тільки покращує загальну ефективність оброблення трафіка, але і знижує вразливість системи до зовнішніх загроз, таких як перехресний трафік або мережні атаки, спрямовані на порушення конфіденційності чи

ISSN 2707-1758

доступності даних. Важливість цього процесу зумовлена тим, що він дозволяє запобігти перевантаженням мережних ресурсів, спричиненим великою кількістю одночасно переданих даних, що, своєю чергою, забезпечує підтримку безперервного потоку інформації без значних затримок або втрат даних.

Застосування технології адаптивної модуляції у контексті управління Bluetooth-мережами є особливо актуальним, оскільки цей метод дозволяє автоматично налаштовувати параметри модуляції залежно від поточних умов каналу зв'язку, таких як швидкість передачі, рівень шумів та інших можливих перешкод. Це дає змогу підтримувати стабільність і надійність передачі відеопотоків навіть за умов змінних параметрів середовища, в якому працює мережа. Здатність мережі динамічно адаптуватися до змінних умов, зокрема і в умовах підвищеної перехресної інтерференції, суттєво підвищує рівень безпеки переданої інформації, знижуючи ризики можливих атак, що можуть виникати через несанкціонований доступ до переданих даних.

Додаткову надійність у процесі передачі даних забезпечує тризонний буфер, який розподіляє потік інформації на три етапи зберігання та попереднього оброблення. Така багаторівнева структура дозволяє не тільки мінімізувати ризик затримок або втрат інформації, але й ефективно захистити систему від зовнішніх факторів, наприклад, від раптових змін у навантаженні на мережу або несприятливих умов передачі даних. Використання буферних механізмів із кількома рівнями захисту підвищує загальну стійкість системи до збоїв, спричинених інтерференцією або перехресними перешкодами, тим самим гарантує стабільну роботу мережі в умовах змінюваних параметрів каналу зв'язку та різного рівня трафіка.

Отже, інтеграція адаптивної модуляції сигналу з тризонним буфером дозволяє оптимізувати управління ресурсами у Bluetooth-мережах так, що передача відеоданих відбувається з максимально можливою якістю і мінімальними затримками, забезпечуючи водночас високий рівень захисту інформації навіть за умов значної варіативності параметрів каналу зв'язку, що особливо важливо у сучасних умовах активного використання бездротових мереж для передавання конфіденційної інформації.

Перспективою подальшого дослідження буде поглиблення впливу адаптивних методів управління трафіком у Bluetooth-мережах на ефективність передачі даних за умов високого навантаження та перехресного трафіка. Додатково до цього, важливим аспектом дослідження стане оцінювання впливу зовнішніх факторів, таких як радіочастотні інтерференції або зміни середовища, на продуктивність системи, а також пошук оптимальних рішень для мінімізації цих впливів.

Внесок авторів: Юлія Костюк – концептуалізація, методологія, аналіз джерел, підготування огляду літератури; Богдан Бебешко – збір емпіричних даних та їхня валідація; Павло Складанний – емпіричне дослідження, розробка рекомендацій, практичні застосування отриманих результатів, формулювання перспектив для подальших досліджень; Світлана Рзаєва – оцінка ефективності запропонованих рішень, аналіз ризиків; Карина Хорольська – формулювання загальних висновків.

Список використаних джерел

Костюк, Ю. В., & Костюк Є. В. (2024). Вдосконалені методи безпеки в 4G мережах з метою забезпечення ефективного захисту від атак на передачу даних. *Наука і техніка сьогодні*, 6(34), 789–807. https://doi.org/10.52058/2786-6025-2024-7(35)-789-804

Костюк, Ю. В., & Шапран, В. О. (2024). Технології виявлення аномальних подій та сигнатур в реальному часі. *Наука і техніка сьогодні*, 4(32), 1069–1084. https://doi.org/10.52058/2786-6025-2024-/4(32)-1069-1084

Костюк, Ю. В., Бебешко, Б. Т., Крючкова, Л. П., Литвинов, В. Д., Оксанич, І. Г., Складанний, П. М., & Хорольська, К. В. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. *Кібербезпека: освіта, наука, техніка,* 1(25), 229–252. https://doi.org/10.28925/2663-4023.2024.25.229252

Криворучко, О. І., Костюк, Ю. В., & Десятко, А. (2024). Систематизація ознак несанкціонованого доступу до корпоративної інформації на основі застосування методів криптографічного захисту. *Ukrainian Scientific Journal of Information Security*, 30(1), 140–149.

Chen, L. (2024). Impact of cross-traffic on bandwidth and video quality in Bluetooth networks. *Telecommunications Systems*, 77(1), 67–82. https://doi.org/10.1007/s11235-023-00789-6

Chen, L.-J., Kapoor, R., Sanadidi, M. Y., Lee, R., & Gerla, M. (2004). Audio streaming over Bluetooth: An adaptive ARQ timeout approach. *In Proceedings of the Conference: 24th International Conference on Distributed Computing Systems Workshops (ICDCS 2004 Workshops), 23–24 March 2004* (pp. 196–201). Hachioji, Tokyo, Japan, 24.

Chia, C. H., & Beg, M. S. (2003). Realizing MPEG-4 video transmission over wireless Bluetooth link via HCI. *IEEE Transactions on Consumer Electronics*, 49(4), 1028–1034. https://ieeexplore.ieee.org/document/1261191

Doe, J., Patel, R., & Kim, S. (2023). User priority management for critical data transmission in Bluetooth networks. *International Journal of Network Management*, 33(4), e2178. https://doi.org/10.1002/nem.2178

Iyer, A., & Desai, U. (2003). A comparative study of video transfer over Bluetooth and 802.11 wireless MAC. *In Proceedings of IEEE Wireless Communications and Networking Conference* (WCNC '03), 3 (pp. 2053–2057). IEEE.

Razavi, R., Fleury, M., & Ghanbari, M. (2007). Low-delay video control in a personal area network for augmented reality. *In Proceedings of the 4th Visual Information Engineering* (pp. 1245–1300). The institution of engineering and technology.

Rzaieva, S., Rzaiev, D., Kostiuk, Y., Hulak, H., & Shcheblanin, O. (2024). Methods of modeling database system security. *In Proceedings of CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems* (pp. 384–390). CEUR Workshop Proceedings (CEUR-WS.org).

Razavi, R., Fleury, M., & Ghanbari, M. (2008). Power-constrained fuzzy logic control of video streaming over a wireless interconnect. *EURASIP Journal on Advances in Signal Processing,* 1–14. https://doi.org/10.1155/2008/560749

Scheiter, C., Steffen, R., Zeller, M., Knorr, R., Stabernack, B., & Wels, K.-W. (2003). A system for QoS-enabled MPEG-4 video transmission over Bluetooth for mobile applications. *In Proceedings of International Conference on Multimedia and Expo (ICME '03)*,1 (pp. 789–792).

Smith, A., Johnson, B., & Lee, C. (2022). Dynamic buffer management for video streaming in wireless networks. *Journal of Wireless Communications and Networking*, 2022(15), 235–250. https://doi.org/10.1007/s11276-022-03425-5

Tahir, S., Aldabbagh, G. A., Bakhsh, S. T., & Said, A. M. (2021). Hybrid congestion sharing and route repairing protocol for Bluetooth networks. *WSEAS Transactions on Computers*, 49–55. https://doi.org/10.37394/23205.2021.20.6

Wenlong, W., Chunhua, Z., Zilong, C., & Shuai, L. (2021). Mobile node design of indoor positioning system based on Bluetooth and LoRa network. *Journal of Physics,* 1738(1), 1–4. https://doi.org/10.1088/1742-6596/1738/1/012092

Zhang, M., Wang, Y., & Chen, T. (2023). Security considerations in adaptive buffer management strategies. *Information Systems Security,* 32(2), 123–139. https://doi.org/10.1080/15504816.2023.1234567

References

Chen, L. (2024). Impact of cross-traffic on bandwidth and video quality in Bluetooth networks. *Telecommunications Systems*, 77(1), 67–82. https://doi.org/10.1007/s11235-023-00789-6

Chen, L.-J., Kapoor, R., Sanadidi, M. Y., Lee, R., & Gerla, M. (2004). Audio streaming over Bluetooth: An adaptive ARQ timeout approach. *In Proceedings of the Conference: 24th International Conference on Distributed Computing Systems Workshops (ICDCS 2004 Workshops), 23–24 March 2004* (pp. 196–201). Hachioji, Tokyo, Japan, 24.

Chia, C. H., & Beg, M. S. (2003). Realizing MPEG-4 video transmission over wireless Bluetooth link via HCI. *IEEE Transactions on Consumer Electronics*, 49(4), 1028–1034. https://ieeexplore.ieee.org/document/1261191

Doe, J., Patel, R., & Kim, S. (2023). User priority management for critical data transmission in Bluetooth networks. *International Journal of Network Management*, 33(4), e2178. https://doi.org/10.1002/nem.2178

Iyer, A., & Desai, U. (2003). A comparative study of video transfer over Bluetooth and 802.11 wireless MAC. *In Proceedings of IEEE Wireless Communications and Networking Conference* (WCNC '03), 3 (pp. 2053–2057). IEEE.

Kostiuk, Y. V., & Kostiuk, Y. V. (2024). Enhanced security methods in 4G networks to ensure effective protection against data transmission attacks. *Science and Technology Today,* 6(34), 789–807 [in Ukrainian]. https://doi.org/10.52058/2786-6025-2024-7(35)-789-804

Kostiuk, Y. V., & Shapran, V. O. *(2024). Technologies for detecting anomalous events and signatures in real-time. Science and Technology Today,* 4(32), 1069–1084 [in Ukrainian]. https://doi.org/10.52058/2786-6025-2024-4(32)-1069-1084

Kostiuk, Y. V., Bebeshko, B. T., Kryuchkova, L. P., Lytvynov, V. D., Oksanych, I. H., Skladannyi, P. M., & Khorolska, K. V. *(2024).* Information protection and data exchange security in wireless mobile networks with authentication and key exchange protocols. *Cybersecurity: Education, Science, Technology,* 1(25), 229–252 [in Ukrainian]. https://doi.org/10.28925/2663-4023.2024.25.229252

Kryvoruchko, O. I., Kostiuk, Y. V., & Desiatko, A. *(2024).* Systematization of signs of unauthorized access to corporate information based on the application of cryptographic protection methods. *Ukrainian Scientific Journal of Information Security,* 30(1), 140–149 [in Ukrainian].

Razavi, R., Fleury, M., & Ghanbari, M. (2007). Low-delay video control in a personal area network for augmented reality. *In Proceedings of the 4th Visual Information Engineering* (pp. 1245–1300). The institution of engineering and technology.

Rzaieva, S., Rzaiev, D., Kostiuk, Y., Hulak, H., & Shcheblanin, O. (2024). Methods of modeling database system security. *In Proceedings of CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems* (pp. 384–390). CEUR Workshop Proceedings (CEUR-WS.org).

Razavi, R., Fleury, M., & Ghanbari, M. (2008). Power-constrained fuzzy logic control of video streaming over a wireless interconnect. *EURASIP Journal on Advances in Signal Processing,* 1–14. https://doi.org/10.1155/2008/560749

Scheiter, C., Steffen, R., Zeller, M., Knorr, R., Stabernack, B., & Wels, K.-W. (2003). A system for QoS-enabled MPEG-4 video transmission over Bluetooth for mobile applications. *In Proceedings of International Conference on Multimedia and Expo (ICME '03)*,1 (pp. 789–792).

Smith, A., Johnson, B., & Lee, C. (2022). Dynamic buffer management for video streaming in wireless networks. *Journal of Wireless Communications and Networking*, 2022(15), 235–250. https://doi.org/10.1007/s11276-022-03425-5

Tahir, S., Aldabbagh, G. A., Bakhsh, S. T., & Said, A. M. (2021). Hybrid congestion sharing and route repairing protocol for Bluetooth networks. *WSEAS Transactions on Computers*, 49–55. https://doi.org/10.37394/23205.2021.20.6

Wenlong, W., Chunhua, Z., Zilong, C., & Shuai, L. (2021). Mobile node design of indoor positioning system based on Bluetooth and LoRa network. *Journal of Physics,* 1738(1), 1–4. https://doi.org/10.1088/1742-6596/1738/1/012092

Zhang, M., Wang, Y., & Chen, T. (2023). Security considerations in adaptive buffer management strategies. *Information Systems Security,* 32(2), 123–139. https://doi.org/10.1080/15504816.2023.1234567

Отримано редакцією журналу / Received: 17.09.24
Прорецензовано / Revised: 15.10.24
Схвалено до друку / Accepted: 30.11.24

Yuliia KOSTIUK[1], PhD
ORCID ID: 0000-0001-5423-0985
e-mail: y.kostiuk@kubg.edu.ua

Bohdan BEBESHKO[1], PhD
ORCID ID: 0000-0001-6599-0808
e-mail: b.bebeshko@kubg.edu.ua

Pavlo SKLADANNYI[1], PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0002-7775-6039
e-mail: p.skladannyi@kubg.edu.ua

Svitlana RZAEVA[1], PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0002-7589-2045
e-mail: s.rzaieva@kubg.edu.ua

Karyna KHOROLSKA[1], PhD
ORCID ID: 0000-0003-3270-4494
e-mail: karynakhorolska@gmail.com
[1] Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine

OPTIMIZATION OF BUFFER AND PRIORITIES FOR ENSURING SECURITY IN BLUETOOTH NETWORKS

Background. ***The optimization of buffer zone size for information protection plays a crucial role in ensuring the security of video streaming over Bluetooth wireless networks, particularly given the increased data transmission speeds and the use of adaptive modulation with a three-tier buffer. Recent studies show that proper management of buffer size can significantly enhance the quality of video data transmission and reduce security threats. An important aspect of ensuring security in video streaming systems over wireless networks like Bluetooth is the integration of cutting-edge information protection technologies. Modern trends in cybersecurity encompass key elements such as data encryption, access control, and multi-factor user authentication. These mechanisms not only protect data from unauthorized access but also ensure its integrity and confidentiality at every stage of processing and transmission.***

Methods. ***The study employed analytical methods including modeling and simulation, statistical and comparative analysis, experimental research, and risk assessment, enabling a comprehensive understanding of data transmission quality management in Bluetooth networks under cross traffic conditions.***

Results. ***Properly configuring the buffer zone size can significantly enhance the efficiency and reliability of protecting critical data from unauthorized access and cyberattacks. Modern approaches to buffer size optimization utilize traffic analysis and modeling methods, as well as machine learning algorithms to predict traffic volumes and characteristics. For instance, clustering algorithms can be employed to identify traffic types and characteristics, allowing for more efficient resource allocation and buffer space management. To effectively optimize the buffer zone size, it is essential to consider system performance and information security standards, including ISO/IEC 27001 and ISO/IEC 27002. ISO/IEC 27001 outlines requirements for information security management systems, emphasizing risk assessment and the implementation of security measures. ISO/IEC 27002 provides recommendations for data protection, such as the use of cryptographic methods. The buffer zone size must meet the requirements of cryptographic algorithms and ensure resilience against attacks such as DoS and buffer overflow, while also considering scalability and compliance with contemporary regulations.***

Conclusions. ***Optimizing the buffer zone size in the context of video data transmission over Bluetooth networks is a critical aspect that affects not only the stable operation of the system as a whole but also the effective management of traffic flows, allowing for improvements in information transmission quality and significantly reducing potential risks from external cyberattacks and internal failures that may arise due to cross traffic or other network anomalies. The application of adaptive signal modulation in close interaction with three-tier data buffering enables the system to dynamically adjust to variable communication channel parameters, such as transmission speed, noise levels, and interference. This, in turn, helps maintain a high level of video stream quality even under adverse environmental conditions and increased signal variability. The integration of three buffer levels, each performing distinct storage and preprocessing functions for incoming data, creates an additional protective barrier that significantly minimizes the negative impact of external factors on system stability, particularly by preventing possible delays, interruptions, or data loss that may arise due to changing environmental conditions or network impediments during information transmission.***

Keywords: ***buffer optimization, video streaming, Bluetooth wireless networks, adaptive management, data transmission, signal quality, packet loss, user priority management, cross traffic, information protection.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; in the decision to publish the results.

ISSN 2707-1758

УДК 004.422.81+004.774
DOI: https://doi.org/10.17721/ISTS.2024.8.17-25

Сергій БУЧИК, д-р техн. наук, проф.
ORCID ID: 0000-0003-0892-3494
e-mail: buchyk@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Андрій КУРОЄДОВ, студ.
ORCID ID: 0009-0007-5811-4798
e-mail: askuroyedov@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

МОДЕЛЬ АНАЛІЗУ ВЕБЕКСПЛОЙТІВ НА ОСНОВІ JAVASCRIPT

Вступ. *Задача забезпечення безпеки вебдодатків і серверів залишається актуальною в умовах постійного зростання кількості атак у кіберпросторі. Використання різних систем керування вмістом із відкритим кодом (наприклад WordPress, Joomla, Open Journal Systems, Drupal), які через свою простоту в установленні та використанні, є доволі популярними для створення вебсайтів, на жаль вимагають постійного оновлення не тільки для покращення за змістом, але і для забезпечення безпеки системи. Автори статті зосередили увагу саме на системі WordPress, хоча цей підхід може бути використаний і для інших систем. Матеріал статті підкреслює значення раннього виявлення вразливостей для запобігання потенційним кіберзагрозам та їх негативним наслідкам. Запропоновано модель і скрипт, які призначені для прискорення виявлення вразливостей у додатках WordPress. Автоматизація процесу сканування за допомогою власного скрипту дозволяє швидко виявляти вразливості, забезпечуючи оперативне виправлення й оновлення. Такий підхід не лише зміцнює безпеку, але і сприяє збереженню репутації вебсайтів та брендів, що є критично важливим у сучасному цифровому середовищі.*

Методи. *Використано методи аналізу вебексплойтів на основі JavaScript з урахуванням загальних принципів їх аналізу та з огляду на методології аналізу вебдодатків на вразливості.*

Результати. *Представлено вдосконалену модель аналізу вебдодатка на CMS WordPress, в основі якої є скрипт, який забезпечує автоматизоване сканування вебдодатка за допомогою запуску таких утиліт: NMAP, Dirb, Nikto, SQLMap, WPScan і PwnXSS. Усі результати записують в окремий файл для подальшого вивчення всіх знайдених проблем безпеки вебдодатка.*

Висновки. *Розроблена модель і скрипт повинні допомогти розробникам і тестувальникам прискорити процес виявлення вразливостей у WordPress, оскільки вони можуть запустити один скрипт і через короткий термін часу отримати об'ємний і змістовний звіт із виявленими вразливостями. За рахунок цього оптимізується виявлення вразливостей за допомогою автоматизованого запуску сканерів.*

Ключові слова: *вразливість, вебсайт, вебдодаток, вебексплуатація, аналіз вебдодатків, пошук вразливостей. SQL, XSS, CSRF.*

Вступ

В сучасному цифровому світі вебексплойти стали однією з найсерйозніших загроз для безпеки вебдодатків та вебінфраструктури. Ця проблема виникає з того, що вебексплойти дають можливість зловмисникам використовувати вразливості вебдодатків для виконання шкідливого коду або отримання несанкціонованого доступу до системи. Методи аналізу вебексплойтів на основі JavaScript є надзвичайно важливими, оскільки JavaScript є однією з основних мов програмування для веброзробки, і відповідно, використовується практично на кожній вебсторінці.

JavaScript, як основна мова програмування для веброзробки, проникає практично в кожен аспект інтернет-простору. Від створення динамічного змісту до взаємодії з користувачем, JavaScript є невід'ємною складовою будь-якого сучасного вебдодатка. Ця широка поширеність робить JavaScript дуже привабливою мішенню для зловмисників, які шукають можливості використовувати вразливості цієї мови для здійснення атак.

Атаки на основі JavaScript можуть мати різноманітні форми і наслідки. Вони можуть включати впровадження шкідливого коду на сторінках вебсайтів для отримання конфіденційної інформації користувачів, викрадення сесійних файлів, а також підміну вмісту сторінок для поширення фішингових атак або розповсюдження шкідливого програмного забезпечення.

Захист вебдодатків і серверів – це багатогранна задача, що поєднує в собі збереження конфіденційності даних, безперебійну роботу ресурсів і запобігання фінансовим втратам. Нехтування безпекою може призвести до серйозних наслідків, таких як втрата репутації, юридичні проблеми та збитки. Дослідження методів аналізу вебексплойтів JavaScript є ключовим фактором у забезпеченні безпеки вебдодатків та інфраструктури в цифрову епоху. Ця тема потребує постійного розвитку та вдосконалення для гарантування безпеки в онлайн-середовищі (Common JavaScript Vulnerabilities and How They Manipulate Data (2022), https://www.preemptive.com/blog/a-review-/on-javascript-security-in-2022/).

Мета дослідження – аналіз існуючих методів і моделей аналізу вебдодатків, побудова власної, удосконаленої моделі аналізу вебексплойтів на основі JavaScript.

Об'єктом дослідження є процес аналізу вебексплойтів на основі JavaScript.

Предметом дослідження є методи та моделі аналізу вебексплойтів на основі JavaScript.

Отже, основне завдання полягає в удосконаленні моделі аналізу вебексплойтів на основі JavaScript, яка має пришвидшити процес виявлення вразливостей у вебдодатках, які побудовані на CMS Wordpress.

Огляд літератури. Атаки на вебдодатки – це зловмисна діяльність, спрямована на використання вразливостей у конструкції або реалізації програм, що працюють через веб. Ці атаки можуть призвести до незаконного доступу, крадіжки даних або інших шкідливих наслідків.

Загальні принципи веббезпеки та поширені вразливості, зокрема і пов'язані з JavaScript розглянуто в (Liang, 2014) та (Stuttard, & Marcus Pinto, 2008).

ISSN 2707-1758

Особливо варто відмітити книгу (Hoffman A., 2024) в якій пояснено наступальні та захисні прийоми кібербезпеки. Автор вважає, що "освоївши концепції, а не прийоми використання платних інструментів, будь-який користувач зможе переходити від одного інструменту до іншого або створювати свої інструменти, виявляти вразливості та вживати заходів щодо пом'якшення наслідків".

З огляду на вказане автори, зосередили увагу як на використанні інструментів, так і на поєднанні певної концепції, шляхом автоматизації самого процесу виявлення вразливостей.

В ході викладення опису результатів, щоб дотримативсь логічної послідовності подання матеріалу, автори додатково здійснюють огляд літератури.

Методи

Використано методи аналізу вебексплойтів на основі JavaScript з урахуванням загальних принципів їх аналізу та з огляду на методології аналізу вебдодатків на вразливості.

Результати

Найпоширеніші методи атак JavaScript включають виконання шкідливих сценаріїв, викрадення даних сесії користувача або даних із локального сховища вебпереглядача, спонукання користувачів до виконання непередбачуваних дій та експлуатацію вразливостей у вихідному коді вебпрограм – рис. 1 (Web Exploitation, 2024: https://devopedia.org/web-exploitation).

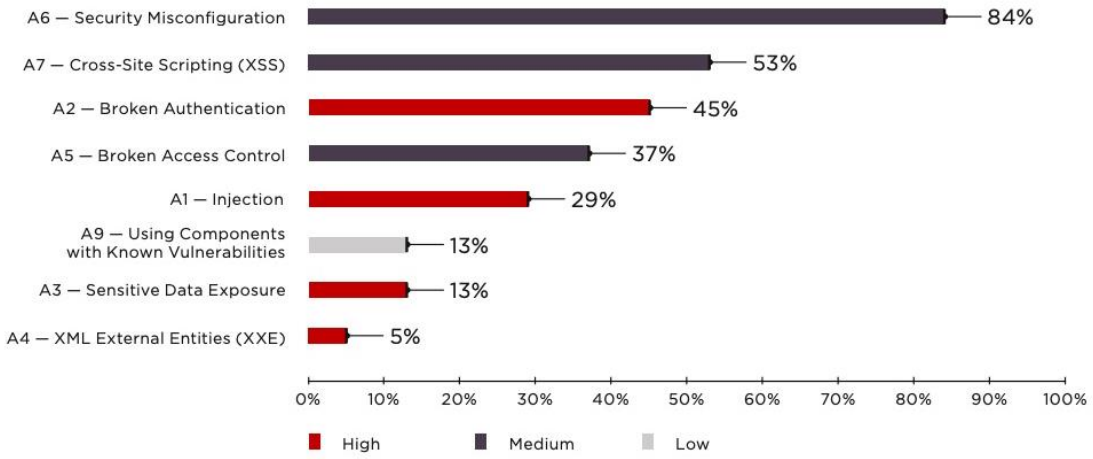

Рис. 1. Найпоширеніші вебатаки

Нижче наведено найпоширеніші атаки на вебдодатки (The 7 Most Common Web Application Attacks And How A WAF Can Prevent Them, 2024, https://www.nexusguard.com/blog/the-7-most-common-web-application-attacks-and-how/-a-waf-can-prevent-them); 8 Types of Web Application Attacks and Protecting Your Organization, 2023, https://brightsec.com/blog/8-types-of-web-application-attacks/-and-protecting-your-organization/).

Однією з найпоширеніших вебатак є *SQL-ін'єкція*. Зловмисники можуть вставляти шкідливий SQL-код у поля введення вебдодатків, що може призвести до несанкціонованого доступу до бази даних. Заходи захисту, такі як вебзахист від вторгнень (WAF), можуть блокувати підозрілі SQL-запити та використовувати методи відповідності шаблонів для виявлення та блокування спроб SQL-ін'єкцій. Ще однією вразливістю є *неправильна конфігурація*, яка виникає, коли налаштування належно не зберігають під час ручного виконання процесів. Це може створювати ризики безпеки та вразливості в системі.

Міжсайтовий сценарій (XSS) є ще однією серйозною проблемою. Він виникає, коли сервер приймає зловмисний код JavaScript через введення користувача та повертає його у відповідь, що призводить до виконання цього коду в браузері, що може мати негативні наслідки для безпеки вебдодатка.

Міжсайтова підробка запитів (CSRF) – це тип атаки на вебпрограму, яка шахрайським шляхом змушує користувача виконати небажану дію з вебпрограмою, в якій він уже автентифікований. Цього часто досягають, надсилаючи спеціально створене посилання або код користувачеві, який потім виконує небажану дію після виконання. Наприклад, атака CSRF може бути використана для проведення несанкціонованих операцій, таких як купівля або зміни налаштувань облікового запису. Щоб запобігти атакам CSRF, можна використовувати анти-CSRF маркери, що є унікальними ідентифікаторами, які генеруються вебпрограмою для кожного сеанса користувача і мають включатися в кожний запит до програми.

Щодо застарілого програмного забезпечення, з огляду на зростання використання пакетів програмного забезпечення з відкритим кодом і сторонніх програм, важливо постійно оновлювати їх. Використання застарілого програмного забезпечення може стати загрозою, особливо якщо вразливості стають загальнодоступними.

HTTP request smuggling. Транспортування HTTP-запитів використовує невідповідність у аналізі невідповідних HTTP-запитів, яка виникає у разі обміну їх між двома HTTP-пристроями, зазвичай між сервером і брандмауером, що підтримує HTTP, або зовнішнім проксісервером. Процес транспортування HTTP-запитів відбувається за допомогою створення кількох налаштованих HTTP-запитів, які дозволяють двом цільовим сутностям бачити дві різні серії запитів.

Заголовок HTTP пропонує два різні способи вказати, де закінчується запит: заголовок Transfer-Encoding і заголовок Content-Length. Уразливість транспортування HTTP-запитів виникає, коли зловмисник надсилає обидва заголовки в одному запиті. Це може призвести до того, що зовнішній або внутрішній сервер неправильно інтерпретує запит через зловмисний HTTP-запит. Уразливості транспортування запитів

ISSN 2707-1758

використовують кіберзлочинці, щоб обійти заходи безпеки, отримати доступ до конфіденційної інформації та для прямого компрометування користувачів різних програм. Можна також використовувати цю вразливість для вторинних експлойтів, наприклад, обхід брандмауерів, часткове отруєння кешу та міжсайтовий сценарій.

Атака відмови в обслуговуванні (DDoS) – це спосіб атаки на вебпрограму, що полягає в перевантаженні програми великою кількістю трафіка з різних джерел, таких як ботнети або скомпрометовані пристрої. Це може призвести до того, що вебпрограма стане недоступною для легітимних користувачів. DDoS-атаки можна уникнути за допомогою пристроїв мережної безпеки – брандмауерів і систем запобігання вторгненням, які можуть виявляти та блокувати шкідливий трафік. До того ж розробники вебдодатків можуть скористатися мережами доставки контенту (CDN) та балансувальниками навантаження для розподілу трафіка між декількома серверами з метою пом'якшення наслідків DDoS-атак.

XML External Entity (XXE) – це форма атаки на вебдодатки, що використовує вразливості у парсерах XML, що застосовані у додатку. Це може дозволити зловмиснику отримати доступ до конфіденційних даних або виконати несанкціоновані дії на сервері вебдодатка. Часто атаки XXE включають упровадження спеціально створених корисних даних XML, які використовують можливість синтаксичного аналізатора XML читати зовнішні сутності. Цим атакам можна запобігти, вимкнувши синтаксичний аналіз зовнішніх об'єктів або використовуючи захищені аналізатори XML, які належно очищують вхідні дані.

Автентифікація та авторизація. Ідентифікатор сесії може бути розкритим через URL-адресу. Пароль може бути незашифрованим. Якщо тайм-аут реалізовано неправильно, можливе викрадення сесії. Доступ до неавторизованих ресурсів можливий, навіть якщо інтерфейс користувача не розкриває їх.

Прямі посилання на об'єкти. Через поганий дизайн або помилку кодування прямі посилання можуть бути доступні для клієнтів. Наприклад, запит GET на download.php?file=secret.txt може обійти авторизацію та дозволити пряме завантаження захищеного файлу. Іншим прикладом є пряме скидання пароля адміністратора.

Brute Force. Атака грубою силою – це автоматичний метод вгадування комбінації імені користувача та пароля для отримання несанкціонованого доступу до вебпрограми. Зловмисники використовують програмні інструменти, щоб спробувати різні комбінації імен користувачів і паролів, поки не отримають доступ. Щоб убезпечити себе від атак грубої сили, вебдодатки можуть упроваджувати стратегії контролю швидкості та блокування облікових записів. Контроль швидкості обмежує кількість спроб входу з однієї IP-адреси, тоді як блокування облікового запису тимчасово призупиняє доступ до облікового запису після певної кількості невдалих спроб входу.

Розкриття даних. Одним із ризиків є витікання конфіденційних даних, які можуть зберігатися в незашифрованому вигляді або бути відкритими у файлах cookie чи URL-адресах під час взаємодії між клієнтом і сервером без використання HTTPS.

В роботі (Noman, Iqbal, & Manzoor, 2020), а також у (Rokia, & El Habib, 2022) описано, що всі вразливості можна поділили на три групи: неправильна перевірка введених даних, неправильне керування сеансами, неналежна автентифікація та авторизація.

До першої групи належать такі вразливості: маніпуляція / додавання запитів, упровадження коду на стороні клієнта, упровадження файлів у вебдодаток. Загалом для експлуатації вразливостей цієї групи, можна здійснити такі атаки, як SQL Injection, NoSQL Injection, Xpath and LDAP Injection, Cross-site scripting, Remote document local record consideration, Path / Directory Injection and Remote Code infusion.

До другої групи відносять вразливість керування сеансами. Для експлуатації цієї вразливості можна впровадити атаку Cross-site request forgery (CSRF).

До третьої групи належить помилка в логіці коду. Відповідно, можуть бути впроваджені такі атаки: Unreliable Direct Object Reference, missing Functional access Control, Invalidated Redirects and Forwards or application rationale susceptibilities.

Існують спеціальні інструменти для аналізу вразливостей до поширених атак на вебдодатки.

Acunetix Vulnerability Scanner – це комплексний і автоматизований інструмент для виявлення вразливостей у програмному забезпеченні. Він використовує методи аналізу Black-Box і Gray-Box для виявлення різноманітних проблем безпеки та може бути розгорнутий як у хмарі, так і на стороні клієнта. Acunetix здатний ідентифікувати і повідомляти про різноманітні вразливості в програмах, що побудовані на різних платформах, таких як WordPress, PHP, ASP.NET, Java Framework, Ruby on Rails тощо. Інструмент має широкий набір можливостей і для автоматизованого, і для ручного тестування, що дозволяє оцінити й усунути виявлені проблеми безпеки. Система Acunetix розрахована на роботу з багатьма користувачами і забезпечує доступ лише до необхідних ресурсів, що сприяє командній гнучкості та підвищує продуктивність (Attack Simulation and Vulnerability Management, 2024, https://itbiz.ua/proizvoditeli/acunetix/acunetix-web-vulnerability/-scanner-standard-premium-360/).

AppSpider – це рішення динамічного тестування безпеки додатків, яке здатне сканувати веб- та мобільні додатки щодо наявності вразливостей. Основною технологією, що використовується в AppSpider, є універсальний перекладач, який адаптується до новітніх технологій, таких як AJAX, HTML5 і JSON, що застосовуються у сучасних веб- та мобільних додатках, і проводить сканування і традиційних, і новітніх програм (Welcome to AppSpider, 2024, https://docs.rapid7.com/appspider/).

OWASP ZAP – це інструмент, який дуже простий у використанні для проведення тестів на проникнення програмою, а також для виявлення вразливостей у вебдодатках. OWASP ZAP проводить тестування на проникнення вебдодатка та дозволяє виявляти такі атаки, як SQL injection, XSS, clickjacking тощо (Introduction to OWASP ZAP, 2024, https://medium.com/@lavanya.agre.cyb/introduction-to-owasp-zap-bdc58293005f).

Nmap чи Network Mapper – це відкритий інструмент, призначений для вивчення мережі та перевірки її безпеки. Початково він був розроблений для швидкого сканування великих мереж, але також ефективно застосовується для аналізу окремих цілей. Nmap використовує IP-пакети у специфічний спосіб для визначення доступних хостів у мережі, надаючи інформацію про надані ними послуги (назву та версію програм), операційні системи та їхні версії, типи використаних пакетних фільтрів / брандмауерів та інші характеристики. Nmap часто застосовують для оцінювання безпеки, а також для контролю структури мережі та керування розкладами запуску служб та обліку часу

роботи хостів або служб (Nmap (Man Page), 2024, https://nmap.org/book/man.html).

Metasploit Framework – це дуже потужний інструмент, який використовують як кіберзлочинці, так і етичні хакери для виявлення системних уразливостей у мережах та на серверах. Оскільки це фреймворк з відкритим кодом, його можна легко налаштувати та використовувати на більшості операційних систем (What is Metasploit? The Beginner's Guide, 2024, https://www.varonis.com/blog/what-is-metasploit).

SQLMap – це інструмент для тестування на проникнення. Інструмент має вбудований механізм виявлення із спеціалізованими можливостями для досвідчених тестерів на проникнення та широким спектром параметрів для отримання детального звіту з тестування на проникнення. SQLMap може використовуватися зловмисниками для проведення SQL-ін'єкцій на потрібні додатки за допомогою різних методів, таких як логічні значення, часові проміжки, помилки, UNION-запити, стековані запити та позасмугове впровадження (SQlMap: automatic SQL injection and database takeover tool, 2024, https://sqlmap.org/).

Дослідження вебдодатків на вразливості нині – це важливе завдання, яке дозволить вебпрограмам належно функціонувати. Це тестування виконують розробники та тестувальники ПЗ, які зазвичай використовують уже існуючі та перевірені часом методики. До таких методологій можна віднести (5 Most Popular Web App Security Testing, 2024, https://www.apriorit.com/qa-blog/524-web-application-security-testing):

- Open Source Security Testing Methodology Manual (OSSTMM);
- Open Web Application Security Project (OWASP);
- Web Application Security Consortium Threat Classification (WASC-TC);
- Penetration Testing Execution Standard (PTES);
- Information Systems Security Assessment Framework (ISSAF);
- PCI Penetration Testing Guide;
- NIST Special Publication 800-115;
- MITRE ATT&CK.

Усі вказані методології – потужні інструменти та техніки, які допомагають у різних сферах упровадження безпеки. Проаналізуємо наскільки ефективними будуть ці методики для вебдодатків, побудованих на CMS WordPress.

OSSTMM може бути корисною для глибокого тестування безпеки.

Методологія OWASP надає широкий перелік рекомендацій і кращих практик із покращення безпеки вебдодатків. З огляду на широке використання платформ WordPress та OpenCart, рекомендації OWASP можуть бути дуже корисними для ідентифікації та уникнення загроз безпеці.

Методологія WASC TC допомагає виявити специфічні загрози, що можуть виникнути в контексті застосування WordPress та OpenCart.

Використання PTES дозволяє ідентифікувати й експлуатувати вразливості, що допоможе покращити безпеку вебдодатків на платформах WordPress та OpenCart.

Розглянемо сценарій, де власник онлайн-магазину на платформі OpenCart прагне підвищити рівень безпеки свого вебдодатка. Використовуючи ISSAF, він може провести аналіз потенційних загроз і ризиків, що можуть виникнути внаслідок недоліків у безпеці мережі, конфігурації сервера або програмного забезпечення. За допомогою цього аналізу він може ідентифікувати критичні вразливості і розробити стратегії для їхнього усунення.

Використовуючи NIST Special Publication 800-115, власник магазину може впровадити стандартизовані методики тестування безпеки для проведення тестування на проникнення й аудиту безпеки. Це дозволить виявити можливі вразливості в додатку й інфраструктурі магазину, такі як SQL-ін'єкції, XSS-атаки, недоліки в конфігурації сервера тощо.

Для створення моделі аналізу вебдодатків обрано середовище для тестування – CMS Wordpress. Через велику кількість користувачів WordPress стає привабливою мішенню для зловмисників, оскільки потенційної шкоди можна завдати багатьом вебсайтам одночасно. Зауважимо, що CMS WordPress містить безліч плагінів і тем, що розширюють функціонал системи.

Розробники плагінів і тем не завжди дотримуються найвищих стандартів безпеки, що може призводити до появи вразливостей у вебдодатку. До того ж активний розвиток WordPress і його постійні оновлення можуть приховувати недоліки безпеки, які тестувальники можуть виявити перед релізом нових версій. Нарешті, широкий функціонал платформи, такий як можливість створювати власні додаткові поля або налаштовувати права доступу, створює додаткові можливості для потенційних вразливостей.

Для проведення дослідження був установлений Wordpress на Ubuntu 22.04. Для тестування встановлено вразливу тему для Wordpress (рис. 2) з github (https://github.com/vavkamil/dvwp).

До плагінів належать:

- Infinite WP client – версія 1.9.4.4;
- Social Warfare – версія 3.5.2;
- Wordpress File Upload – версія 4.12.2;
- WP-Advanced-Search – версія 3.3.3;
- Askimet Anti-Spam – версія 4.1.3;
- Backup and Staging by WP Time Capsule – версія 1.21.15;
- Hello Dolly – версія 1.7.2.

Wordpress містить безліч плагінів для аналізу вразливостей у вебдодатку, проте ці плагіни можуть і самі бути вразливими.

Коли йдеться про аналіз вразливостей у вебдодатках, створення власного скрипту може бути кращим рішенням, ніж використання плагінів у WordPress, тому що власний скрипт може бути розроблений під ваш вебдодаток, що дозволить врахувати особливості цього вебдодатка. Зазначимо, що при розробленні і використанні власного рішення, ви можете мати повний контроль над кодом, що дозволяє гарантувати безпеку вашого рішення, оскільки ви не залежите від сторонніх плагінів та бібліотек і використовуєте свої функції. Застосовуючи власний скрипт, можна оперативно виправляти вразливості, які можуть бути знайдені.

Отже, власний скрипт для аналізу вразливостей може бути надійнішим та ефективнішим варіантом, ніж використання плагінів у WordPress.

Модель аналізу вебдодатка на CMS Wordpress зображено на рис. 3. Нижче опишемо її.

1. Початкова розвідка вебдодатка та сканування всіх існуючих сервісів, портів і служб. Використовуючи інструменти, такі як nmap, скрипт зможе сканувати порти та визначати відкриті служби.

2. Аналіз вебсайту на вразливості. Скрипт зможе використовувати інструменти, такі як Nikto або OWASP ZAP, для сканування вебсайту на наявність відомих вразливостей.

3. Генерація звіту. Скрипт зможе створювати звіт із виявленими вразливостями та рекомендаціями щодо їхнього виправлення.

ISSN 2707-1758

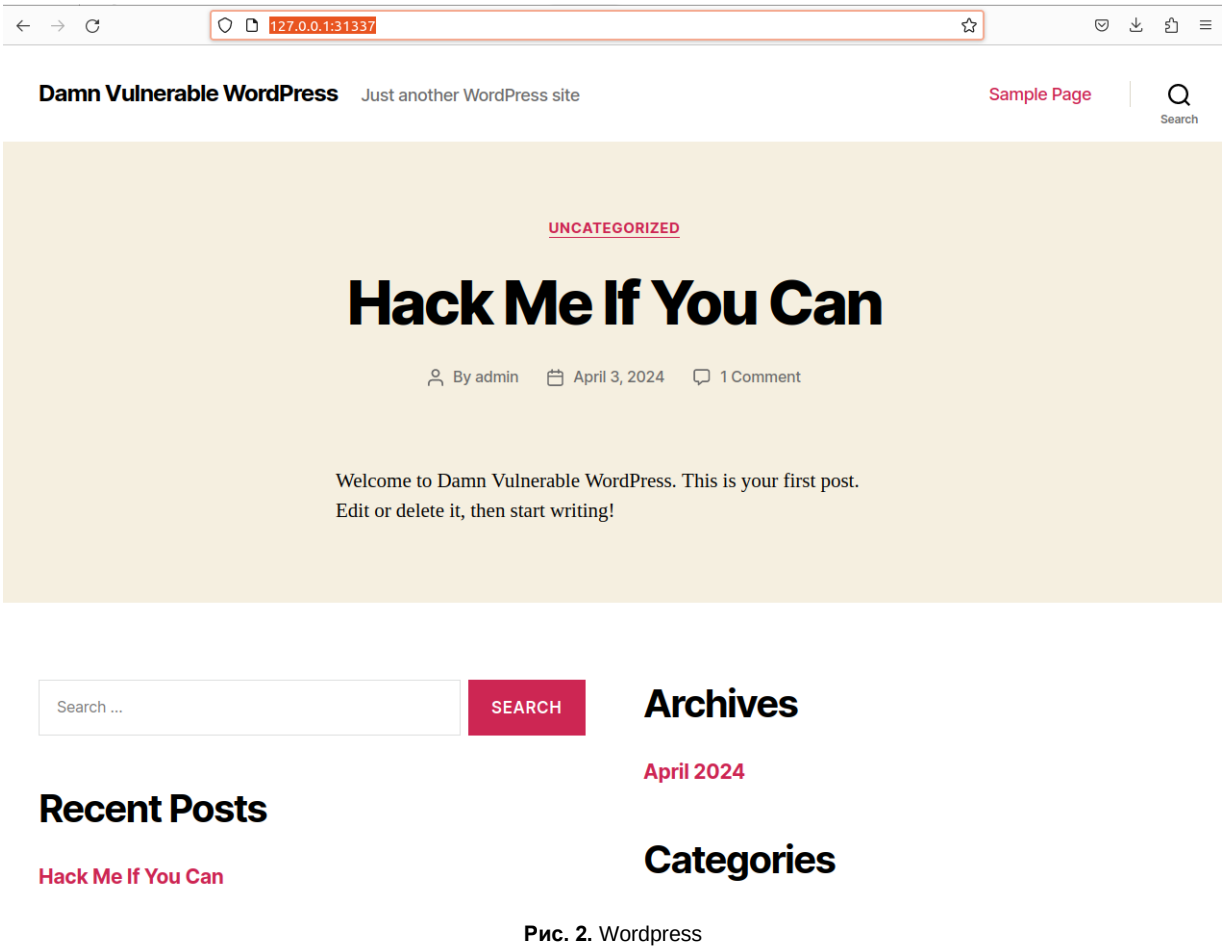

Рис. 2. Wordpress

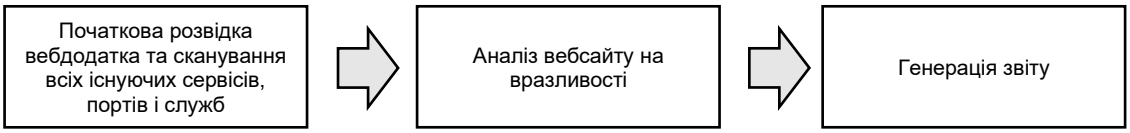

Рис. 3. Модель аналізу вебдодатка на CMS Wordpress

На першому етапі моделі використаємо інструмент NMap і Dirb для пошуку файлів / директорій, до яких має доступ звичайний користувач.

На другому етапі застосуємо інструменти для пошуку вразливостей, наприклад, WPScan, nikto, SQLmap, PwnXSS.

WPScan – це сканер, який широко використовують спеціалісти з кібербезпеки, які бажають визначити всі можливі слабкі місця в CMS WordPress. Сканер дозволяє виявляти вразливості у версіях систем, у плагінах, а також темах. Отже, використання такого програмного забезпечення – це спосіб забезпечити надійну безпеку вебдодатка.

До того ж WPScan здатний проводити брутфорс-атаку на WordPress. Використовуючи додаткові словники з даними, можна підібрати дані для авторизації.

На третьому етапі потрібно згенерувати звіт з усіма результатами. Звіт має містити детальний результат тестування вебдодатка за допомогою всіх згаданих вище утиліт і програм.

У віртуальному середовищі Oracle Virtual Box створено й налаштовано віртуально ОС Ubuntu 22.04, де було написано bin / bash скрипт для аналізу вебдодатка WordPress, про який вказано раніше. Цей скрипт забезпечує автоматизоване сканування вебдодатка за допомогою запуску утиліт, таких як NMAP, Dirb, Nikto, SQLMap, WPScan та PwnXSS. Зауважимо, що всі результати записують в окремий файл для подальшого вивчення всіх знайдених проблем безпеки вебдодатка.

На рис. 4 продемонстровано код скрипту.

На першому етапі отримано результати сканування NMap і Dirb. За допомогою nmap знайдено відкриті порти та служби (рис. 5).

Завдяки Dirb було знайдено приховані директорії та файли, до яких має доступ звичайний користувач (рис. 6).

Наступний крок – це сканування за допомогою утиліти Nikto.

Під час сканування вебдодатка утиліта виявила багато можливих вразливих місць, які здатні порушити безпеку додатків, наприклад, OSVDB 3092, 2695.

Знайдені OSVDB вразливості включають вразливість бібліотеки / плагіна "My Photo Gallery pre 3.6". Також за допомогою Nikto знайдено доступні директорії для звичайного користувача, які зловмисник може використати для проникнення в систему (рис. 7).

ISSN 2707-1758

```
 GNU nano 6.2                                  script.sh *
#!/bin/bash


echo "Start nmap"

nmap -p- -sV -sC -A 127.0.0.1 | tee -a "scan-results.txt"
echo "Finished"


echo "Start dirb"

dirb http://127.0.0.1:31337/ -f | tee -a "scan-results.txt"
echo "Finished"

echo "Start Nikto"

nikto -h http://127.0.0.1:31337/ | tee -a "scan-results.txt"
echo "Finished"


echo "Start SQLmap"

sqlmap -u 127.0.0.1:31337/?s=gngh | tee -a "scan-results.txt"
echo "Finished"


echo "Start WPSCAN"

wpscan --url http://127.0.0.1:31337/ --api-token IAph8RXF1kSeypxDAsXDVrmPr3AaFsHXimatV0YeeS4 | tee -a "scan-results.txt"
echo "Finished"

echo "Start PwnXSS"

python3 PwnXSS/pwnxss.py -u http://127.0.0.1:31337/ | grep -i "WARNING" | tee -a "scan-results.txt"
echo "Finished"


fi

exit 0
```

Рис. 4. Вихідний код скрипту

```
PORT      STATE SERVICE         VERSION
80/tcp    open  http            Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Welcome to Test.com!
631/tcp   open  ipp             CUPS 2.4
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: CUPS/2.4 IPP/2.1
|_http-title: Home - CUPS 2.4.1
3306/tcp  open  nagios-nsca     Nagios NSCA
| mysql-info:
|   Protocol: 10
|   Version: 8.0.36-0ubuntu0.22.04.1
|   Thread ID: 346279
|   Capabilities flags: 65535
|   Some Capabilities: Support41Auth, LongPassword, DontAllowDatabaseTableColumn, SupportsTransactions, LongColumnFlag, Sp
eaks41ProtocolOld, SupportsLoadDataLocal, SupportsCompression, InteractiveClient, Speaks41ProtocolNew, FoundRows, SwitchTo
SSLAfterHandshake, IgnoreSigpipes, IgnoreSpaceBeforeParenthesis, ODBCClient, ConnectWithDatabase, SupportsAuthPlugins, Sup
portsMultipleStatments, SupportsMultipleResults
|   Status: Autocommit
|   Salt: s     uU"gMb3x+\x1E%0\x015\x06\x7Fkr
|_  Auth Plugin Name: caching_sha2_password
31337/tcp open  hadoop-datanode Apache Hadoop 2.4.38 ((Debian))
| hadoop-datanode-info:
|_  Logs: http://127.0.0.1:31337/wp-login.php
| hadoop-tasktracker-info:
|_  Logs: http://127.0.0.1:31337/wp-login.php
|_http-generator: WordPress 5.3
|_http-title: Damn Vulnerable WordPress &#8211; Just another WordPress site
|_http-trane-info: Problem with XML parsing of /evox/about
31338/tcp open  http            Apache httpd 2.4.57 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: phpMyAdmin
33060/tcp open  mysqlx?
```

Рис. 5. Результати сканування NMap

```
Start dirb

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Apr 17 22:08:20 2024
URL_BASE: http://127.0.0.1:31337/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Fine tunning of NOT_FOUND detection

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://127.0.0.1:31337/ ----
+ http://127.0.0.1:31337/cgi-bin/ (CODE:200|SIZE:1633)
+ http://127.0.0.1:31337/favicon.ico (CODE:200|SIZE:0)
+ http://127.0.0.1:31337/index.php (CODE:301|SIZE:0)
+ http://127.0.0.1:31337/info.php (CODE:200|SIZE:6098)
+ http://127.0.0.1:31337/php.ini (CODE:200|SIZE:2)
+ http://127.0.0.1:31337/server-status (CODE:403|SIZE:277)
+ http://127.0.0.1:31337/xmlrpc.php (CODE:405|SIZE:5)

-----------------
END_TIME: Wed Apr 17 22:13:15 2024
DOWNLOADED: 4612 - FOUND: 7
Finished
```

Рис. 6. Результати сканування Dirb

ISSN 2707-1758

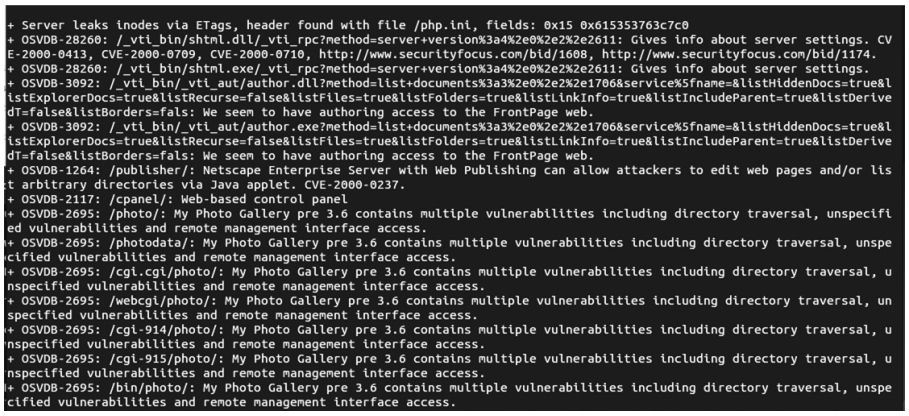

Рис. 7. Результати сканування Nikto

Наступний інструмент для виявлення можливих вразливостей – це SQLMap. Під час тестування не виявлено вразливостей (рис. 8).

Відтак запускається утиліта WPScan. Це дуже потужне програмне забезпечення, яке надає багато можливостей у дослідженні безпеки вебдодатка і не тільки. Сканер ідентифікував 52 різні вразливості, які потенційно можуть завдати шкоди для вебдодатка на WordPress. Виявлено вразливості встановлених плагінів і теми Wordpress (рис. 9).

Рис. 8. Результати сканування SQLMap

Рис. 9. Результати сканування WPScan

Останнім інструментом у дослідженні безпеки вебдодатка на WordPress є програмне забезпечення PwnXSS, яке тестує додаток щодо наявності можливих вразливостей міжсайтового сценарію XSS. Під час сканування він виявив потенційно цікаві посилання з різними ідентифікаторами, які можуть налічувати вразливості XSS (рис. 10).

Рис. 10. Результати сканування PwnXSS

Усі результати зберігають в окремому файлі, де зручно досліджувати й аналізувати знайдені вразливості вебдодатка. Отже, в результаті сканування вебдодатка, розробник або тестувальник, який запускає цей скрипт, може знайти чимало цікавої інформації про свій вебдодаток. Знайдені вразливості частково описуються самими сканерами, але не всі. Деякі знайдені вразливості потрібно досліджувати, тому що не обов'язково всі знайдені потенційно вразливі точки вебдодатка можуть бути вразливі. Найкориснішим цей сканер буде для вебдодатків, побудованих на CMS Wordpress, оскільки утиліта WPScan знаходить вразливі версії плагінів. Тому, якщо даний сканер знайшов вразливі плагіни, то їх необхідно терміново оновити, щоб зловмисники не скористались цими вразливостями до того, як ви їх виправите.

Дискусія і висновки

Атаки на основі JavaScript можуть мати різні форми і наслідки, від впровадження шкідливого коду до крадіжки конфіденційної інформації. Забезпечення безпеки вебдодатків і серверів є критично важливою задачею, оскільки недбалість у цьому питанні може призвести до серйозних наслідків, таких як втрата репутації і фінансові втрати.

Виявлення вразливостей у системі керування контентом WordPress на ранніх етапах має критичне значення з кількох причин. По-перше, це допомагає підвищити захист від можливих атак, оскільки розробники мають можливість оперативно виправити проблеми і випустити оновлення з виправленнями. Це зменшує ризик успішного злому або недозволених дій на сайтах, що працюють на WordPress.

Друга причина полягає у збереженні репутації. Уразливості, які залишаються непоміченими або не виправляються вчасно, можуть призвести до втрати контролю над сайтом або витоку конфіденційних даних, що серйозно нашкодить репутації компанії чи особистого бренду.

Третя причина – виконання нормативних вимог. Деякі стандарти безпеки (наприклад, PCI DSS для платіжних систем) передбачають виявлення та швидке усунення вразливостей як обов'язковий етап для дотримання вимог.

Зазначимо, що вчасне виявлення вразливостей допомагає зменшити ризик фінансових втрат, оскільки це дозволяє уникнути можливих наслідків, пов'язаних із збоями в роботі сайту, втратою даних чи клієнтів.

Розроблена модель та скрипт допоможе розробникам і тестувальникам прискорити процес виявлення вразливостей у Wordpress, оскільки вони можуть запустити один скрипт і в середньому через 10 хвилин отримати об'ємний і змістовний звіт із виявленими вразливостями. У такий сросіб оптимізується виявлення вразливостей через автоматизований запуск сканерів.

Внесок авторів: Сергій Бучик – концептуалізація, методологія; Андрій Куроєдов – аналіз джерел, підготовка огляду літератури, теоретичних засад дослідження, підготовка лабораторії для дослідження, проведення дослідження.

Список використаних джерел

Hoffman, A. (2024). *Web Application Security.* O'Reilly Media (2nd Ed.).

Liang, Y. (2014). *JavaScript Security.* PACKT Publishing.

Noman, M., Iqbal, M., & Manzoor, A. (2020). A Survey on Detection and Prevention of Web Vulnerabilities. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 11(6). http://dx.doi.org/10.14569/IJACSA.2020.0110665

Rokia, A., & El Habib, N. (2022). Deep Learning for Vulnerability and Attack Detection on Web Applications: A Systematic Literature Review. *Future Internet,* 14(4). https://doi.org/10.3390/fi14040118

Stuttard, D., & Marcus Pinto, M. (2008). *The Web Application Hacker's Handbook.* Wiley Publishing.

References

Hoffman, A. (2024). *Web Application Security.* O'Reilly Media (2nd Ed.).

Liang, Y. (2014). *JavaScript Security.* PACKT Publishing.

Noman, M., Iqbal, M., & Manzoor, A. (2020). A Survey on Detection and Prevention of Web Vulnerabilities. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 11(6). http://dx.doi.org/10.14569/IJACSA.2020.0110665

Rokia, A., & El Habib, N. (2022). Deep Learning for Vulnerability and Attack Detection on Web Applications: A Systematic Literature Review. *Future Internet,* 14(4). https://doi.org/10.3390/fi14040118

Stuttard, D., & Marcus Pinto, M. (2008). *The Web Application Hacker's Handbook.* Wiley Publishing.

Отримано редакцією журналу / Received: 30.10.24
Прорецензовано / Revised: 25.11.24
Схвалено до друку / Accepted: 30.11.24

ISSN 2707-1758

Serhii BUCHYK, DSc (Engin.), Prof.
ORCID ID: 0000-0003-0892-3494
e-mail: buchyk@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Andrii KUROIEDOV, Student
ORCID ID: 0009-0007-5811-4798
e-mail: askuroyedov@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

JAVASCRIPT-BASED WEB EXPLOIT ANALYSIS MODEL

Background. ***The task of ensuring the security of web applications and servers remains important and relevant in the face of the ever-increasing number of attacks in cyberspace. The use of various open-source content management systems (e.g. WordPress, Joomla, Open Journal Systems, Drupal), which are quite popular for creating websites due to their ease of installation and use, unfortunately, require constant updating not only to improve the content but also to ensure the security of the system. In this article, the authors focus on the WordPress system, although this approach can be used for other systems as well. The article emphasises the importance of early detection of vulnerabilities to prevent potential cyber threats and their negative consequences. The article proposes a model and a script designed to speed up the detection of vulnerabilities in WordPress applications. Automation of the scanning process with a custom script allows you to quickly detect vulnerabilities, ensuring prompt fixes and updates. This approach not only strengthens security, but also helps preserve the reputation of websites and brands, which is critical in today's digital environment.***

Methods. ***The methods of analysing JavaScript-based web exploits were used, taking into account the general principles of their analysis and taking into account the methodologies for analysing web applications for vulnerabilities.***

Results. ***An improved model of analysing a web application on CMS Wordpress based on a script that provides automated scanning of a web application by running the following utilities is presented: NMAP, Dirb, Nikto, SQLMap, WPScan and PwnXSS. All the results are recorded in a separate file for further study of all the found security issues of the web application.***

Conclusions. ***The developed model and script should help developers and testers speed up the process of identifying vulnerabilities in Wordpress, as they can run one script and get a voluminous and meaningful report with the identified vulnerabilities in a short time. This optimises vulnerability detection by automating the launch of scanners.***

Keywords: ***vulnerability, website, web application, web exploitation, web application analysis, vulnerability scanning, SQL, XSS, CSRF.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.

UDC: 004.75+004.8:519.23
DOI: https://doi.org/10.17721/ISTS.2024.8.26-33

Serhii TOLIUPA, DSc (Engin.), Prof.
ORCID ID: 0000-0002-1919-9174
e-mail: tolupa@i.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Maksym KOTOV, PhD Student
ORCID ID: 0000-0003-1153-3198
e-mail: maksym_kotov@ukr.net
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

PROTECTION MODEL AGAINST DISTRIBUTED GRADUAL DEGRADATION ATTACKS BASED ON STATISTICAL AND SEMANTIC APPROACHES

Background. *Nowadays, every critical sector of social institutions conducts its operations on top of distributed processing systems. Contemporary digital infrastructure heavily relies on user-provided data in its operation. As a result, distributed attacks based on botnets are in a continuous state of arms race with the protection methods that filtrate malicious data influx. A common method to do so often relies on heuristics and human-oriented verifications. As the new advancements in the field of artificial intelligence emerge, such attacks adopt new oblique paths towards achieving their goals. The successful execution of the said plan could lead to a gradual resource depletion on the target system. The purpose of this research is to address such threats with a combination of statistical and semantic approaches.*

Methods. *The following research conducts a theoretical analysis and systematization of the distributed gradual degradation attack in distributed systems and its implication in the context of the evolving technologies of artificial intelligence. Mathematical modeling is leveraged to define the proposed model's properties and execution process. The proposed model heavily relies on statistical methods for analyzing time series data and its deviations, as well as classification neural networks for semantic detection of suspicious behavior.*

Results. *As a result of the following research, a new model is developed that leverages statistical and semantical verification for anomaly detection. The continuous monitoring and detection process is optimized towards highly loaded systems with a constant flurry of data streams.*

Conclusions. *Since the distributed attacks could be potentially equipped with intelligent means to bypass existing security measures, the development of a protection model against potential resource leaks is gaining relevance. The recent success in the development of artificial generative intelligence leads to raising concerns about the safety and adequacy of the current security measures against automation-based distributed attack vectors. It is often a case that the protection models are inclined towards prevention of the attack rather than recovery. This approach, while targeting the source of risks, often leads to complacent design decisions without considering the potential outcomes of a successful breach. The proposed model provides a theoretical foundation for building systems that both react to the active execution of threats and perform recovery mechanisms, assuming that the attack may potentially bypass initial security measures.*

Keywords: *distributed systems, gradual degradation attacks, resource exhaustion, statistical analysis, semantic approaches, resilience, LightGBM, Distilbert, EWMA.*

Background

The majority of contemporary cloud and distributed systems work on top of a client-server model. Within the context of such an approach, the server expects requests from a client system to initiate an interaction process. Once the message is received, the service nodes perform desired computation and resource allocation as defined per operational logic. It is often a case for such RPC or HTTP endpoints to have an authentication system in place that relies on multi-factor human interaction verification by involving multiple external services or identification credentials, such as phone number. Nonetheless, it is also a common approach to have a dedicated public subset of services since it could be useful to provide a succinct demonstration of the system's capabilities or simply used to request initial access rights.

In that context, it is important to emphasize the difference between transient and mutation requests. Transient requests are executed on a stateless basis. Each subsequent request does not influence the system's state nor the results of any subsequent execution. Such requests often rely on data reads or real-time computation rather than deferred, asynchronous execution or static storage services. Mutating requests involve the allocation or creation of additional computational or storage assets as per the request's parameters. These requests could be generalized further by including state changes of non-persistent logical resources. An example of such could be rate limits for external services.

Additionally, mutating requests could be further split into categories of idempotent and cumulative state-changing interactions. Where the first guarantees that any subsequent operation of the same nature will result in the same state of the system. As a matter of fact, the idempotent category spans between a subset of mutating and the whole set of transient requests. Each subsequent transient request does not change the state at all, hence leaving it the same after an arbitrary amount of requests of the same nature. Whereas cumulative state operations gradually modify the shared state and always impact the allocation of computational assets in one way or another.

Service providers could be categorized into two categories: stateful and stateless systems. Stateless systems typically rely on providing transient services. Such systems are extremely scalable and easy to coordinate since no consensus is required. In addition to that, they do not rely on persistent resource allocation and utilize exclusively dynamic operational hardware. Stateful systems are characterized by their operational uniqueness. Interaction with such a system could involve the allocation or deallocation of persistent resources, mainly storage. It is usually the case that within a single distributed system that provides a complex multi-step service, there are sets of both categories.

Having established the context of interaction-driven services, we can now discuss the security implications and attack vectors for each described processing model. In the context of this article, automation-based distributed attacks

ISSN 2707-1758

are in the limelight of the research. The most common and known attack of such type is Deny of Service (DOS) and its invariant Distributed Deny of Service (DDOS). The origins of this attack took root in the times of developing global interconnection networks. Its implications, strategies, and modern protection mechanisms are well studied and defined in numerous scientific works (Mirkovic, & Reiher, 2004; Douligeris, & Mitrokotsa, 2004; Srivastava et al., 2011; Zargar, Joshi, & Tipper, 2013; Zhang, Wang, & Chen, 2017). DOS is characterized by its aggressive nature and is applicable to every type of request described previously.

Though the impact could differ greatly between mutating and transient requests, the primary goals are generally the same: overwhelm the target system with a barrage of nonsensical computational tasks to stifle or preclude execution of concurrent legitimate processing threads. The congestion often leads to temporal downtimes, loss of reputation, trust, and, as a result, of fungible assets. The protection methods often involve massive cloud networks with innate capabilities of service masking and traffic distribution. Such networks often rely on pattern-recognition models to differentiate between authentic and malicious packet streams.

In contrast, this article aims to define a potential new attack vector that is more subtle and clandestine. The Distributed Gradual Degradation attack does not rely on aggressive bombardment of the target systems. It relies on the gradual creation and execution of mutative cumulative requests that incrementally reduce the system's capacity to provide a service. Since it's not based on congestion surge, it's less conspicuous and is more likely to be executed successfully. The said attack is inefficient for transient and has limited efficiency on idempotent requests since they by definition have a limited impact on the system's state. The common approach to fending off automated requests is based on human authenticity verification based on interaction heuristics, such as mouse moves or choices made.

With the recent development of generative artificial intelligence and its ever-improving qualities, a new arms race between such challenge-based approaches and their automated solution is ongoing. AI models are potentially capable of mimicking human behavior and decision-making processes to a sufficient degree to bypass current identification methods. This led to the development of yet more confounding challenges with multiple logical steps. Though with a rapid evolution of the generative AIs, it remains unclear whether those measures are sufficient (Hernández-Castro et al., 2017; Kovács, & Tajti, 2023; Sukhani et al., 2021).

The purpose of the article. The intention and goal of this research is to develop a theoretical protection model against the distributed gradual degradation attack vector. This article aims to provide a solid set of active and passive measures towards ensuring adequate usage of the system's resources by external requests. Within the scope of this research, we consider and outline the integration of the aforementioned protection model within the context of streaming asynchronous communication services and static storage engines.

The key principles that form the foundation of this model are efficiency and a knowledge-based approach. The first principle is straightforward: as the model aims to protect resources, it should rationally utilize them itself. The latter means that ability should be tapered towards capabilities of classification neural networks in juxtaposition to generative AIs. The reasoning behind this approach stems from the significant computational complexity involved in developing and training these models. The training and execution of generative models require exponentially more time than that of classification models. Hence, the attack becomes ineffectual since it would require more sources than it would seemingly degrade on a target machine.

Analysis of literary sources. The distributed gradual degradation attack vector enhanced by recent developments and improvements in artificial intelligence is not extensively studied as of now but is a looming topic of scientific research. Nevertheless, its foundational components, such as bypassing contemporary bot detection systems, and its implications are growing rapidly in relevance.

Active research on DDOS has been ongoing since the early 2000s. Significant contributions towards attack definition, classification, and potential prevention methods are provided by the works of (Mirkovic, & Reiher, 2004; Douligeris, & Mitrokotsa, 2004; Srivastava et al., 2011; Zhang, Wang, & Chen, 2017).

With the development of deep learning models, computer vision, and artificial intelligence in general, common protection methods against automation-based attacks become increasingly susceptible. In that direction, impactful research results were published by (Na et al., 2020; Sukhani, et al., 2021; Kovács, & Tajti, 2023; Hernández-Castro et al., 2017).

Improving detection model efficiency involves statistical estimation and evaluation of time series data. Exponentially Weighted Moving Average (EWMA) is described within the works of (Hunter, 1986; Lucas & Saccucci, 1990; Cox, 1961). The Integrated Moving Average (ARIMA) method and its implications are outlined by (Box, & Pierce, 1970; Nelson, 1998). Semantic detection in the context of phishing attacks is assessed by the following studies: (Buchyk et al., 2024; Buchyk, Shutenko, & Toliupa, 2022; Toliupa et al., 2023). The authors provide and describe models of detecting suspicious contents of emails with a set of semantic methods such as cosine distance between data-driven vectors.

Classification neural networks serve as the backbone of the proposed model. Their key feature is a simplified and efficient training process that is exponentially faster than that of the generative AIs. The significance and operational basis of such technology are described within the works of (Zhang, Zhang, & Yu, 2017). Decision trees LightGBM and XGBoost are described within works of (Leevy et al., 2020; Zhao, Wang, & Wang, 2023). Last, but not least, the language processing model Distilbert is assessed and studied by (Adoma, Henry, & Chen, 2020; Büyüköz, Hürriyetoğlu, & Özgür, 2020).

Methods

The following research conducts a theoretical analysis and systematization of the distributed gradual degradation attack in distributed systems and its implication in the context of the evolving technologies of artificial intelligence. Mathematical and graphic modeling are leveraged to define the proposed model's properties and execution process. The proposed model heavily relies on statistical methods for analyzing time series data and its deviations, as well as classification neural networks for semantic detection of suspicious behavior.

This work additionally describes an exemplary architecture of a target distributed system that utilizes static-storage and stream-oriented services to outline an

integration of the proposed model in the workloads based on different processing paradigms. Since most contemporary distributed systems utilize queuing and asynchronous communication models, the implications and middleware-oriented integration method of the developed protection model are described within the context of the streaming architectures. Additionally, this paper outlines the external monitoring-oriented integration of the said protection model for the static data warehouses analysis and resource deallocation.

Results

The following section presents a novel theoretical model of protection against distributed gradual degradation attacks. We will initially outline the statistical approach towards detecting anomalies. After that, we will delve into the application of a neural network for deep semantical scanning of suspicious activity spikes. This theoretical model will later be applied to an exemplary distributed system's architecture. First and foremost, we will describe the architecture itself, its services, and intercommunication methods. After that, an integration plan for the static data storage engines and real-time streaming services will be provided to facilitate integration of the proposed method into modern distributed systems.

Protection model against distributed gradual degradation attacks. The automated activity detection model is comprised of multiple parts. Firstly, it defines the global and internal timeframe segregation and boundaries to achieve better performance results. Based on those intervals, an Exponentially Weighted Moving Average (EWMA) method is used to control the degree of suspiciousness. That degree influences the aggressiveness of semantic scanning.

We will first start with the management aspect of the proposed model. Let us define time parameters:

- T: Total timeline over which data (incoming requests) are observed.
- t: Specific time point within T.
- $R(t)$: Set of records (incoming requests) at time t.
- W: Size of the sliding window (in time units).
- $W(t)$: Sliding window at time t, containing records from $t - W$ to t.

The interval parameters are expressed as:

- G_s: Size of each global interval (Global Interval Size).
- I_s: Size of each internal interval within a global interval (Internal Interval Size).
- G_i: The i-th global interval, $G_i = [(i-1)G_s, iG_s)$.
- $I_{i,j}$: The j-th internal interval within G_i, $I_{i,j} = [(i-1)G_s + (j-1)I_s, (i-1)G_s + jI_s)$.
- n_I: Number of internal intervals per global interval, $n_I = G_s/I_s$.

Semantic sampling parameters are defined as follows:

- n_s: Initial number of samples per global interval ($Num\_Samples$) ($0 < n_s \leq n_I$).
- T_s: Sampling threshold ($Sampling\_Threshold$), expressed as a percentage.
- α: Smoothing factor for EWMA ($0 < \alpha \leq 1$).
- β: Sensitivity factor for adjusting the number of samples based on statistical anomalies.
- δ: Sensitivity factor for adjusting the number of samples based on semantic anomalies.
- $N_{i,j}$: Number of records in internal interval $I_{i,j}$.
- $N_{\text{total},i}$: Total number of records in global interval G_i.

At any time t:

$$\mathrm{W(t)} = \{\mathrm{R(s)} \mid \mathrm{t - W \leq s \leq t}\}. \quad (1)$$

The sliding function defines a set of records that are being buffered and evaluated. It practically limits the resources allocated to the detection model and provides a granular control for environments with different memory capacities. The sliding function continuously moves in time and contains a set of the most recent records. This function could also be used to establish a retrospective analysis by propelling the window backwards in time rather than forward.

The entire timeline T is divided into global intervals:

$$\mathrm{G_i} = [(\mathrm{i}-1)\mathrm{G_s}, \mathrm{iG_s}), \quad \mathrm{i} \in \mathrm{N}. \quad (2)$$

Global intervals allow set boundaries for semantic sampling strategy. Since semantic sampling is computationally heavy, as we will see later on, it is important to use it as a last resort rather than brute force. Records are assigned to these intervals based on timestamps.

Each global interval G_i is subdivided into n_I internal intervals:

$$I_{i,j} = [(i-1)G_s + (j-1)I_s, (i-1)G_s + jI_s), \quad j = 1,2,\dots,n_I. \quad (3)$$

Internal discretization is another aspect of performance improvement. It allows limiting sampling size to a controlled set of records. The combinations of these parameters allow to manage the risks and resource utilization, where the latter is of high importance because the entire purpose of the model is to save resources.

Moving on the semantic sampling, the dynamic number of samples for time t is defined as follows:

$$n_s(t) = n_s + \lceil \beta \times D(t) \rceil. \quad (4)$$

Where $D(t)$ is the degree of anomalies detected at time t; $\lceil \cdot \rceil$ is a ceiling function to ensure an integer number of samples. This approach allows to continuously react in stochastic environments.

Statistical approach based on EWMA is used to manage $n_s(t)$ and react efficiently to ongoing security events at each time t (Cox 1961, p. 414; Hunter, 1986, p. 203; Lucas, & Saccucci, 1990, p. 1):

- Compute the average number of records in the sliding window:

$$\mathrm{x_t} = \frac{\mathrm{N_W(t)}}{\mathrm{W}}, \quad (5)$$

- where $N_W(t) = |W(t)|$.
- Update EWMA:

$$\mathrm{EWMA(t)} = \alpha \mathrm{x_t} + (1-\alpha)\mathrm{EWMA(t-1)}, \quad (6)$$

- Compute the deviation:

$$D(t) = |x_t - \mathrm{EWMA}(t)|. \quad (7)$$

An anomaly is detected if $D(t)$ exceeds a predefined anomaly threshold A_T. The number of samples $n_s(t)$ is adjusted dynamically in real time as shown in equation 4.

The sampling is done at random for n_s internal timeframes. Let us first define utility functions:

- $P_{\text{bot}}(r)$: $R \to [0,1]$ a function that maps each record $r \in R$ to a probability $P_{\text{bot}}(r)$, where $P_{\text{bot}}(r)$ represents the likelihood that record r is bot-origin. We will discuss its definition later.
- $\mathrm{A(r)}$: activation function outputs 1 if $P_{\text{bot}}(r) \geq T_{\text{bot}}$, and 0 otherwise.
- T_{bot}: is the threshold for determining bot-origin.

The process itself is defined as follows:

For $k = 1$ **to** $n_s(t)$**:**

- Randomly select an internal interval I_{i,j_k} within G_i.
- Collect records R_{i,j_k} in I_{i,j_k}.
- Compute $N_{i,j_k} = |R_{i,j_k}|$.

ISSN 2707-1758

- **For each** $r \in R_{i,j_k}$, **do:**
  - Apply the semantic recognition function $P_{\text{bot}}(r)$, which returns a probability from 0 to 1 that the record is bot-origin.
  - Compute the output of the activation function:

$$\mathrm{A(r)}=\begin{cases}1 & \text{if } P_{\text{bot}}(\mathrm{r}) \geq T_{\text{bot}} \\ 0 & \text{if } P_{\text{bot}}(r) < T_{\text{bot}}\end{cases}, \quad (8)$$

- Compute the total number of likely bot-origin entries in I_{i,j_k} as:

$$\mathrm{B_{i,j_k}} = \sum_{\mathrm{r}\in \mathrm{R_{i,j_k}}} \mathrm{A(r)}\,, \quad (9)$$

- Evaluate the sampling condition:

$$\frac{\mathrm{B_{i,j_k}}}{\mathrm{N_{i,j_k}}} > T_s\,, \quad (10)$$

- **If** the condition is met increment $n_s(t)$ by δ (increase sampling rate).
- **Else** continue to the next sample without adjusting $n_s(t)$.

This process allows the algorithm to react and adjust itself depending on events inside stochastic environments. This model is also highly customizable, allowing for different threshold and resource management parameters.

Semantic sampling model. Now let's move on the discussion of $P_{\text{bot}}(r)$ and its definition. Firstly, the model processes input data consisting of structured features x_s and textual content x_t. The structured data $x_s \in R^m$, where m is the number of structured features, is transformed into a feature vector $h_s \in R^{d_s}$ through a function f_{LGBM} (Ke et al., 2017, p. 3149; Leevy et al., 2020, p. 190; Zhao, Wang, Y., & Wang, J., 2023, p. 622):

$$\mathrm{h_s} = \mathrm{f_{LGBM}(x_s)}. \quad (11)$$

Function f_{LGBM} represents the processing performed by a LightGBM model. LightGBM is a gradient boosting decision-tree model that maps the structured input x_s to a learned feature representation h_s of dimension d_s. The output of that function is a high-dimensional vector that captures features of the provided data.

Simultaneously, the textual data x_t is mapped to an embedding vector $h_t \in R^{d_t}$ using a function $f_{\text{DistilBERT}}$ (Adoma, Henry, & Chen, 2020, p. 117; Büyüköz, Hürriyetoğlu, & Özgür, 2020, p. 9; Dogra et al., 2021, vol. 248):

$$\mathrm{h_t} = \mathrm{f_{DistilBERT}(x_t)}. \quad (12)$$

In this case, $f_{\text{DistilBERT}}$ represents the DistilBERT model, which processes raw text and converts it into a contextual embedding of dimension d_t. DistilBERT is a transformer-based language model that captures the semantic meaning and contextual nuances of the textual data and provides a dense vector representation h_t.

The key factors while choosing the models were performance, accuracy, and their ratio. Since the main goal is to preserve resources and reduce costs, the decision was made towards most efficient available models.

The feature vectors $\boldsymbol{h_s}$ and $\boldsymbol{h_t}$ are then concatenated to form a combined feature vector $h_c \in R^d$:

$$\mathrm{h_c} = \begin{bmatrix}\mathbf{h_s} \\ \mathbf{h_t}\end{bmatrix}. \quad (13)$$

Where $d = d_s + d_t$ is the total dimensionality after concatenation.

The combined feature vector $\boldsymbol{h_c}$ serves as the input to a sequence of L fully connected layers. Each layer l in this sequence performs a linear transformation followed by a non-linear activation function ϕ, the ReLU (Rectified Linear Unit) (Arora et al., 2018).

For $l = 1$ **to** L**:**

- Linear transformation:

$$\mathrm{z^{(l)}} = \mathrm{W^{(l)}a^{(l-1)}} + \mathrm{b^{(l)}}, \quad (14)$$

- Activation function:

$$\mathrm{a^{(l)}} = \phi\left(\mathrm{z^{(l)}}\right) = \max\left(0, \mathrm{z^{(l)}}\right). \quad (15)$$

Where:

- $W^{(l)} \in R^{n_l \times n_{l-1}}$ is the weight matrix for layer l.
- $b^{(l)} \in R^{n_l}$ is the bias vector for layer l.
- $a^{(l-1)}$ is the activated output from the previous layer (with $a^{(0)} = h_c$).
- n_l is the number of neurons in layer l.
- $n_0 = d$ is the size of the input layer.

After processing through the L fully connected layers, the model applies a final linear transformation followed by a sigmoid activation to produce the output probability $\hat{y}$ (Arora et al., 2018; Pratiwi et al., 2020, vol. 1471):

- Linear transformation:

$$\mathrm{z^{(L+1)}} = \mathrm{w^{(L+1)^T}a^{(L)}} + \mathrm{b^{(L+1)}}\,, \quad (16)$$

- Sigmoid activation:

$$\hat{\mathrm{y}} = \sigma\left(\mathrm{z^{(L+1)}}\right) = \frac{1}{1+\mathrm{e^{-z^{(L+1)}}}}. \quad (17)$$

Where:

- $w^{(L+1)} \in R^{n_L}$ is the weight vector for the output layer.
- T signifies that the matrix is transposed.
- $b^{(L+1)} \in R$ is the bias scalar for the output layer.
- The sigmoid function σ maps the input to a probability between 0 and 1.

The overall function of the model can be summarized as:

$$\hat{\mathrm{y}} = \mathrm{f_{model}(x_s, x_t)} = \\ = \sigma\left(\mathrm{w^{(L+1)^T}}\left(\phi \circ \ldots \circ \phi\left(\mathrm{W^{(1)}h_c} + \mathrm{b^{(1)}}\right)\right) + \mathrm{b^{(L+1)}}\right). \quad (18)$$

Where:

- f_{model} represents the composition of the LightGBM processing of structured data, the DistilBERT processing of textual data, and the subsequent fully connected layers leading to the final output.
- ∘ denotes function composition.
- ϕ is the activation function applied at each hidden layer.

This architecture essentially fuses two lightweight models that concern separate tasks to produce a probabilistic answer whether the data is a part of an automation-based attack. Messages that arrive at the server's endpoints are often structured and have multiple sensical fields. Such fields often hold textual, categorical, and numerical data types. Different models perform better on different data types and provide corresponding accuracy rates. DistilBERT is used to extract complex features from textual data, while LightGBM is used for categorical and numeric data.

The concrete applied definition of the model involves specifying a number of neurons in each fully connected layer through a tuple, such as $(512,256,128)$. The shown structure defines three layers with 512, 256, and 128 neurons. In this case, the dimensions of the weight matrices and bias vectors would be:

- $W^{(1)} \in R^{512 \times d}$, $b^{(1)} \in R^{512}$;
- $W^{(2)} \in R^{256 \times 512}$, $b^{(2)} \in R^{256}$;

- $W^{(3)} \in R^{128\times256}$, $b^{(3)} \in R^{128}$;
- $w^{(4)} \in R^{128}$, $b^{(4)} \in R$.

The combined vector h_c is passed through L fully connected layers with ReLU activations, computing outputs in a cycle for $l = 1$ to L:

$$\begin{cases} \boldsymbol{z}^{(l)} = \boldsymbol{W}^{(l)}\boldsymbol{a}^{(l-1)} + \boldsymbol{b}^{(l)} \\ \mathbf{a}^{(l)} = \phi\left(\mathbf{z}^{(l)}\right) = \max\left(0, \mathbf{z}^{(l)}\right) \end{cases}. \quad (19)$$

The final output is computed using a linear transformation followed by a sigmoid activation (Thakur & Dhawale):

$$\begin{cases} z^{(L+1)} = w^{(L+1)^{\mathrm{T}}} a^{(L)} + b^{(L+1)} \\ \hat{y} = \sigma\left(z^{(L+1)}\right) \end{cases}. \quad (20)$$

The model parameters, including the weights and biases of the fully connected layers and any trainable parameters within f_{LGBM} and $f_{\mathrm{DistilBERT}}$, are optimized during training to minimize the binary cross-entropy loss. This enables the model to make accurate predictions based on the input data and learning from both structured and textual information that could be passed to the system through the common communication structures, such as JSON.

Description of a target distributed system. Having defined the protection model against distributed gradual degradation attacks based on continuous monitoring and semantic sampling, let us now discuss its applied integration into contemporary distributed systems. With the theoretical context, parameters, and model properties in place, we first outline the architecture of the distributed system depicted on Fig. 1:

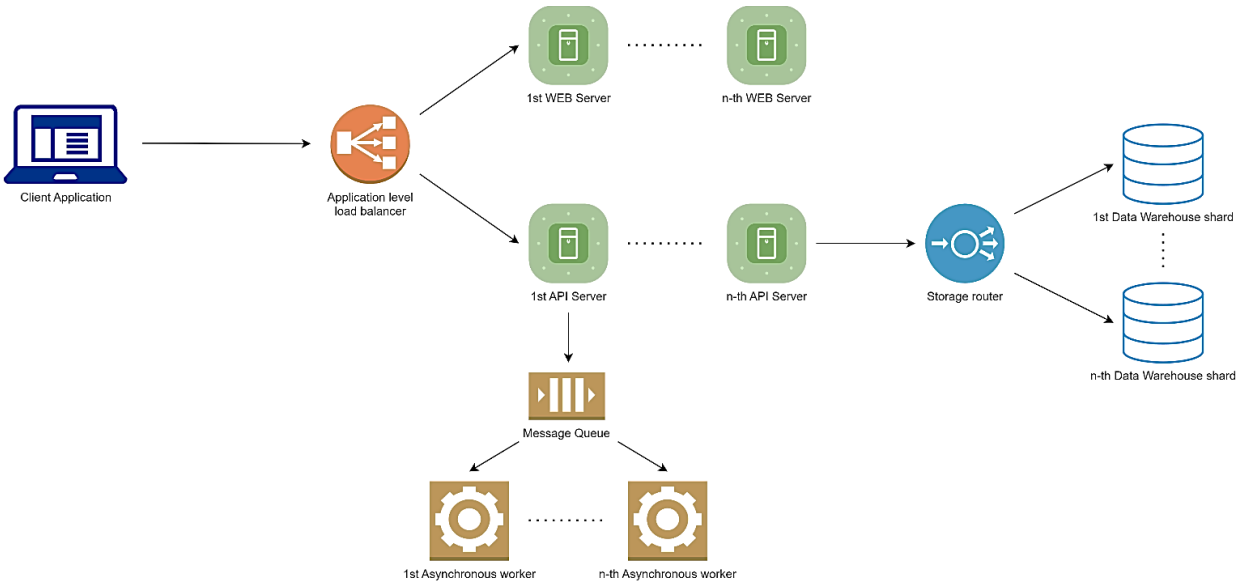

Fig. 1. Architecture of the target distributed system

This architecture represents an abstract system that uses the most common data flow methods: storage and stream-oriented. It consists of the application-level load balancer that routes the requests to the API and WEB servers based on the request paths. Subsequently, API servers could either perform a state-mutating operation in the data warehouse or initiate an asynchronous task through the means of queueing services. The common approach for building such workflows involves AMQP protocol (Prajapati, 2021).

Protection model application for data warehouse services. The data warehouse service is responsible for persistent storage, processing, and retrieval of information. It is often the case that such services are extremely hard to scale and are also the backbone of the stateful distributed system. Having said that, due to the extreme requirements for availability and consistency, it is important to integrate the protection model without impacting the response times and minimize influence on the overall performance. Fig. 2 shows the integration architecture with the persistent storage service:

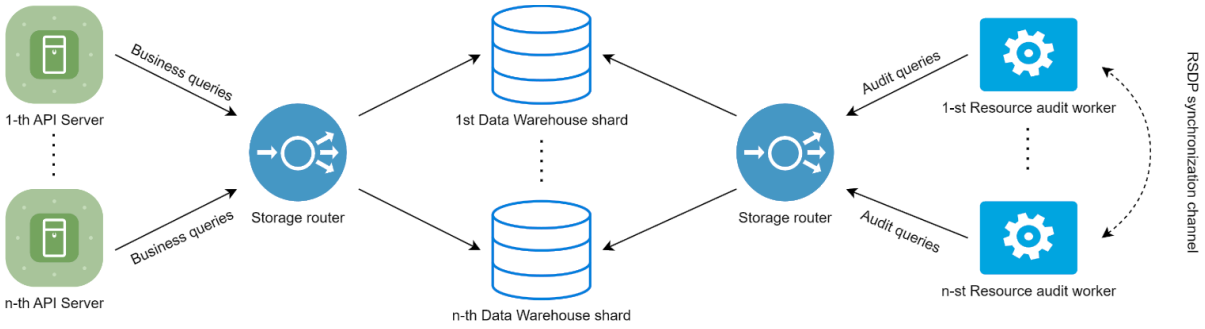

Fig. 2. Proposed model's integration as an asynchronous monitoring solution

ISSN 2707-1758

The architecture reflects an asynchronous, batch-processing approach towards resource utilization audits and protection gains distributed through gradual degradation attacks. The key principle is to allow flowless execution of requests and after that schedule retrospective tasks to verify the authenticity and validity of the mutations. For that purpose, the external "resource audit workers" perform the algorithm described within the protection model. Since the sliding window $W(t)$ is itself a parameter, it is possible to initialize such batch tasks in the required context.

Moreover, contemporary production systems tend to grow extensively in size. For that purpose, the service clusterization could be performed based on the Replica State Discovery Protocol (RSDP). RSDP provides a lightweight and efficient framework to coordinate cluster-wide operations execution and state management. Each node within such a cluster could leverage the deterministic parameters and based on its cluster position, schedule its sliding window accordingly (Kotov, Toliupa, & Nakonechnyi, 2024, p. 102; p. 156). Such an approach is efficient in terms of processing power and yet allows for scaling if needed.

Protection model application for data queueing and streaming services. The message queuing services primarily work in an "eventually transient mode". That is, these services do not save data for too long, often until the message processing is confirmed by a connected worker. These services are most frequently utilized for asynchronous and deferred operations. Which implies that the response time is not an issue, allowing for the middleware-oriented architecture. Figure 3 shows the integration architecture with the message streaming service:

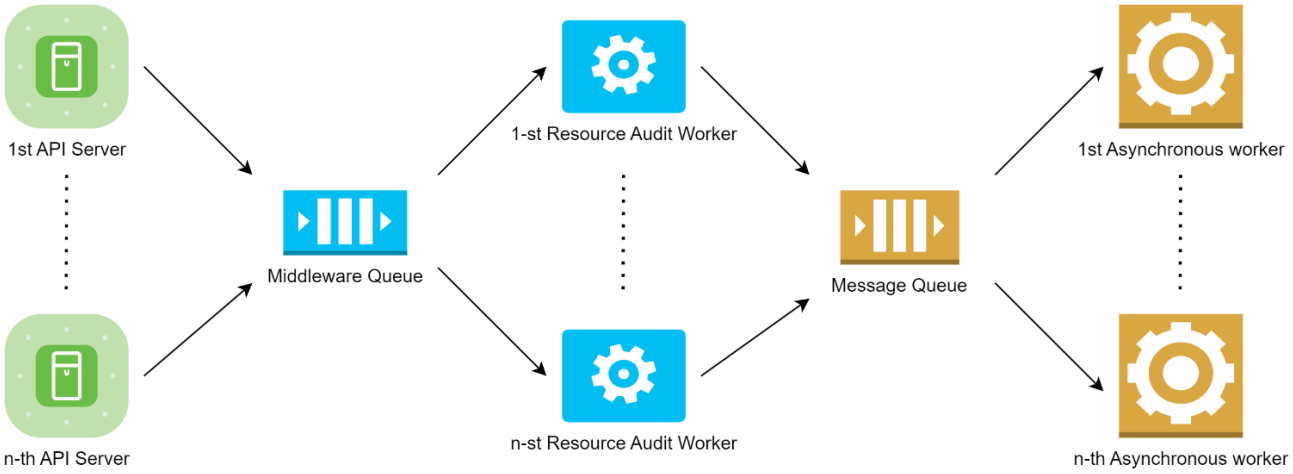

Fig. 3. Proposed model's integration as a middleware monitoring solution

Before the target message queue, this architecture implies the middleware queue for analytical and security processing. The entire model described earlier would be executed inside the "resource audit worker". Scalability in this case is trivial and does not require any coordination mechanism since the logic would entirely mirror the target queue's message processing infrastructure. Upon receiving new messages, the sliding would operate on a real-time basis and directly control the stored buffer size during the runtime. The message processing is often coordinated and distributed between the workers in a round-robin manner, thus effectively integrating load balancing capabilities for both the protection model's worker execution and the target logic itself (Prajapati, 2021).

Discussion and conclusions

Since the distributed attacks could be potentially equipped with intelligent means to bypass existing security measures, the development of a protection model against potential resource leaks is gaining relevance. The recent success in the development of artificial generative intelligence leads to raising concerns about the safety and adequacy of the current security measures against automation-based distributed attack vectors. It is often a case that the protection models are inclined towards prevention of the attack rather than recovery. This approach, while targeting the source of risks, often leads to complacent design decisions without considering the potential outcomes of a successful breach. The proposed model provides a theoretical foundation for building systems that both react to the active execution of threats and perform recovery mechanisms, assuming that the attack may potentially bypass initial security measures.

While developing the protection model against the gradual degradation attacks, the primary concern was twofold: ensuring that the system is capable of recovering from unexpected resource loss and ensuring that the detection and monitoring processes themselves don't require a superfluous amount of processing power. The primary focus was on the integration of the model within the operation context of streaming and static storage services. As a result, a set of diagrams, mathematical models, and theoretical descriptions is provided to simplify implementation of the said model in modern distributed systems.

The proposed model heavily relies on the semantic feature extraction capabilities of both decision trees and the neural networks. Even though LightGBM and Distilbert are both regarded as extremely fast models, tuned towards performance and memory usage, it is still a case that the execution of the trained model takes a significant amount of resources. That is why the proposed protection model focuses on the logical optimization based on global and internal timeframe discretization and statistical methods such as EWMA to reduce as much as possible the number of execution calls of the pretrained models for the semantic sampling.

To address the issue of efficiency with static data warehouse analysis, the proposed model utilizes global and internal discretization of the timeframes. This approach allows it to coordinate its operation in a batch-oriented way. The scalability of such a solution is hence

ISSN 2707-1758

possible by leveraging deterministic scheduling properties. Each monitoring node, knowing its own position in a replica, can effectively determine its assigned timeframes. In that context, the integration of RSDP provides an essential capability to organize a deterministic approach by synchronizing states between cluster nodes.

While addressing streaming services, this paper considers thoroughly the capabilities provided by queueing protocols such as AMQP. The introduction of middleware queues allows us to analyze suspicious messages in real-time. Additionally, the proposed scaling model involves logical extensions for exchanges that allow for statistical analysis and avoid redundant verification logic invocation. This approach significantly enhances the potential efficiency of the proposed model.

To summarize, the proposed model provides a solid and efficient theoretical foundation for managing intelligent threats towards digital and processing resources. Its implications necessitate continuous monitoring of emerging zero-day attacks that may easily bypass modern security measures. It is the intention of this article to inspire further empirical research, impact assessment of distributed gradual degradation attacks and their mitigation methods.

Authors' contribution: Maksym Kotov – conceptualization, methodology, formal analysis, development of software; Serhii Toliupa – analysis of sources, preparation of a literature review and theoretical foundations of research, editing and reviewing.

References

Adoma, A. F., Henry, N.-M., & Chen, W. (2020). *Comparative analyses of Bert, Roberta, Distilbert, and Xlnet for text-based emotion recognition*. *2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP),* 117–121. IEEE. https://doi.org/10.1109/ICCWAMTIP51612.2020.9317379

Arora, R., Basu, A., Mianjy, P., & Mukherjee, A. (2018). *Understanding deep neural networks with rectified linear units.* https://doi.org/10.48550/arXiv.1611.01491

Box, G. E. P., & Pierce, D. A. (1970*).* Distribution of residual autocorrelations in autoregressive-integrated moving average time series models. *Journal of the American Statistical Association*, 65(332), 1509–1526. https://doi.org/10.1080/01621459.1970.10481180

Buchyk, S., Shutenko, D., & Toliupa, S. (2022*).* Phishing attacks detection. *CEUR Workshop Proceedings*, 3384, 193–201. https://ceur-ws.org/Vol-3384/Short_7.pdf

Buchyk, S., Toliupa, S., Buchyk, O., & Shevchenko, A. (2024). *Method for detecting phishing sites*. In A. Luntovskyy, M. Klymash, I. Melnyk, M. Beshley, & A. Schill (Eds.). *Digital ecosystems: Interconnecting advanced networks with AI applications. TCSET 2024. Lecture notes in electrical engineering*, 1198. Springer, Cham. https://doi.org/10.1007/978-3-031-61221-3_15

Büyüköz, B., Hürriyetoğlu, A., & Özgür, A. (2020). Analyzing ELMo and DistilBERT on socio-political news classification. *In Proceedings of the Workshop on Automated Extraction of Socio-political Events from News 2020* (pp. 9–18). European Language Resources Association (ELRA).

Cox, D. R. (1961). Prediction by exponentially weighted moving averages and related methods. *Journal of the Royal Statistical Society. Series B (Methodological*), 23(2), 414–422. https://doi.org/10.1111/j.2517-6161.1961.tb00424.x

Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: Classification and state-of-the-art. *Computer Networks*, 44(5), 643–666. https://doi.org/10.1016/j.comnet.2003.10.003

Hernández-Castro, C. J., R-Moreno, M. D., Barrero, D. F., & Gibson, S. (2017). Using machine learning to identify common flaws in CAPTCHA design: FunCAPTCHA case analysis. *Computers & Security*, 70, 744–756. https://doi.org/10.1016/j.cose.2017.05.005

Hunter, J. S. (1986). The exponentially weighted moving average. *Journal of Quality Technology*, 18(4), 203–210. https://doi.org/10.1080/00224065.1986.11979014

Kotov, M., Toliupa, S., & Nakonechnyi, V. (2024). Replica state discovery protocol based on advanced message queuing protocol. *Cybersecurity: Education, Science, Technique*, 3(23), 156–171. https://doi.org/10.28925/2663-4023.2024.23.156171

Kovács, Á., & Tajti, T. (2023*).* CAPTCHA recognition using machine learning algorithms with various techniques. *Annales Mathematicae et Informaticae*, 58, 81–91. https://doi.org/10.33039/ami.2023.11.002

Leevy, J. L., Hancock, J., Zuech, R., & Khoshgoftaar, T. M. (2020). Detecting cybersecurity attacks using different network features with LightGBM and XGBoost learners. *IEEE Second International Conference on Cognitive Machine Intelligence (CogMI)*, 190–197. IEEE. https://doi.org/10.1109/CogMI50398.2020.00032

Lucas, J. M., & Saccucci, M. S. (1990*).* Exponentially weighted moving average control schemes: Properties and enhancements. *Technometrics*, 32(1), 1–12. https://doi.org/10.1080/00401706.1990.10484583

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *SIGCOMM Computer Communication Review*, 34(2), 39–53. https://doi.org/10.1145/997150.997156

Na, D., Park, N., Ji, S., & Kim, J. (2020). CAPTCHAs are still in danger: An efficient scheme to bypass adversarial CAPTCHAs. In I. You (Ed.). *Information security applications. WISA 2020. Lecture Notes in Computer Science*, 12583. Springer, Cham. https://doi.org/10.1007/978-3-030-65299-9_3

Nelson, B. K. (1998). Time series analysis using autoregressive integrated moving average (ARIMA) models. *Academic Emergency Medicine*, 5(7), 739–744. https://doi.org/10.1111/j.1553-2712.1998.tb02493.x

Prajapati, A. (2021). AMQP and beyond. *In 2021 International Conference on Smart Applications, Communications and Networking (SmartNets).* Glasgow, United Kingdom. https://doi.org/10.1109/SmartNets50376.2021.9555419

Srivastava, A., Gupta, B. B., Tyagi, A., Sharma, A., & Mishra, A. (2011*).* A recent survey on DDoS attacks and defense mechanisms. In D. Nagamalai, E. Renault, & M. Dhanuskodi (Eds.). Advances in parallel distributed computing. PDCTA 2011. *Communications in computer and information science*. *Vol. 203*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-24037-9_57

Toliupa, S., Buchyk, S., Shabanova, A., & Buchyk, O. (2023). The method for determining the degree of suspiciousness of a phishing URL. *CEUR Workshop Proceedings*, 3646, 239–247.

Zargar, S. T., Joshi, J., & Tipper, D. (2013*).* A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials*, 15(4), 2046–2069. https://doi.org/10.1109/SURV.2013.031413.00127

Zhang, B., Zhang, T., & Yu, Z. (2017*). DDoS detection and prevention based on artificial intelligence techniques*. In 2017 3rd IEEE International Conference on Computer and Communications (ICCC) (pp. 1276–1280). IEEE. https://doi.org/10.1109/CompComm.2017.8322748

Zhao, G., Wang, Y., & Wang, J. (2023). Intrusion detection model of Internet of Things based on LightGBM. *IEICE Transactions on Communications*, E106–B(8), 622–634. https://doi.org/10.1587/transcom.2022EBP3169

Отримано редакцією журналу / Received: 17.10.24
Прорецензовано / Revised: 15.10.24
Схвалено до друку / Accepted: 30.11.24

ISSN 2707-1758

Сергій ТОЛЮПА, д-р техн. наук, проф.
ORCID ID: 0000-0002-1919-9174
e-mail: tolupa@i.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Максим КОТОВ, асп.
ORCID ID: 0000-0003-1153-3198
e-mail: maksym_kotov@ukr.net
Київський національний університет імені Тараса Шевченка, Київ, Україна

МОДЕЛЬ ЗАХИСТУ ВІД РОЗПОДІЛЕНИХ АТАК ПОСТУПОВОГО ВИСНАЖЕННЯ РЕСУРСІВ, ЗАСНОВАНА НА СТАТИСТИЧНИХ І СЕМАНТИЧНИХ ПІДХОДАХ

В с т у п . *Нині кожен критично важливий сектор соціальних інституцій виконує свої операції на основі розподілених систем оброблення. Сучасна цифрова інфраструктура у своїй роботі значною мірою покладається на дані, що надають користувачі. В результаті, розподілені атаки на основі ботнетів перебувають у безперервних "перегонах озброєнь" із методами захисту, які фільтрують надходження шкідливих даних. Методи протидії часто покладаються на евристичні способи перевірки, орієнтовані на людину. З появою нових досягнень у сфері штучного інтелекту, такі атаки набувають додаткові шляхи досягнення своїх цілей. Успішне виконання зазначеного плану може призвести до поступового виснаження ресурсів цільової системи. Метою цього дослідження є намагання уникнути таких загроз за допомогою поєднання статистичних і семантичних підходів.*

М е т о д и . *Це дослідження проводить теоретичний аналіз і систематизацію розподіленої атаки поступового виснаження ресурсів у розподілених системах і її значення в контексті технологій штучного інтелекту, що розвиваються. Математичне моделювання використовують для визначення властивостей запропонованої моделі захтсту, процесу її інтеграції та виконання. Запропонована модель значною мірою покладається на статистичні методи для аналізу часових рядів та їхніх відхилень, а також класифікаційні нейронні мережі для семантичного виявлення підозрілої поведінки.*

Р е з у л ь т а т и . *У результаті цього дослідження розроблено нову модель, яка використовує статистичну та семантичну перевірку для виявлення аномалій. Процес безперервного моніторингу оптимізований для високонавантажених систем із постійним шквалом потоків даних.*

В и с н о в к и . *Оскільки розподілені атаки можуть бути оснащені інтелектуальними засобами для обходу існуючих заходів безпеки, то розроблення моделі захисту від потенційних витоків ресурсів набуває актуальності. Відомий нещодавній успіх у розробленні штучного генеративного інтелекту викликає занепокоєння щодо безпеки й адекватності поточних заходів безпеки проти векторів розподілених атак на основі автоматизації. Часто буває так, що моделі захисту налаштовані на запобігання нападу, а не на відновлення. Цей підхід, що орієнтований на джерело збитків, часто призводить до проєктних рішень без урахування потенційних результатів успішного порушення. Запропонована модель забезпечує теоретичну основу для створення систем, які одночасно реагують на активне виконання загроз і виконують механізми відновлення, припускаючи, що атака потенційно може обійти початкові заходи безпеки.*

К л ю ч о в і с л о в а : *розподілені системи, атаки поступового виснаження ресурсів, виснаження ресурсів, статистичний аналіз, семантичні підходи, стійкість, LightGBM, Distilbert, EWMA.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.

ISSN 2707-1758

УДК 004.056/.57+339.986:004.91+316.472.4
DOI: https://doi.org/10.17721/ISTS.2024.8.34-41

Олександр ПУЧКОВ, канд. філос. наук, проф.
ORCID ID: 0000-0002-8585-1044
e-mail: iszzi@iszzi.kpi.ua
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна

Дмитро ЛАНДЕ, д-р техн. наук, проф.
ORCID ID: 0000-0003-3945-1178
e-mail: dwlande@gmail.com
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна

Ігор СУБАЧ, д-р техн. наук, проф.
ORCID ID: 0000-0002-9344-713X
e-mail: igor_subach@ukr.net
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна

МЕТОДИКИ ЕКСТРАГУВАННЯ ОБ'ЄКТІВ КІБЕРБЕЗПЕКИ З ЕЛЕКТРОННИХ ДЖЕРЕЛ ІЗ ЗАСТОСУВАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Вступ. ***Стрімкий розвиток інформаційних технологій призвів до виникнення нових загроз і викликів у сфері кібербезпеки. Кібервійна стала реальністю та справжньою проблемою для держав, організацій та окремих користувачів кіберпростору. В Україні вживають заходи з розроблення системи кібердій у кіберпросторі, які включають сукупність взаємопов'язаних підсистем кіберрозвідки, кіберзахисту та кібервпливу. Однією з форм кіберрозвідки є розвідка з відкритих джерел – комп'ютерна розвідка (OSINT), яка здійснюється для пошуку й добування розвідувальної інформації, зокрема і для виявлення й аналізу об'єктів кібербезпеки щодо прогнозування можливих проявів кіберзагроз та їхніх наслідків. Це вимагає розроблення ефективних методів виявлення й аналізу об'єктів кібербезпеки за допомогою екстрагування фактографічних даних про об'єкти кібербезпеки з великих масивів неструктурованої текстової інформації.***

Методи. ***Досліджено технології штучного інтелекту, зокрема й великі мовні моделі (ВММ), та генеративного штучного інтелекту (ГШІ) в контексті застосування їх для розв'язання задач комп'ютерної розвідки об'єктів кібербезпеки з відкритих електронних джерел і соціальних мереж.***

Результати. ***У результаті проведеного дослідження, для здійснення дієвої аналітики результатів добування інформації, запропоновано методику екстрагування іменованих сутностей – назв хакерських угруповань та їхніх контекстуальних зв'язків із текстів повідомлень електронних мережних джерел, що стосуються предметної області кібербезпеки, а також формування мереж їхніх взаємозв'язків і змістовного аналізу цих мереж. Для визначення áкторів, які мають відношення до кібервійни, запропоновано методику аналізу відібраних документів, доступних в електронних джерелах інтернету та соціальних мережах. Обидві методики ґрунтуються на застосуванні ГШІ.***

Висновки. ***Результати дослідження демонструють ефективність запропонованих підходів і можливість їхнього застосування на практиці під час розв'язання завдань забезпечення кібербезпеки. Запропоновані методики можуть стати важливим інструментом для фахівців сфери кібербезпеки щодо розроблення ними ефективних стратегій захисту від кіберзагроз.***

Ключові слова: ***кібервійна, кібербезпека; генеративний штучний інтелект; великі мовні моделі; інтернет; відкриті електронні джерела; соціальні мережі, аналіз тексту; об'єкти кібервійни.***

Вступ

Стрімкий розвиток інформаційних технологій (ІТ) призвів до виникнення нових загроз і викликів у сфері кібербезпеки. Кібервійна стала реальністю та справжньою проблемою для держав, організацій та окремих користувачів інтернету. Кібервпливи все частіше стають ефективним інструментом для досягнення мети щодо контролю й управління як об'єктами критичної інфраструктури держави, так і окремо взятими громадянами та їхніми об'єднаннями (Даник, Воробієнко, & Чернега, 2019). Нині практично всі провідні держави світу зіткнулися з кіберзагрозами й необхідністю формувати системи кібербезпеки та кібероборони.

Залежність безпеки й економіки держави від стану важливих об'єктів та інформаційної інфраструктури об'єктів критичної інфраструктури, таких як: енергозабезпечення, водопостачання, транспорт, електронні комунікації тощо, обумовлює визнання кібербезпеки провідним елементом державної безпеки. Кіберзагрози у сучасному суспільстві набувають значного масштабу та являють собою наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі та негативно впливають на стан кібербезпеки держави.

З огляду на це в Україні вживають заходів із розроблення системи кібердій у кіберпросторі, під якими розуміють сукупність взаємопов'язаних підсистем кіберрозвідки, кіберзахисту, кібервпливу та кіберконтррозвідки, які утворюють цілісну єдність, на яку покладаються функції із забезпечення кібербезпеки (Даник, Воробієнко, & Чернега, 2019).

Зауважимо, що нині розвідка перемістилася у новий вимір бойових дій **–** кіберпростір – і стала важливою складовою системи кібердій – кіберрозвідкою, під якою розуміють процес добування усіма наявними технічними засобами розвідки (космічної, повітряної, радіоелектронної, мережної, програмно-комп'ютерної, розвідки систем управління тощо) й засобами розвідки з відкритих джерел (OSINT) інформації, наявної в кіберпросторі про протилежну сторону, а також подальше її оброблення, що здійснюється за єдиним задумом і планом із метою викриття процесів управління, які протікають у кібернетичних системах під час їхнього функціонування та формування вихідних даних для здійснення заходів кіберзахисту та кібервпливу на фізичні, соціальні, інформаційні й інші кібернетичні системи (Даник, Воробієнко, & Чернега, 2019).

ISSN 2707-1758

Однією з форм кіберрозвідки є розвідка з відкритих джерел – комп'ютерна розвідка, яка здійснюється для пошуку й добування розвідувальної інформації, у тому числі, виявлення й аналіз об'єктів кібербезпеки для прогнозування можливих проявів кіберзагроз та їхніх наслідків. Основними джерелами отримання інформації для OSINT є відкриті електронні джерела в інтернеті, соціальних мережах і месенджерах.

Відповідно до цього, актуальним є наукове завдання щодо розроблення ефективних методів виявлення й аналізу об'єктів кібербезпеки екстрагуванням фактографічних даних про них із великих масивів текстової інформації.

Традиційні методи аналізу тексту, які використовують нині, мають свої обмеження, особливо коли йдеться про оброблення й аналіз великих за обсягом даних, що мають складну структуру.

Розв'язати цю проблему можна, застосувавши сучасні ІТ, такі як ВММ і ГШІ, які дозволяють ефективно обробляти й аналізувати текстові дані великого обсягу та складної структури.

Метою статті є розроблення нових методик екстрагування об'єктів кібербезпеки з великих за обсягом і складних за структурою текстових документів, розміщених у відкритих електронних джерелах інтернету та соціальних мережах із використанням ВММ та ГШІ для ефективного розв'язання задач комп'ютерної розвідки фахівцем із кібербезпеки для відпрацювання ним ефективних стратегій захисту від кіберзагроз.

Для досягнення мети дослідження розв'язувались такі часткові завдання:

1. Розроблення методики виявлення суб'єктів кібербезпеки засобами ГШІ.
2. Розроблення методики екстрагування а́кторів кібервійни з використанням ГШІ.

Суть першого завдання полягає у використанні системи ГШІ, наприклад, ChatGPT, для екстрагування понять і зв'язків між ними, шляхом звернення до неї зі змістовними запитами (промптами), та розробці алгоритму для формування мереж взаємозв'язків між суб'єктами кібербезпеки на основі екстрагованих даних.

Друга задача пов'язана з визначенням об'єктів кібербезпеки – а́кторів кібервійни на основі даних, отриманих у результаті інформаційно-пошукових запитів (ІПЗ) до агрегаторів інформації та формування промптів до ГШІ, та, відповідно до цього, розробити алгоритм для побудови мережі а́кторів у формі графа, який враховує взаємозв'язки між ними.

Огляд літератури. У науковій літературі широко обговорюють методи аналізу текстових даних. Наприклад, у статті (Yi et al., 2020) розглянуто модель RDF-CRF розпізнавання іменованих об'єктів безпеки на основі регулярних виразів і словника відомих об'єктів, а також умовних випадкових полів у поєднанні з чотирма шаблонами ознак. Ця модель, на основі правил, дозволяє здійснювати зіставлення об'єктів безпеки з необхідною точністю в простих ситуаціях. Словник відомих об'єктів застосовують для вилучення загальних і специфічних об'єктів безпеки, а екстрактор на основі CRF використовує ідентифіковані об'єкти за допомогою екстракторів на основі правил і словника для подальшого покращення продуктивності розпізнавання.

У роботі (Halbouni et al., 2022) наведено аналіз ефективності традиційних алгоритмів машинного навчання для розв'язування задач кібербезпеки. Проте наведені у статтях методи мають свої обмеження, особливо під час роботі з великими за обсягом та складною структурою даними. З іншого боку, у теперішній час спостерігається стрімкий розвиток ІТ, які ґрунтуються на досягненнях у сфері штучного інтелекту, зокрема і ВММ, і ГШІ, які призвані для подолання недоліків та обмежень, що властиві для традиційних методів оброблення текстових даних.

У статті (Bayer et al., 2024) розглянуто застосування ВММ для аналізу текстових даних у сфері кібербезпеки. Зокрема, запропоновано використання спеціально адаптованої до сфери кібербезпеки мовної моделі, яка може слугувати основою для розроблення систем кібербезпеки.

Наведено аналіз ефективності застосування ГШІ для розв'язування задач у сфері національної безпеки у праці Hassanin і Moustafa. У цій роботі досліджуються наслідки інтеграції ВММ, аналізується їхній потенціал щодо оброблення інформації, прийняття рішень і оперативності рішень, що приймаються. Проаналізовано переваги застосування ВММ, такі як автоматизація завдань і покращення аналізу даних, ризики і проблеми, пов'язані з конфіденційністю даних і їхньою вразливістю до атак з боку супротивника. Зроблено висновок про доцільність поєднання застосування ВММ із методами теорії прийняття рішень, що може значно полегшити перехід від даних до обґрунтованих рішень, дозволяючи особам, які приймають рішення, швидко отримувати й аналізувати наявну інформацію з меншими витратами людських ресурсів.

У статті (Gao, Zhang, & Han, 2021) обговорено застосування методу розпізнавання іменованих об'єктів для виявлення іменованих сутностей у текстах, що є важливим аспектом у виявленні об'єктів кібербезпеки. Описано різні підходи і методи для розпізнавання іменованих сутностей у сфері кібербезпеки, включаючи підхід на основі правил, підхід на основі словників і підхід на основі машинного навчання, а також проведено аналіз проблем, з якими стикаються дослідження в цій області. Запропоновано майбутні напрями розпізнавання іменованих сутностей у сфері кібербезпеки серед яких: застосування неконтрольованої або напівконтрольованої технології навчання; розробка більш повної онтології кібербезпеки; розробка більш повної моделі глибокого навчання.

Автори роботи Hanks et al. (2022) розглядають використання бібліотеки spaCy для аналізу текстових даних у кібербезпеці. Тут наведено початковий неструктурований корпус інформації, що описує вектори загроз, вразливості та кібератаки з різних відкритих джерел, який використовується для навчання та тестування моделей об'єктів кібербезпеки за допомогою фреймворку spaCy та вивчення методів самонавчання для автоматичного розпізнавання об'єктів кібербезпеки.

У статті (Alam et al., 2022) проаналізовано ефективність бібліотеки Flair у розпізнаванні іменованих сутностей. Описано бібліотеку CyNER, з відкритим вихідним кодом на мові python для розпізнавання іменованих об'єктів у сфері кібербезпеки, яка поєднує в собі трансформаційні моделі для вилучення об'єктів, пов'язаних із кібербезпекою, евристики для вилучення різних індикаторів компрометації, а також загальнодоступні моделі для загальних типів об'єктів.

Застосування методу тематичного моделювання для аналізу текстових даних, що належать до сфери кібербезпеки, обговорено в роботі (Piyush, & Okamura,

2021). Запропонований метод дозволяє виявляти тематичні зв'язки між різними об'єктами кібербезпеки,

У статті (Lande, Puchkov, & Subach, 2022) запропоновано інформаційну технологію вилучення концептів із текстів повідомлень мережних джерел, що належать до предметної області кібербезпеки. Ці концепти фільтруються за статистичними характеристиками та ранжуються. Розглянуто питання створення, кластеризації та візуалізації мережі концептів та їхніх взаємозв'язків.

У дослідженні (Lande, Puchkov, & Subach, 2020) запропоновано й обґрунтовано підходи до побудови системи моніторингу й аналізу соціальних медіа з питань кібербезпеки, які базуються на концепції оброблення великих обсягів даних, складних мереж, добування знань із текстових масивів. Основна ідея створення цієї системи – одночасне застосування методів і засобів інформаційного пошуку, аналізу даних та агрегування інформаційних потоків.

Питанням формування в реальному часі моделей предметних областей і дайджестів на основі автоматичного аналізу великої кількості повідомлень із соціальних мереж, присвячено публікацію (Lande et al., 2020]. Запропоновано метод кластерного аналізу, який базується на оцінюванні дискримінантного значення термів, новизна якого полягає у використанні найбільш значущих дискримінантних значень як центроїдів для визначення кластерів.

Проте проведений аналіз вказує на відсутність ефективних методів, які повною мірою задовольняли б потреби користувачів – фахівців сфери кібербезпеки щодо екстрагування об'єктів кібербезпеки з великих масивів текстових документів, що мають складну структуру.

Отже, зважаючи на те, що існуючі методи мають суттєві обмеження для роботи з великими за обсягом масивами текстових даних з одного боку, та сучасні досягнення у цій сфері та сфері штучного інтелекту, з іншого, стає доцільним і перспективним розроблення та застосування новітніх ІТ, які ґрунтуються на нових методах екстрагування об'єктів з електронних джерел і соціальних мереж, зокрема й у сфері кібербезпеки, на основі застосуванні ВММ і ГШІ.

Методи

Виділення іменних сутностей – об'єктів кібербезпеки є важливим для ідентифікації можливих кіберзагроз і розкриття кіберзлочинів, виявлення і розслідування діяльності злочинних хакерських угруповань тощо.

Результати виділення іменних сутностей можуть бути використані для подальшого їхнього аналізу у контексті кібербезпеки. Є кілька методів та інструментів, які можна використовувати для виокремлення іменних сутностей:

1. Аналіз вебсторінок:
   - використання інструментів для вилучення текстової інформації з вебсторінок відповідно до тег веброзмітки;
   - отримання метаданих (наприклад, EXIF-даних із фотографій), які можуть містити іменні сутності.
2. Аналіз соціальних мереж:
   - застосування інструментів для виявлення згадок конкретних імен, компаній або інших сутностей на публічних сторінках;
   - вивчення зв'язків між різними сутностями через аналіз друзів, фоловерів тощо.
3. Аналіз електронної пошти:
   - використання інструментів для аналізу публічної інформації, яка може містити імена, адреси, телефонні номери тощо.
4. Методи роботи з неструктурованим текстом:
   - використання шаблонів (регулярних виразів – regular expressions, RegExp);
   - застосування алгоритмів оброблення текстів природною мовою (Natural Language Processing, NLP) для виділення імен, назв організацій тощо з текстової інформації;
   - автоматична ідентифікація іменованих сутностей – Named Entity Recognizer (NER): spaCy, Natural Language Toolkit (NLTK), Stanford Named Entity Recognizer;
   - використання інструментів для розпізнавання іменованих сутностей (осіб, місць, організацій, а́кторів тощо) в тексті, що може вказувати на сталі словосполучення.
5. Аналіз коду:
   - аналіз вихідного коду програм (зокрема, коментарів) для виявлення імен та інших інформаційних сутностей, пов'язаних із розробниками чи компаніями сфери кібербезпеки.
6. Застосування ВММ і ГШІ:
   - формування спеціальних запитів (промптів) до систем ГШІ, таких як ChatGPT, Gemini, Groq тощо для виявлення відповідних іменованих сутностей сфери кібербезпеки.
   - Для виявлення іменованих сутностей можуть використовуватися такі інструментальні засоби OSINT:
   - бази даних кіберзлочинців, такі як SANS Internet Storm Center, The Honeynet Project тощо;
   - інструменти соціальних мереж, такі як Social Mention , BuzzSumo тощо;
   - системи аналізу журналів роботи систем, такі як Splunk, LogRhythm тощо;
   - інструменти OSINT, такі як Maltego, OSINT Framework тощо.

Методика виявлення суб'єктів кібербезпеки засобами генеративного штучного інтелекту. Для здійснення дієвої аналітики результатів добування інформації, запропоновано методику екстрагування іменованих сутностей – назв хакерських угруповань та їхніх контекстуальних зв'язків із текстів повідомлень електронних мережних джерел, що стосуються предметної сфери кібербезпеки, а також формування мереж їхніх взаємозв'язків і змістовного аналізу цих мереж засобами ГШІ, зокрема і системи ChatGPT, яка дозволяє отримувати результати змістовних запитів (промптів) через програмний інтерфейс (Application Programming Interface, API).

Екстрагування понять і зв'язків між ними здійснюється за допомогою звернення до системи ГШІ змістовними промптами, що належать до заздалегідь відібраних текстів повідомлень із вебпростору і соціальних мереж.

Суть методики така.

На першому кроці для отримання інформаційного масиву публікацій щодо кібербезпеки визначають необхідний період (наприклад, місяць до і місяць після початку події у кіберпросторі) й опрацьовують тематичні запити до системи OSINT, як-от:

– кібервійна в Україні:

- (кібератак~/3/украї)|(хакер~/3/атак~/2/украї)|(кибератак~/3/украин)| (хакер~/3/атак~/2/украин)
- (hack~/3/ukrain)|(cyber~attack~/3/ukrain)|(cyberattack~/3/ukrain)

На другому кроці для кожного з отриманих документів застосовують промпт до системи ChatGPT, результати якого надходять до програм через API й агрегуються для подальшого формування мереж (рис. 1).

ISSN 2707-1758

Надай список назв хакерських угруповань з тексту без пояснень у Вигляді переліку. Текст:...

Рис. 1. Приклад промпта до системи ChatCPT
для отримання списку назв хакерських угруповань

На третьому та четвертому кроці здійснюють аналіз відібраної мережі та її візуалізацію (рис. 2).

Формальна постановка задачі й алгоритм її розв'язання виглядає так.

Дано:

множина документів $D = \{d_1, d_2, ..., d_N\}$ – набір документів, отриманих за допомогою OSINT-систем на основі тематичних запитів; H – множина назв хакерських угруповань, які потрібно виявити з текстів документів; C – множина контекстуальних зв'язків між хакерськими угрупованнями, що екстрагуються з текстів документів.

Необхідно: відібрати з множини текстових документів D суб'єкти кібербезпеки та сформувати і візуалізувати мережу їхніх взаємозв'язків.

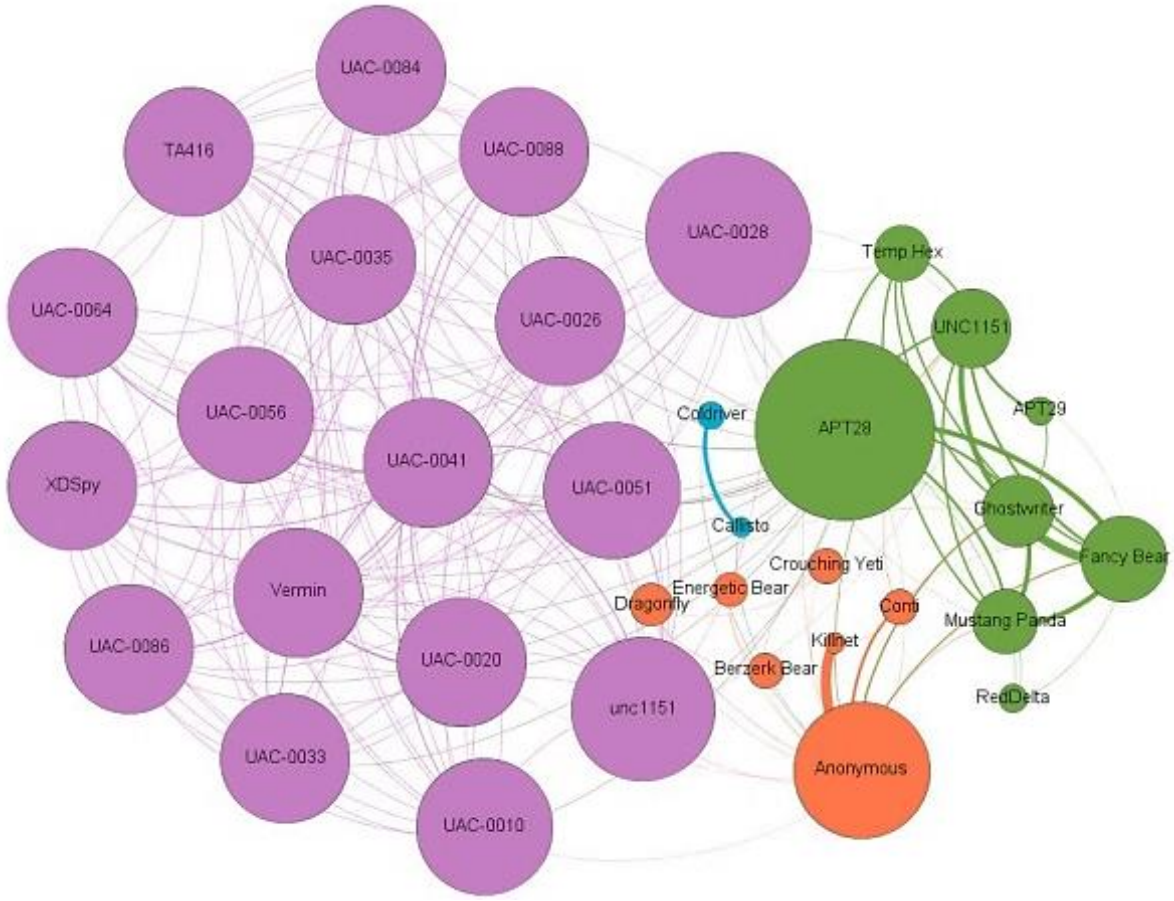

Рис.2. Фрагмент мережі злочинних хакерських угруповань,
пов'язаних із російсько-українською кібервійною

Алгоритм розв'язку

Крок 1. Для кожного набору тематичних запитів $q \in Q$ (напр., запитів щодо кібератак в Україні), отримати множину документів $D = \{d_1, d_2, ..., d_N\}$, що відповідають цим запитам:

$$D = \bigcup_{q \in Q} OSINT(q), \quad (1)$$

де $OSINT(q)$ – функція, що повертає множину документів за тематичним запитом q.

Крок 2. Екстрагування назв хакерських угруповань. Для кожного документа $d \in D$ формується відповідний промпт до системи ГШІ (напр., ChatGPT) для екстракції назв хакерських угруповань:

$$H(d) = GenAI(prompt, d), \quad (2)$$

де $H(d)$ – множина хакерських угруповань, екстрагованих із документа d; prompt – змістовний запит до системи GenAI.

Крок 3. Побудова мережі зв'язків. На основі екстрагованих назв хакерських угруповань, для кож-

ISSN 2707-1758

ного документа сформувати множину контекстуальних зв'язків:

$$C(d) = \{(h_i, h_j) \mid h_i, h_j \in H(d)\}, \quad (3)$$

де $C(d)$ – множина парних зв'язків між хакерськими угрупованнями з документа d.

Загальна множина зв'язків для всіх документів визначається як

$$C = \bigcup_{d \in D} C(d). \quad (4)$$

Крок 4. Візуалізація та аналіз мережі. Мережа зв'язків хакерських угруповань, побудована на основі множини H і множини зв'язків C, може бути представлена у вигляді графа $G = (H, C)$, де: H – множина вершин (хакерських угруповань); C – множина ребр (контекстуальних зв'язків між угрупованнями).

Відповідно до наведено вище, обчислювальну складність алгоритму можна оцінити, оцінивши обчислювальну складність його кроків.

Обчислювальна складність кроку формування інформаційного масиву публікацій залежить від кількості запитів Q та кількості документів N. Її можна оцінити як $O(|Q| \times N)$.

Обчислювальна складність кроку екстрагування назв хакерських угруповань оцінюється з таких міркувань: для кожного документа d здійснюється звернення до системи GenAI. Якщо t_{AI} – середній час оброблення одного запиту до системи ГШІ, то загальна обчислювальна складність цього етапу складатиме: $O(N \times t_{AI})$.

Обчислювальна складність побудови мережі зв'язків розраховується таким способом: для кожного документа d екстрагуються зв'язки між угрупованнями. Якщо в документі d знайдено $|H(d)|$ хакерських угруповань, то кількість зв'язків між ними оцінюється як $O(|H(d)|^2)$. Тоді загальна складність процесу побудови мережі буде така: $O(\sum_{d \in D} |H(d)|^2)$.

У свою чергу, обчислювальна складність кроку візуалізації та аналізу мережі залежить від кількості вершин $|H|$ та ребер $|C|$ у графі $G = (H, C)$. У найгіршому випадку, складність візуалізації та аналізу можна оцінити як $O(|H| + |C|)$.

З урахуванням наведеного, загальна складність алгоритму дорівнюватиме

$$O(|Q| \times N + N \times t_{GPT} + \sum_{d \in D} |H(d)|^2 + |H| + |C|). \quad (5)$$

Отже, можна зробити висновок про те, що запропонована методика й алгоритм її реалізації дозволяють ефективно екстрагувати й аналізувати взаємозв'язки між хакерськими угрупованнями на основі даних із текстових джерел, використовуючи засоби ГШІ.

Методика екстрагування а́кторів кібервійни засобами генеративного штучного інтелекту. Для визначення а́кторів, які мають відношення до кібервійни, запропоновано методику аналізу відібраних документів, доступних в електронних джерелах інтернету та соціальних мережах, шляхом застосування системи ГШІ.

Формально цю задачу можна сформулювати так.

Дано:

множина документів $D = \{d_1, d_2, ..., d_N\}$ – набір текстових документів, відібраних з електронних джерел інтернету та соціальних мереж;

$K = \{k_1, k_2, ..., k_m\}$ – набір ключових слів, обов'язкових для наявності їх у документі для подальшого аналізу; $N = \{(n_1, s_1), (n_2, s_2), ..., (n_p, s_p)\}$ – множина пар імен і прізвищ, екстрагованих із текстів електронних документів; $f_{\min}$ – мінімальна кількість поява імені та прізвища для збереження під час аналізу (мінімальний поріг частотності).

Необхідно: побудувати мережу а́кторів кібервійни та взаємозв'язків між ними.

Суть запропонованої методики розв'язання сформульованої задачі така.

На першому кроці методики формується запит до пошукової системи-агрегатора, наприклад, системи "КіберАгрегатор" (Ланде, Субач, & Соболєв, 2019) з ключовими словами, які мають міститися в документі для подальшого аналізу. Після знаходження достатньої кількості текстових повідомлень, вони фільтруються за допомогою програмного коду, згенерованого ГШІ (напр., ChatGPT), для пошуку пар понять, які мають формат "Ім'я Прізвище".

На наступному кроці розв'язується завдання фільтрації наданих словосполучень. Інформація конвертується у файл формату PDF і формується запит (промпт) до системи ГШІ, наприклад, ChatGPT з наступним формулюванням (рис. 3).

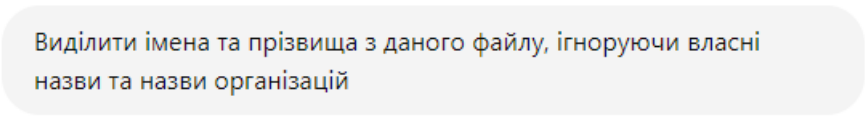

Рис. 3. Приклад промпта до системи ГШІ для фільтрації наданих словосполучень

Під час проведення експерименту з понад 30 000 словосполучень виділено близько 700 імен. Для оптимізації побудови мережі був розроблений програмний код мовою програмування Python за допомогою якого здійснювався підрахунок кількості повторень і вилучення всіх появ сутностей, окрім першої, а також вилучення слів, які згадуються кількість разів, що менша заданого порогового значення (у проведеному експерименті – 3), оскільки вони не мають статистичної важливості й лише перевантажують мережу зайвою інформацією.

За допомогою системи ГШІ (у нашому дослідженні – ChatGPT) створюються зв'язки між а́кторами кібервійни (рис. 4).

ISSN 2707-1758

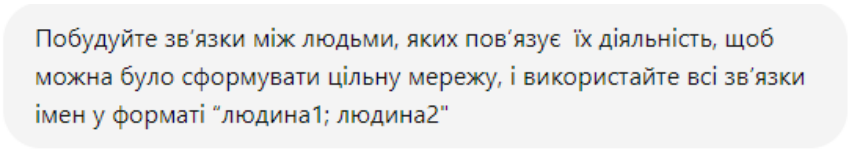

Рис. 4. Приклад промпта до системи ГШІ для створення зв'язків між а́кторами кібервійни

На третьому кроці, після встановлення зв'язків між учасниками в заданому форматі, отримана інформація записується у CSV-файл.

На четвертому, заключному кроці, використовуть спеціальний програмний застосунок і створюють графічне представлення мережі а́кторів кібервійни та їхніх зв'язків (рис. 5).

Побудована мережа а́кторів у формі графа надає важливий інструмент для аналізу та візуалізації взаємодії між ними. Проте варто зауважити, що під час застосування систем ГШІ потрібна експертна перевірка для уточнення складу а́кторів та їхніх зв'язків.

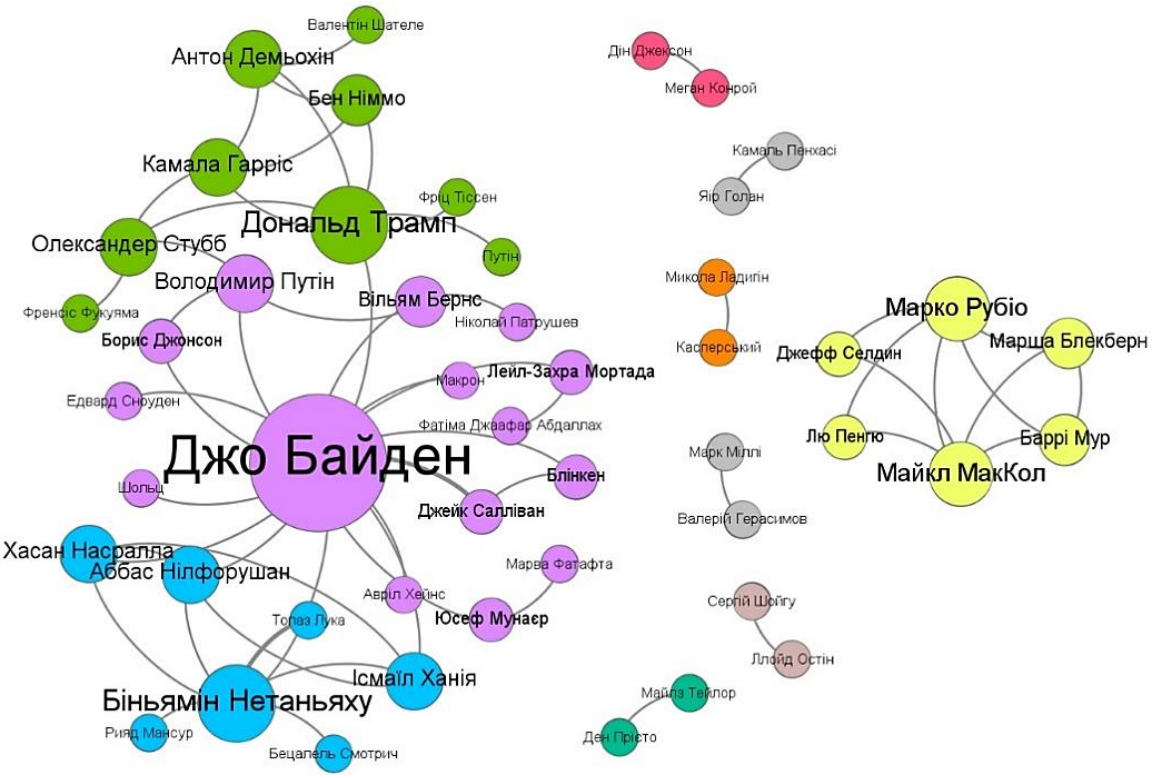

Рис. 5. Фрагмент мережі а́кторів кібервійни ВИПРАВИТИ НА РИС. – БЕНЬЯМІН НетаньяГу

Алгоритм розв'язання задачі

Крок 1. Сформувати запит до пошукової системи-агрегатора з використанням ключових слів K:

$$Query(K) = aggregate\_search(K), \quad (6)$$

де $aggregate\_search(K)$ – функція, що виконує пошук документів *D*, які містять усі ключові слова з множини *K*.

Крок 2. Екстрагувати імена та прізвища. З відібраних документів D екстрагувати пари імен і прізвищ, що мають формат "Ім'я Прізвище", за допомогою системи ГШІ:

$$N = \{(n,s) \mid (n,s) \in extract\_names(d), d \in D\}, \quad (7)$$

де $extract\_names(d)$ – функція, яка використовує систему ГШІ для вилучення імен і прізвищ із документа d.

Крок 3. Фільтрувати й оптимізувати список імен. На цьому кроці застосовується фільтрація отриманих імен для відкидання власних назв і назв організацій, а також для вилучення менш частотних слів. Фільтрація власних назв виконується системою ГШІ для відокремлення імен від власних назв і назв організацій.

Фільтрація отриманих пар імен за частотністю здійснюється так. Для кожної пари $(n,s) \in N$ підраховують кількість її появ:

$$f(n,s) = \sum_{d \in D} count(n,s,d), \quad (8)$$

де $count(n,s,d)$ – кількість появ пари імен (n,s) у документі d.

Після підрахунку вилучають пари, для яких $f(n,s) < f_{\min}$:

$$N' = \{(n,s) \mid (n,s) \in N, f(n,s) \geq f_{\min}\}. \quad (9)$$

Крок 4. Побудувати мережу зв'язків між а́кторами кібервійни. На цьому кроці визначають зв'язки між

ISSN 2707-1758

а́кторами кібервійни на основі їхньої наявності в документах або контекстних взаємодіях:

$$C = \{(a_1, a_2) \mid a_1, a_2 \in N', connected(a_1, a_2, D)\}, \quad (10)$$

де $connected(a_1, a_2, D)$ – функція, що визначає зв'язок між акторами a_1 та a_2 на основі їхньої наявності в одному або кількох документах, або на основі контексту, визначеного системою ГШІ.

Крок 5. Візуалізувати мережу а́кторів. Зібрана інформація записується у файл формату CSV, після чого будується графічне представлення мережі а́кторів кібервійни. Мережу а́кторів G представлено у вигляді графа $G = (V, E)$, де $V = N'$ – множина вузлів, що відповідають а́кторам; $E = C$ – множина зв'язків між а́кторами.

Граф G візуалізують із використанням програмного забезпечення для аналізу соціальних мереж.

Обчислювальна складність наведеного алгоритму буде така.

- обчислювальна складність кроку формування запиту до пошукової системи залежить від кількості ключових слів $|K|$ і кількості знайдених документів N;
- обчислювальна складність кроку екстрагування імен залежить від кількості документів N та обсягу тексту в кожному документі M_d. Отже, загальна складність цих кроків буде $O(N \times M_d)$;
- обчислювальна складність кроку фільтрації та оптимізації складається зі складності підрахунку частотності: $O(N \times M_d)$ та складності відбору значущих пар: $O(p)$, де p – кількість пар (n, s);
- обчислювальна складність кроку побудови мережі зв'язків визначається кількістю а́кторів $|N'|$ та кількістю зв'язків між ними $|C|$. Тоді загальна складність цього кроку буде $O(|N'|^2)$.

Відповідно до наведеного, загальна складність алгоритму з урахуванням усіх кроків дорівнюватиме

$$O(N \times M_d + p + |N'|^2). \quad (11)$$

Реалізована на практиці запропонована методика дозволяє ефективно визначати а́кторів кібервійни з використанням системи ГШІ, а також формувати та візуалізувати мережу їхніх взаємодій.

Дискусія і висновки

У статті ми представили методики екстрагування об'єктів кібербезпеки з використанням ВММ і ГШІ. Основну увагу приділяли розробленню підходів та алгоритмів до виявлення фактографічних даних про об'єкти кібербезпеки з текстових документів. Результати дослідження демонструють ефективність запропонованих підходів і можливість їхнього застосування на практиці для розв'язання задач сфери кібербезпеки.

Використання системи ГШІ, такої як ChatGPT, дозволяє екстрагувати поняття та зв'язки між ними за допомогою звернення до системи із змістовними промптами. Проведене дослідження показує, що вказаний підхід може бути застосованим для ефективного оброблення й аналізу електронних текстів із вебпросторе та соціальних мереж, дозволяючи формувати мережі взаємозв'язків між суб'єктами кібербезпеки.

Запропонована методика екстрагування а́кторів кібервійни дозволяє визначати їх на основі даних, отриманих унаслідок інформаційно-пошукових запитів до агрегаторів інформації та формування промптів до системи ГШІ. Результатом є побудована мережа а́кторів у формі графа, що враховує взаємозв'язки між ними.

Проведені експерименти показують, що отримані результати дозволяють досягти високої ефективності у виявленні й аналізі об'єктів кібербезпеки, а використання ВММ і ГШІ уможливлює подолання обмежень традиційних методів і забезпечує високу точність і швидкість оброблення текстових даних великого обсягу та складної структури.

Реалізація на практиці отриманих результатів може стати важливим інструментом для фахівців сфери кібербезпеки, допомагаючи їм у розробленні ефективних стратегій захисту від кіберзагроз.

Перспективи подальшого розвитку цієї сфери включають удосконалення алгоритмів екстрагування, а також інтеграцію їх з іншими системами кібербезпеки для отримання більш повної картини кіберзагроз.

Внесок авторів: Олександр Пучков – формальний аналіз, методологія; Дмитро Ланде – програмне забезпечення, валідація даних; Ігор Субач – концептуалізація, написання (перегляд і редагування).

Список використаних джерел

Даник, Ю. Г, Воробієнко, П. П., & Чернега, В. М. (2019). *Основи кібербезпеки та кібероборони.* Одеська національна академія зв'язку імені О. С. Попова.

Ланде, Д., Субач, І., & Соболєв А. (2019). Комп'ютерна програма контент-моніторингу соціальних мереж з питань кібербезпеки – КіберАгрегатор ("КіберАгрегатор"). *Свідоцтво про реєстрацію авторського права на твір № 92744.* Міністерство економіки.

Alam, T., Bhusal, D., Park, Y., & Rastogi, N. (2022). CyNER: A Python Library for Cybersecurity Named Entity Recognition. https://doi.org/10.48550/arXiv.2204.05754

Bayer, M., Kuehn, P., Shanehsaz, R., & Reuter, C. (2024). CySecBERT: A Domain-Adapted Language Model for the Cybersecurity Domain. *ACM Transactions on Privacy and Security*, 27(2), 1–20. https://doi.org/10.1145/3652594

Lande, D., Subach, I., Puchkov, O., & Soboliev, A. (2020). A Clustering Method for Information Summarization and Modelling a Subject Domain. *Information & Security*, 50(1), 79–86. https://doi.org/10.11610/isij.5013

Gao, C., Zhang, X., & Han, M. (2021). A review on cyber security named entity recognition. *Front Inform Technol Electron Eng*, 1153–1168. https://doi.org:/10.1631/FITEE.2000286

Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). Machine Learning and Deep Learning Approaches for CyberSecurity. *IEEE Access*, 10, 19572–19585. https://doi.org/10.1109/ACCESS.2022.3151248

Hanks, C., Maiden, M., Ranade, P., Finin, T., & Joshi, A. (2022). Recognizing and extracting cybersecurity entities from text. *In Workshop on Machine Learning for Cybersecurity. International Conference on Machine Learning.* https://www.researchgate.net/publication/361618891_Recognizing/_and_Extracting_Cybersecurity_Entities_from_Text

Lande, D., Puchkov, O., & Subach, I. (2020). Система аналізу великих обсягів даних з питань кібербезпеки із соціальних медіа. *Collection "Information Technology and Security*, 8(1), 4–18. https://doi.org/10.20535/2411-1031.2020.8.1.217993

Lande, D., Puchkov, O., & Subach, I. (2022). Method of Detecting Cybersecurity Objects Based on OSINT Technology. *In XXII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2022), Vol. 3503* (pp. 115–124). State University of Information and Communication Technologies. https://ceur-ws.org/Vol-3503/paper11.pdf

Piyush, G., & Okamura, K. (2021). Investigating Cybersecurity News Articles by Applying Topic Modeling Method. *In International Conference on Information Networking (ICOIN)* (pp. 432–438). IEEE.

Yi, F., Jiang, B., Wang, L., & Wu, J. (2020). Cybersecurity Named Entity Recognition Using Multi-Modal Ensemble Learning. *IEEE Access*, 8, 63214–63224. https://doi.org/10.1109/ACCESS.2020.2984582

References

Alam, T., Bhusal, D., Park, Y., & Rastogi, N. (2022). CyNER: A Python Library for Cybersecurity Named Entity Recognition. https://doi.org/10.48550/arXiv.2204.05754

ISSN 2707-1758

Bayer, M., Kuehn, P., Shanehsaz, R., & Reuter, C. (2024). CySecBERT: A Domain-Adapted Language Model for the Cybersecurity Domain. *ACM Transactions on Privacy and Security*, 27(2), 1–20. https://doi.org/10.1145/3652594

Danyk, Y. G., Vorobienko, P. P., & Chernega, V. M. (2019). *Fundamentals of Cybersecurity and Cyberdefense.* O. S. Popov Odessa National Academy of Telecommunications [in Ukranian].

Lande, D., Subach, I., & Soboliev, A. (2019). Computer Program for Content Monitoring of Social Networks on Cybersecurity Issues – CyberAggregator ("CyberAggregator"). *Copyright registration certificate No 92744.* Ministry of Economy [in Ukranian].

Lande, D., Subach, I., Puchkov, O., & Soboliev, A. (2020). A Clustering Method for Information Summarization and Modelling a Subject Domain. *Information & Security*, 50(1), 79–86. https://doi.org/10.11610/isij.5013

Gao, C., Zhang, X., & Han, M. (2021). A review on cyber security named entity recognition. *Front Inform Technol Electron Eng*, 1153–1168. https://doi.org:/10.1631/FITEE.2000286

Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). Machine Learning and Deep Learning Approaches for CyberSecurity. *IEEE Access*, 10, 19572–19585. https://doi.org/10.1109/ACCESS.2022.3151248

Hanks, C., Maiden, M., Ranade, P., Finin, T., & Joshi, A. (2022). Recognizing and extracting cybersecurity entities from text. *In Workshop on Machine Learning for Cybersecurity. International Conference on Machine Learning.* https://www.researchgate.net/publication/361618891_Recognizing/_and_Extracting_Cybersecurity_Entities_from_Text

Lande, D., Puchkov, O., & Subach, I. (2020). Система аналізу великих обсягів даних з питань кібербезпеки із соціальних медіа. *Collection "Information Technology and Security*, 8(1), 4–18. https://doi.org/10.20535/2411-1031.2020.8.1.217993

Lande, D., Puchkov, O., & Subach, I. (2022). Method of Detecting Cybersecurity Objects Based on OSINT Technology. *In XXII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2022), Vol. 3503* (pp. 115–124). State University of Information and Communication Technologies.https://ceur-ws.org/Vol-3503/paper11.pdf

iyush, G., & Okamura, K. (2021). Investigating Cybersecurity News Articles by Applying Topic Modeling Method. *In International Conference on Information Networking (ICOIN)* (pp. 432–438). IEEE.

Yi, F., Jiang, B., Wang, L., & Wu, J. (2020). Cybersecurity Named Entity Recognition Using Multi-Modal Ensemble Learning. *IEEE Access*, 8, 63214–63224. https://doi.org/10.1109/ACCESS.2020.2984582

Отримано редакцією журналу / Received: 17.10.24
Прорецензовано / Revised: 27.10.24
Схвалено до друку / Accepted: 05.11.24

Olexandr PUCHKOV, PhD (Philos.), Prof.
ORCID ID: 0000-0002-8585-1044
e-mail: iszzi@iszzi.kpi.ua
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine

Dmytro LANDE, DSc (Engin.), Prof.
ORCID ID: 0000-0003-3945-1178
e-mail: dwlande@gmail.com
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine

Ihor SUBACH, DSc (Engin.), Prof.
ORCID ID: 0000-0002-9344-713X
e-mail: igor_subach@ukr.net
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine

METHODS OF EXTRACTING CYBERSECURITY OBJECTS FROM ELECTRONIC SOURCES USING ARTIFICIAL INTELLIGENCE

Background. ***The rapid development of information technology (IT) has led to new threats and challenges in the field of cybersecurity. Cyber warfare has become a reality and a real problem for states, organizations and individual users of cyberspace. Ukraine is taking a number of measures to develop a system of cyber actions in cyberspace, which include a set of interconnected subsystems of cyber intelligence, cyber defense, cyber influence and cyber counterintelligence. One of the forms of cyber intelligence is open-source computer intelligence (OSINT), which is used to search for and obtain intelligence information, including the identification and analysis of cybersecurity objects to predict possible manifestations of cyber threats and their consequences. This requires the development of effective methods for detecting and analyzing cybersecurity objects by extracting factual data on cybersecurity objects from large amounts of unstructured textual information.***

Methods. ***The paper investigates artificial intelligence technologies, in particular, large language models (LLM) and generative artificial intelligence (GenAI) in the context of their application to solve the problems of computer intelligence of cybersecurity objects from open electronic sources and social networks.***

Results. ***As a result of the study, in order to carry out an effective analysis of the results of information extraction, a methodology for extracting named entities - the names of hacker groups and their contextual connections from the texts of messages of electronic network sources related to the subject area of cybersecurity, as well as the formation of networks of their interconnections and a substantive analysis of these networks is proposed. To identify the actors involved in cyber warfare, the author proposes a methodology for analyzing selected documents available in electronic sources on the Internet and social networks. Both methods are based on the use of artificial intelligence.***

Conclusions. ***The results of the study demonstrate the effectiveness of the proposed approaches and the possibility of their practical application in solving cybersecurity problems. The proposed methods can be an important tool for cybersecurity professionals to develop effective strategies to protect against cyber threats.***

Keywords: ***cyber warfare, cybersecurity; generative artificial intelligence; large language models; Internet; open electronic sources; social networks, text analysis; objects of cyber warfare.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.

UDC: 004.8+004.056/.57:005.334
DOI: https://doi.org/10.17721/ISTS.2024.8.42-48

Serhii DAKOV, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0001-9413-3709
e-mail: serhii.dakov@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Dmytro MANKOVSKYI, Student
ORCID ID: 0009-0004-5053-2432
e-mail: dimamankovskyi@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Ivan BILOKON, PhD (Engin.), Assoc. Prof.
ORCID ID: 0009-0008-3074-7064
e-mail: ivan.bilokon@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ARTIFICIAL INTELLIGENCE SYSTEMS IN CYBER SECURITY AND THEIR CAPABILITIESFRONT MODERN CYBER THREATS

Background. ***In recent years, the level of cybercrime has grown rapidly. The complexity and diversity of these threats has forced organizations to prioritize advanced cybersecurity solutions, including the use of artificial intelligence technologies that can quickly analyze data to identify potential threats and anomalies. By 2027, the AI-based cybersecurity market is expected to exceed $46 billion. However, as AI strengthens and refines defenses, cybercriminals are adapting by exploiting vulnerabilities and even using AI to enhance attacks. This dual use of AI underscores the need for balanced and intelligent strategies that combine the predictable capabilities of AI with human knowledge and talent.***

Methods. ***My Research highlights effective risk prevention strategies, including promoting a security-aware culture, implementing strong passwords and two-factor authentication, regularly assessing and updating systems, enhancing firewalls, and adhering to cybersecurity regulations. AI proves valuable in threat detection and response, giving companies a competitive edge, though it raises concerns about reducing human roles in security tasks.***

Results. ***The research indicates that AI positively impacts cybersecurity by enabling faster detection and response to threats, allowing organizations to proactively identify and address vulnerabilities. Companies that integrate AI into their cybersecurity strategies gain an advantage in managing complex cyber threats. However, concerns persist about AI's dual-use nature, as it could also be leveraged by cybercriminals for advanced attacks. This potential for AI to operate independently raises questions about the diminishing role of human oversight. Ultimately, the findings stress the need for a balanced approach: while AI is essential for modern cybersecurity, human involvement remains crucial. Continuous adaptation and a blend of technological and human expertise are necessary to protect critical infrastructure and data.***

Conclusions. ***To summarise, the rapid growth of cybercrime underscores the necessity for robust cybersecurity measures to protect sensitive information and ensure operational integrity. Artificial Intelligence is becoming crucial in enhancing cybersecurity through advanced threat detection, pattern recognition, and predictive analysis. While AI offers significant benefits, it can also be exploited by cybercriminals, highlighting the importance of vigilance and innovation in security strategies. Despite advancements in AI, human expertise remains vital for interpreting insights, making informed decisions, and adapting to new threats. A multi-faceted approach, including employee training, regular audits, and strong data protection, is essential for effective cybersecurity. Enhanced cooperation among organizations, governments, and international partners is crucial for developing effective strategies to combat cybercrime. Continued research into AI capabilities and ethical considerations is necessary to address the evolving landscape of cybersecurity threats.***

Keywords: ***artificial intelligence, measures, strategy, cybersecurity, threats, analysis.***

Background

In recent years, artificial intelligence (AI) has had a significant impact on cybercrime and other industries. It is projected that the cost of the cybercrime industry will reach $8 trillion in 2023 and $10.5 trillion by 2025. It is clear that this figure will continue to grow. A robust cybersecurity system is more important than ever, especially now, as cyber professionals and criminals alike strive to stay ahead of the curve in a rapidly changing environment. Researching and preventing potential cybercrimes and their consequences should be a strategic goal for humanity, in which the role of digital technologies is growing every year. As in many other areas, the role of artificial intelligence in cyber security is likely to become more significant (https://www.village.com.ua/village/business/news/305021-tse-reytingkrayin-za-rivnem-kiberbezpeki-/ukrayina-na-25-mu-mistsi, 2024). Companies that implement AI technologies offer significant advantages, providing essential tools for navigating cybersecurity challenges and adapting flexibly to ever-evolving cyber threats. Moreover, some cyber threats are evolving faster than cybersecurity systems. Cyber threats are inherently complex and constantly adapt to the demands of time and technological progress. It is estimated that in 2024, cybercrime will cost the global economy more than a trillion dollars. Many organizations are investing heavily in modern cybersecurity to avoid financial and reputational damage from cyber threats. However, cybercriminals–often professionals in their field–always find new ways to infiltrate secure cybersecurity structures, exploiting vulnerabilities and even the latest technologies. AI is expected to play an increasingly important role in cybersecurity systems, potentially identifying threats autonomously and adjusting security infrastructure accordingly. AI technologies will also analyze security risks using analytical tools and data, providing companies' employees and regular internet users with advice on how to fine-tune security systems. Yet, there is a significant concern that AI may eventually surpass humans and perform all security-related tasks independently. This presents a challenge for humanity, which must maintain its role in IT security. However, technology is developing rapidly, and its impact on security architecture is already apparent today–especially in Ukraine (Impact of AI on

ISSN 2707-1758

Cybersecurity, 2024). Artificial Intelligence Plays a Crucial Role in the science, where AI stimulates the optimization and development of research in new ways. It also facilitates enhanced collaboration with international partners. In cyber security, in addition to the fact that artificial intelligence accelerates the development of modern systems for countering cyber threats, it is also involved in the prevention of risks and threats, as well as helping to develop methods to protect important information. In cyberspace, the risks associated with cyberattacks are constantly rising–new risks are being invented all the time, with each one more dangerous than the last. New attackers emerge with increasingly sophisticated and unconventional ideas. Therefore, it is essential to leverage our knowledge to develop strategies for countering these ever-growing risks to the information space. It is also necessary to harness all the capabilities of artificial intelligence (AI) to achieve a high level of security (https://robotdreams.cc/uk/blog/352-shtuchniy-intelekt-/ne-zahistit-yakshcho-nevikoristovuvati-intelekt-prirodniy-/yak-rozvitok-shi-vplivaye-na-kiberbezpeku, 2024). Risk prevention methods are highly diverse and depend on the specific situation. Figure 2 illustrates the most commonly used methods for ensuring information security. These include employee vigilance, securing data through passwords and two-factor authentication, conducting regular information security audits, updating software, improving security control, training employees to address new challenges, and complying with all relevant laws. AI plays a supporting role in this critical issue by offering advice on how to act in different scenarios. However, it is quite possible that, in the near future, AI technologies will autonomously manage cybersecurity systems, diminishing the role of humans. The influence of AI technologies on the number of cyber incidents is generally considered positive. However, the limitless potential of AI means that it can also be exploited by malicious actors to increase the scale and intensity of cyberattacks. Below are examples of both the positive and negative impacts of AI technologies on cybersecurity systems (https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/the-role-of-ai-in-cybersecurity-/anticipating-and-preventing-attacks, 2024).

Positive Impact:

Advanced Response Systems: Modern AI-powered response systems can reduce the number of cyber incidents and mitigate their financial impact.

Improved Cybersecurity: AI systems enhance cybersecurity, increasing resilience against vulnerabilities.

Threat Forecasting and Network Modeling: AI can predict various cyber threats and simulate network behavior, enabling the development of new countermeasures.

Vulnerability Analysis: AI helps analyze existing cyber threats and identify weaknesses in computer systems.

Support for Human Decision-Making: AI can offer advice to humans on how to respond to emerging threats.

Data Analysis: AI aids in analyzing large datasets and interpreting information that humans might not be able to process, potentially uncovering critical insights about cyber threats.

Minimizing Damage: AI technologies can help minimize losses from cyber threats by implementing systems for threat prevention and prediction.

Negative Impact:

Facilitating Malicious Software: AI can assist attackers in generating more malware and launching cyberattacks at a scale far beyond human capabilities.

Identifying Vulnerabilities: AI can help attackers discover new vulnerabilities and weaknesses in enterprises and software systems that might otherwise go unnoticed.

Autonomous Attacks: AI could autonomously conduct attacks on computer systems without human intervention.

Strategic Advice for Attackers: AI might provide malicious actors with recommendations on how to act more effectively in specific situations to maximize their gains.

Privacy Issues: AI can cause user privacy problems, thereby increasing security risks.

Errors Leading to Cyberattacks: AI systems are not immune to errors, and these mistakes can also lead to cyberattacks.

Actuality. The cybercrime industry is projected to escalate to $10.5 trillion by 2025, highlighting the urgent need for effective cybersecurity measures as financial losses mount. Cyber threats are increasingly sophisticated, with new methods emerging constantly. This dynamic environment demands that organizations stay ahead through adaptive security measures. The integration of AI in cybersecurity is not just a trend but a necessity, as its capabilities enable organizations to analyze threats more efficiently and respond more rapidly. Nations and organizations are recognizing cybersecurity as a critical area of focus, with significant investments in modern technologies to protect against evolving threats. The ongoing importance of human oversight in cybersecurity strategies is gaining recognition, as the combination of AI tools and human expertise proves to be the most effective defense. There is an increasing emphasis on collaboration across industries and borders to share intelligence and resources, creating a united front against cybercriminal activities. As AI technologies advance, ethical considerations regarding their use and potential misuse are becoming a vital part of the conversation in cybersecurity.

Analysis of the sources. The analysis of sources reveals a comprehensive understanding of the current landscape of cybersecurity in Ukraine, particularly in relation to the integration of artificial intelligence (AI). The article detailing Ukraine's cybersecurity ranking provides insights into the country's position globally, indicating the significance of ongoing efforts to combat cyber threats. Furthermore, the discussion on AI applications across various sectors highlights the increasing interest in utilizing AI technologies, not just in cybersecurity but across the entire economy. Artificial intelligence in cyber security has potential in predicting and preventing cyber attacks (https://www.technologyreview.com/2023/05/24/1073395/ai-in-cybersecurity-yesterdays-promise-todays-reality, 2024). This is confirmed by the Security Service of Ukraine, which emphasizes the preventive measures taken to neutralize a significant number of cyber attacks, reflecting the constant threat that the country faces. The impact of artificial intelligence on cyber security requires further research, its advantages in detecting threats and reducing risks are analyzed. In this case, the National Cyber Security Index is indicative, as it provides quantitative data that help assess Ukraine's achievements and capabilities in the field of cyber security and identify areas for improvement and improvement. An important aspect is the distinction between artificial and natural intelligence in cybersecurity, emphasizing the limited capabilities of AI when operating independently of human control. This emphasizes the need and role of human intelligence and knowledge to develop effective information security strategies. In addition, various strategies that can be applied to use AI to

predict and prevent cyber threats are explored. The connection between artificial intelligence and cybersecurity is becoming increasingly close, and this is leading to significant growth in the artificial intelligence cybersecurity sector, emphasizing opportunities for development. Scientific article materials containing research findings on contemporary cybersecurity issues contribute to academic discourse, while analysis of the current state of artificial intelligence in cybersecurity reveals expectations and today's realities.

Methods

My research investigates a variety of risk prevention methods that organizations can adopt to enhance their cybersecurity posture. These methods include promoting a culture of awareness, where employees are trained to recognize potential threats and suspicious activities. Implementing robust measures, such as strong passwords and two-factor authentication, is crucial for securing sensitive information. Additionally, conducting frequent assessments of security practices and systems helps identify and rectify vulnerabilities effectively. Regular software updates are essential to patch known vulnerabilities and protect against new threats. Moreover, improving existing security measures–such as firewalls and intrusion detection systems–can significantly strengthen defenses. Ongoing education and training for employees ensure they stay informed about the latest security challenges and response strategies. Adherence to relevant cybersecurity laws and regulations is vital to mitigate legal risks and maintain trust with stakeholders. The effectiveness of a cybersecurity strategy involving artificial intelligence highlights the importance of adapting approaches to meet specific organizational needs and contexts. This roadmap can significantly improve an organization's overall information security resilience. The effectiveness of specific solutions using artificial intelligence technologies also differs from each other (table 1).

Table 1

The effectiveness and ineffectiveness of ai technologies in cyber security

Effective	Ineffective
Faster, more coordinated, and stronger response to cyber threats	Displacement of humans by AI programs, diminishing the role of individuals in cybersecurity
Forecasting, modeling cyberattacks, and their evolution to develop appropriate response strategies. Analysis of existing cyberattacks	AI misuse by malicious actors could have severe consequences, as malware may autonomously adapt to the latest security systems
Assistance to humans in organizing defenses against cyberattacks. Ability to analyze vast data sets and scan the cyberspace for threats	AI aiding attackers by identifying vulnerabilities in computer systems
Providing qualified assistance to people through AI technologies	AI may also offer qualified assistance to attackers, thereby strengthening them
AI can potentially reduce the number of cyber incidents by improving security protocols and minimizing losses from cyberattacks to zero	On the contrary, AI could autonomously generate cyberattacks, increasing their frequency and making them more damaging

Impact of Artificial Intelligence Technologies on Information Security

Positive Impact:

AI helps people manage security systems more efficiently by automating processes and streamlining operations.

AI's analytical capabilities enable it to forecast potential threats and incidents, helping prevent cyberattacks.

AI allows cybersecurity systems to quickly adapt to new types of threats and changes in infrastructure.

AI takes over routine tasks, allowing humans to focus on more complex and critical activities.

AI provides suggestions for modernizing security architectures and identifying vulnerabilities.

Negative Impact:

Cybercriminals can leverage AI to discover vulnerabilities within security systems.

AI can autonomously generate sophisticated malware capable of bypassing traditional security measures.

In some cases, AI can fully automate cybersecurity processes, minimizing human control and oversight.

AI may sometimes offer incorrect advice on improving security systems, potentially leading to weaker defenses and increased vulnerabilities (https://ela.kpi.ua/items/bf50435a-bfc2-48ef-a400-d31ca2e99b06, 2022) and (Ilchenko, 2024; Mankovskyi, 2024), table 2 & table 3.

Formulas, shown in Table 4 allow us to analyze mathematical and analytical processes in the work of artificial intelligence systems. Making such calculations can improve our cybersecurity strategy.

Table 2

In cyber security, the use of AI technologies is very broad and diverse

Area of Application	Description	Area of Application	Description
Threat Detection and Prevention		AI can analyze malware, phishing attacks, and other cyber threats in real time by analyzing superb datasets and scanning fo anomalies in network traffic	
Intrusion Detection Systems (IDS)		AI enhances IDS by identifying unauthorized access attempts, suspicious behavior, and unknown attack vectors faster than traditional methods	
User Behavior Analytics (UBA)		AI monitors and learns normal user behaviors, helping detect unusual activities that might indicate insider threats or compromised accounts	
Fraud Detection		AI systems analyze transaction patterns to identify fraudulent activities in banking, e-commerce, and other sectors	

ISSN 2707-1758

End of the tabl. 2

Area of Application	Description	Area of Application	Description
Incident Response Automation		AI can automate responses to threats, such as isolating infected systems or blocking malicious IP addresses, reducing response time	
Vulnerability Management		AI tools scan systems and applications for vulnerabilities, helping organizations prioritize patches and mitigate risks effectively	
Predictive Threat Intelligence		AI analyzes historical data to predict future attacks, enabling proactive defense strategies	
Security Operations Center (SOC) Support		AI assists SOC teams by filtering false positives, providing insights, and offering recommendations for threat mitigation	
Endpoint Protection		AI-based endpoint protection platforms prevent malicious files and activities on individual devices, even before known malware signatures are developed	
Phishing Detection and Email Security		AI filters emails and flags phishing attempts by identifying suspicious language patterns, links, or attachments	

Table 3

Examples of AI cyber security solutions

Solution	Description
Darktrace	A platform that uses AI to identify various cyber threats in real-time. It employs the "Enterprise Immune System," modeling network behavior and learning from it to identify new attacks and anomalies. Darktrace also provides tools for tracking, responding to, and analyzing the consequences of security incidents
CylancePROTECT	A program leveraging AI to detect and prevent cyberattacks and risks. Known for its "holistic protection" approach, it identifies and analyzes both known and unknown malware and cyber threats. It supports defense against various cyber threats proactively
IBM QRadar	A Security Information and Event Management (SIEM) platform that uses AI to detect abnormal activities, counter threats, and analyze security events. It combines network monitoring, log analysis, intrusion detection, incident classification, and response mechanisms to mitigate or prevent cybercrime losses
FireEye Helix	A cybersecurity platform offering a wide range of monitoring, analysis, and response functions. It uses AI to detect and analyze attacks from multiple angles and assists in managing incidents, tracking their impacts, and predicting future risks
Splunk Enterprise Security	An extension for the Splunk platform that analyzes security events and detects cyber threats in real-time. It provides continuous monitoring, threat detection, and response protocols. AI technologies are employed to improve the identification and mitigation of risks
Cisco Stealthwatch	A network security monitoring tool that uses traffic analytics and AI to detect and respond to cyber threats in real-time. It enables organizations to analyze network traffic, identify abnormal activities and vulnerabilities, and take appropriate actions to mitigate potential threats
ChatGPT and Other Chatbots	Advanced chatbot technology assists in developing cybersecurity strategies, providing advice on the best approaches, and solving various tasks and issues. These chatbots help identify network vulnerabilities and suggest solutions. However, caution is needed to avoid misuse of such technologies

Table 4

Math Formulas

Formula	Usage
$$P(y=1\mid x)=\frac{1}{1+e^{-(\beta_0+\beta_{1x1}+\ldots+\beta_{nxn})}}$$ (1) Logistic Regression for Binary Classification (Phishing vs. Safe Email)	Used to classify emails or files as malicious or safe. It also outputs a probability between 0 and 1, indicating the likelihood of a given instance being malicious.
$$p(y_i)=\frac{e^{z_i}}{\sum_{j=1}^{n} e^{z_i}}$$ (2) Softmax Function for Multi-Class Classification	Assigns probabilities to multiple classes (e.g., different types of attacks).It ensures that the output is a valid probability distribution over multiple classes
$$P(X_{n+1}=j\mid X_n=i)=p_{ij}$$ (3) Markov Chains for Predicting Attack Patterns	It is used in modeling sequential events, such as user behavior over time, to detect abnormal actions (e.g., lateral movement in cybersecurity)
$$EMA_t=\alpha\cdot x_t+(1-\alpha)\cdot EMA_{t-1}$$ (4) Exponential Moving Average (EMA) for Real-Time Threat Detection	This formula smooths time-series data for anomaly detection in network traffic

End of the tabl. 4

Formula	Usage
$Q(s,a) = r + \gamma \max_{a^I} Q(s^I, a^I)$ (5) Bellman Equation for Reinforcement Learning in Automated Responses	Helps optimize automated threat responses by learning the best action to take in each state. It is used in SOAR (Security Orchestration, Automation, and Response) systems

Fig. 1. Ukraine is 6th in NCSI Ranking (Cybersecurity rankings)

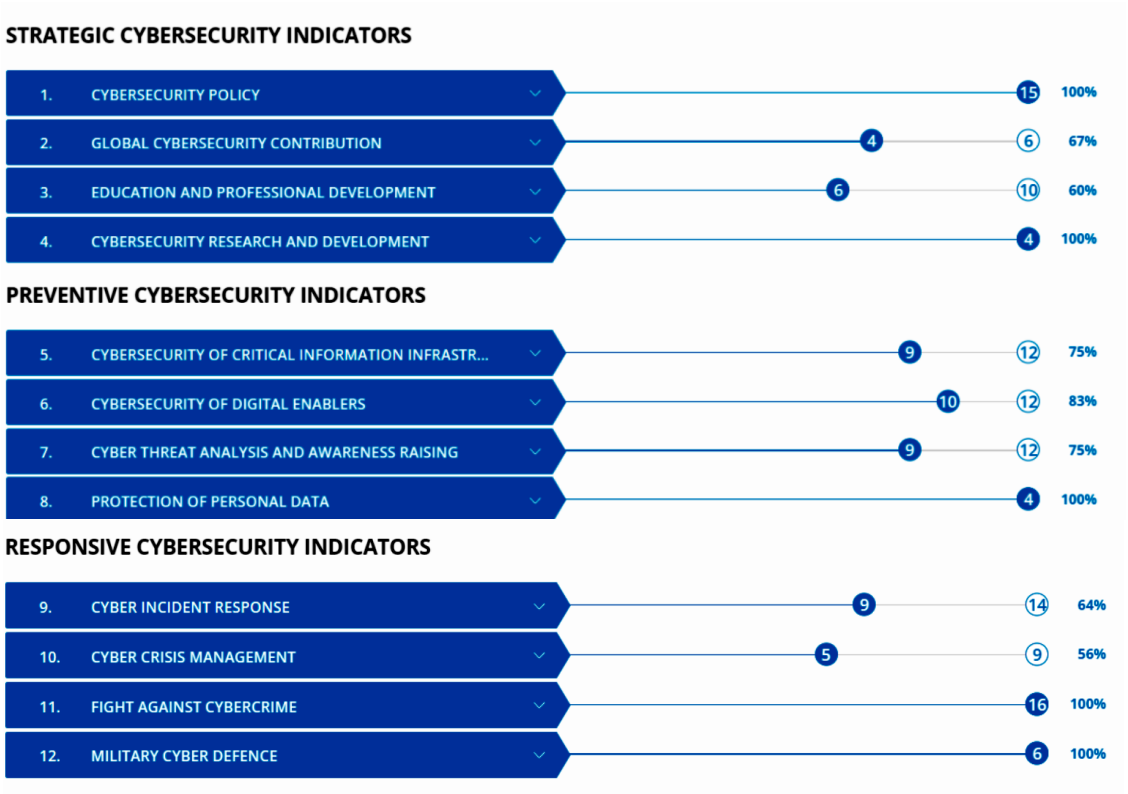

Fig. 2. How experts value Ukraine`s cybersecurity level

As illustrated in Fig. 1, 2, several areas of cybersecurity receive top ratings, emphasizing the importance of personal data protection, military cybersecurity, and well-structured security policies, along with continuous research in the field. AI plays a significant role in enhancing these efforts, contributing to effective strategies across different domains.

Key insights from the figure include:

High Ratings in Critical Areas: Personal data protection, military cybersecurity, properly structured cybersecurity policies, ongoing research and innovation

Critical Infrastructure and Anti-Cybercrime Efforts: Cybersecurity in critical infrastructure and personal

ISSN 2707-1758

data protection is rated positively, as is the fight against cybercrime.

Threats to Ukraine's cyber security have been known and identified for a long time, which indicates opportunities for creating an effective strategy for countering threats.

There are areas that need improvement, in particular: risk management and prevention, anti-crisis management, regulation of the role of AI in cyber security at the legislative level.

This analysis highlights the current situation in Ukrainian cyber security and highlights the need for an AI implementation strategy that will help ensure effective operation while leveraging its potential for protection.

Results

The role of artificial intelligence in various sectors of the economy and human life is becoming more and more important, especially in IT, which is changing rapidly. Cyber security requires modern strategies to counter security threats. With the advent of new technologies, more and more dangerous vulnerabilities, viruses and other cyber threats appear. Organizations are trying to adapt their security protocols to new requirements. AI has the potential to ease some of this work by making security systems more productive, allowing people to focus on strategic planning and other important tasks. However, cyber threats are also evolving and intensifying. Cybercriminals can also use artificial intelligence to design and adapt malware, find system vulnerabilities, and execute more sophisticated attacks. There is a possibility and a risk that the rapid progress of AI may reduce, or even nullify, the human role in the cybersecurity architecture. This is a challenge and a problem that should be taken seriously. In cybersecurity, AI can analyze threat data, make far-sighted and far-reaching predictions, process large volumes of information, and create decoy networks to divert would-be cybercriminals away from mission-critical systems. Timely detection, modeling and forecasting of cyber threats, along with real-time response and accurate analysis of malicious software, as well as the human role in these processes are important aspects of the development of cyber security systems in combination with AI technologies. To effectively address the surge in cyberattacks and the challenges posed by artificial intelligence (AI), the following solutions are proposed:

Create sophisticated software that minimizes the impact of cyberattacks, enhancing overall resilience against threats.

Improve the quality of cyber incident prevention by adapting systems to better anticipate and respond to emerging threats.

Urge both governments and private companies to significantly invest in cybersecurity measures. For example, an investment of $300 million in cybersecurity and AI can help protect $10 billion in critical state assets.

Implement AI systems and leverage cutting-edge software technologies. While initial costs may be high, this investment can lead to substantial long-term savings and more efficient security architectures.

Ensure effective collaboration between humans and AI systems, preventing any reduction in human roles within cybersecurity frameworks.

Tighten access to AI technologies for malicious actors and increase penalties and countermeasures against cybercrime.

By combining strategic efforts and utilizing AI purposefully, it is possible to build a resilient cybersecurity system that effectively predicts and prevents various threats, adapting to contemporary demands.

This strategic approach highlights the dual nature of AI as both a powerful tool for enhancing cybersecurity and a challenge that necessitates careful management and oversight. By implementing these solutions, organizations can better protect their assets and respond to the evolving landscape of cyber threats.

Table 5

Measures to improve cybersecurity

Measure	How it works	Results
Network anomaly detection	AI analyzes network traffic and behavioral patterns to detect unusual activities (e.g., DDoS attacks or intrusions).	**30–50%** reduction in undetected threats through real-time anomaly detection
Malware detection and prevention	AI analyzes the code of programs and files to detect potential malware, including zero-day attacks, without relying on known signatures.	**40–60%** increase in detecting new types of malware
Automated incident response via SOAR platforms	AI triggers automated actions to mitigate threats (e.g., blocking IP addresses or isolating infected devices).	**30–40%** reduction in response time, minimizing potential damage
Phishing attack detection	AI scans emails and messages to identify phishing attempts based on textual, metadata, and behavioral patterns.	**25–40%** decrease in successful phishing attacks
Enhanced authentication using biometrics and behavioral factors	AI leverages user behavior (like typing patterns) or biometric data for additional access control.	**20–30%** decrease in account compromises
Threat prediction and prevention (threat intelligence)	AI analyzes data from multiple sources to predict and prepare for future attacks or vulnerabilities.	**30–50%** improvement in readiness for new threats
Log Analysis for anomaly detection	AI reviews logs and events to detect patterns that may indicate intrusions or policy violations.	**20–40%** reduction in undetected incidents
User education and defense against social engineering	AI personalizes phishing awareness training and educates users about social engineering threats.	**10–25%** reduction in the risk of social engineering attacks

To summarise the information given in Table 5, implementing AI-powered measures can **improve cybersecurity by 50–70%**, depending on the environment (network complexity, user behavior, and current defenses). However, **100% security is unattainable** as threats evolve continuously, and new malware samples appear and improve daily.

Discussion and conclusions

During the research, the following conclusions were drawn: Artificial intelligence is a highly valuable and rapidly

evolving technology, with applications across diverse fields such as weather forecasting and complex software development. AI technologies have already made significant strides in cybersecurity and information protection, creating new opportunities for enhancing data security. With a thoughtful and cautious approach, it is possible to develop robust information systems that provide a high level of cybersecurity. There has been an analysis of the rising number of cyberattacks in recent years and the impact of AI technologies on these trends. While AI offers numerous benefits, it also poses challenges, as malicious actors can exploit these technologies to further their agendas. The study examined the various ways offenders utilize AI technologies. As AI increasingly takes over roles traditionally held by humans, the risks within the cybersecurity domain remain significant. Humanity must adapt to effectively collaborate with AI to preserve its role in this rapidly evolving field. Proper utilization of AI for its intended purposes can lead to the development of a dependable system for preventing cyber threats. This will help reduce the adverse effects of cyberattacks on the economy, businesses, and the lives of ordinary individuals, potentially safeguarding substantial financial and human resources from cybercrime.

Authors' contribution: Serhiy Dakov – conceptualization, methodology; Dmytro Mankovsky – analysis of sources, preparation of literature review, theoretical foundations of the study, preparation of the laboratory for the study, conducting the study.

References

Ilchenko, V. (2024). Cybersecurity Issues in Information and Telecommunication Systems. *VII International Scientific and Practical Conference "Problems of Cybersecurity of Information and Telecommunications Systems" (PCSITS)* (pp. 122–124) Taras Shevchenko National University of Kyiv [in Ukrainian]. [Ільченко В. (2024). Питання кібербезпеки в інформаційно-телекомунікаційних системах. *VII Міжнародна науково-практична конференція "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS)* (с. 122–124). Київський національний університет імені Тараса Шевченка].

Mankovskyi, D. (2024). Study on AI Systems Adaptation to New Threats: Analytical research. *VII International Scientific and Practical Conference "Problems of Cybersecurity of Information and Telecommunications Systems"* (223–225). Taras Shevchenko National University of Kyiv.

Отримано редакцією журналу / Received: 30.10.24
Прорецензовано / Revised: 27.11.24
Схвалено до друку / Accepted: 30.11.24

Сергій ДАКОВ, канд. техн. наук, доц.
ORCID ID: 0000-0001-9413-3709
e-mail: serhii.dakov@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Дмитро МАНЬКОВСЬКИЙ, студ.
ORCID ID: 0009-0004-5053-2432
e-mail: dimamankovskyi@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Іван БІЛОКОНЬ, канд. техн. наук, доц.
ORCID ID: 0009-0008-3074-7064
e-mail: ivan@bilokon@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ ТА ЇХНІ МОЖЛИВОСТІ ПРОТИСТОЯТИ СУЧАСНИМ КІБЕРЗАГРОЗАМ

В с т у п . ***Останніми роками рівень кіберзлочинності стрімко зріс. Складність і різноманітність цих загроз змусили організації віддавати пріоритет передовим рішенням із кібербезпеки, включаючи використання технологій штучного інтелекту, які можуть швидко аналізувати дані для виявлення потенційних загроз і аномалій. Очікують, що до 2027 р. ринок кібербезпеки на основі ШІ перевищить 46 млрд дол. Однак, оскільки штучний інтелект зміцнює та покращує захист, кіберзлочинці адаптуються, використовуючи вразливості та навіть застосовуючи штучний інтелект для посилення атак. Таке подвійне використання ШІ підкреслює необхідність збалансованих і розумних стратегій, які поєднують передбачувані можливості ШІ з людськими знаннями та талантом.***

М е т о д и . ***Наведене дослідження зазначає ефективні стратегії запобігання ризикам, зокрема і сприяння культурі безпеки, впровадження надійних паролів і двофакторної автентифікації, регулярне оцінювання й оновлення систем, удосконалення брандмауерів і дотримання правил кібербезпеки. Штучний інтелект доводить свою цінність у виявленні загроз і реагуванні на них, надаючи компаніям конкурентну перевагу, хоча викликає занепокоєння зменшення ролі людини в задачах безпеки.***

Р е з у л ь т а т и . ***Дослідження показує, що штучний інтелект позитивно впливає на кібербезпеку, забезпечуючи швидке виявлення загроз і реагування на них, дозволяючи організаціям завчасно виявляти й усувати вразливості. Компанії, які інтегрують штучний інтелект у свої стратегії кібербезпеки, отримують перевагу в керуванні складними кіберзагрозами. Проте все ще викликає занепокоєння подвійне використання штучного інтелекту, оскільки його також можуть використовувати кіберзлочинці для розширених атак. Потенціал штучного інтелекту працювати незалежно ставить питання про зменшення ролі людського нагляду. Зрештою, результати підкреслюють необхідність збалансованого підходу: хоча ШІ є важливим для розв'язання задач сучасної кібербезпеки, участь людини у цьому процесі залишається вирішальною. Для захисту критичної інфраструктури та даних необхідні постійна адаптація і поєднання технологічного та людського досвіду.***

В и с н о в к и . ***Швидке зростання кіберзлочинності свідчить про необхідність розроблення надійних заходів кібербезпеки для захисту конфіденційної інформації та забезпечення операційної цілісності. Штучний інтелект стає вирішальним у підвищенні кібербезпеки за допомогою розширеного виявлення загроз, розпізнавання образів і прогнозного аналізу. Хоча штучний інтелект пропонує значні переваги, ним також можуть скористатися кіберзлочинці, що підкреслює важливість пильності й інновацій у стратегіях безпеки. Незважаючи на прогрес ШІ, людські знання залишаються життєво важливими для інтерпретації інформації, прийняття обґрунтованих рішень і адаптації до нових загроз. Для ефективної кібербезпеки важливий багатогранний підхід, включаючи навчання співробітників, регулярні аудити та надійний захист даних. Розширена співпраця між організаціями, урядами та міжнародними партнерами має вирішальне значення для розроблення ефективних стратегій боротьби з кіберзлочинністю. Необхідно продовжувати дослідження можливостей штучного інтелекту й етичних міркувань, щоб подолати мінливий ландшафт загроз кібербезпеці.***

К л ю ч о в і с л о в а : ***штучний інтелект, заходи, стратегія, кібербезпека, загрози, аналіз.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.

ISSN 2707-1758

UDC: 004.056/.57:004.8:519.87OSINT
DOI: https://doi.org/10.17721/ISTS.2024.8.49-55

Laryisa DAKOVA, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0001-6104-8217
e-mail: dacova@ukr.net
State University of Information and Communication Technologies, Kyiv, Ukraine

Maryana LEVYTSKA, Student
ORCID ID: 0009-0007-1617-029X
e-mail: levytskam@fit.knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Katerina HAVENKO, Student
ORCID ID: 0009-0005-7036-9318
e-mail: havenkok@fit.knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

USAGE OF OPEN-SOURCE INTELLIGENCE FOR SECURITY OF CRITICAL INFRASTRUCTURE

Background. *In the metter of critical infrastructure, it refers to the systems and assets that are essential for the functioning of modern society and the economy. These sectors include energy, transportation, elecommunications, healthcare, and water supply, all of which are crucial for national security and public well-being. Disruptions in these infrastructures can lead to decent amount of social and economic vital consequences.*

With the technologies happening to become more advanced, critical infrastructure security systems have become more complex and affiliated. Alterations in example being smart grids, automated transportation systems, and sophisticated communication networks have enhanced efficiency but also increased vulnerabilities. The convergence of digital and physical systems makes these sectors more exposed to risks like cyberattacks, natural disasters, terrorism, and other threats. This growing complexity emphasizes the need for governments and organizations to prioritize the protection of these vital infrastructures.

Methods. *In this research, we developed a mathematically rigorous approach to OSINT in the protection of critical infrastructure, improving on existing methods by providing a structured model for threat detection, vulnerability assessment, and risk calculation. The proposed method employs mathematical representations and probability functions, ensuring a more accurate analysis of threat information and vulnerability scoring. This advancement enables more precise mitigation strategies and better response coordination. While existing OSINT methods rely heavily on unstructured data collection and analysis, our approach introduces a mathematical foundation for data gathering and threat evaluation, providing several key improvements, such as Mathematical Representation of Data; Probabilistic Threat Detection and Vulnerability and Risk Assessment with Weighted Metrics.*

Results. *The study's findings underscore the value of a quantitative OSINT model in critical infrastructure security, demonstrating improvements in accuracy, speed, and decision-making. By reducing ambiguity through probabilistic risk assessments, the model minimizes unnecessary alerts and focuses on actionable threats. Scalability testing showed the model could handle large datasets effectively without overwhelming analysts. Finally, objective risk assessments were validated as enhancing decision-making processes, thus proving beneficial in real-time threat detection and mitigation. The model provides a solid foundation for continuously evolving OSINT practices and suggests potential for further optimization by minimizing risk and balancing mitigation efforts through a defined objective function.*

Conclusions. *After all conducted analytical works, we could definitely say that this mathematical model demonstrates how OSINT can be systematically used to enhance the security of critical infrastructure by assessing vulnerabilities, detecting threats, calculating risk, and applying targeted mitigation strategies. It leverages data collection from open sources, threat analysis, and continuous feedback to ensure that infrastructure systems are resilient to evolving risks.*

Keywords: *OSINT, critical infrastructure security, cyber threats, vulnerability assessment, infrastructure resilience, public sources, data analysis, cybersecurity, information security.*

Background

Open-source intelligence (OSINT) consists of targeted information that is gathered and organized in a specific manner to address particular questions.

This concept evolved from the term "information from open sources" (Open Source Information). In its simplest form, it refers to information that is not classified as "secret." The U.S. Intelligence Community defines this type of information as "publicly available material that can be legally acquired through requests, purchases, or observation, while adhering to copyright protection regulations".

The basis of intelligence gathering is research, which appears to be a verified intelligence requirements with existing sources in order to create a product that fulfills vital needs. This general approach to the collection is the equal way applicable to already classified sources as it is to open sources.

The aim of this work is to investigated the contribution of Open-Source Intelligence to the protection of critical infrastructure. OSINT involves the collection and analysis of publicly accessible data, such as content from social media platforms, news articles and web services. The research highlights how OSINT can be utilized to pinpoint potential security gaps, examine risks, and upgrade and develop responses to emerging threats in critical sectors like energy, transportation, telecommunications, and utilities.

Figure 1 below shows an overview of the elements of the Open Intelligence Collection (OSINT) process.

Background and Importance of the Security of Critical Infrastructure. In the metter of critical infrastructure, it refers to the systems and assets that are essential for the functioning of modern society and the economy. These sectors include energy, transportation, elecommunications, healthcare, and water supply, all of which are crucial for national security and public well-being. Disruptions in these infrastructures can lead to decent amount of social and economic vital consequences (Clarke, 2011; Best, 2011; MTLS, 2010).

With the technologies happening to become more advanced, critical infrastructure security systems have become more complex and affiliated. Alterations in example being smart grids, automated transportation

ISSN 2707-1758

systems, and sophisticated communication networks have enhanced efficiency but also increased vulnerabilities. The convergence of digital and physical systems makes these sectors more exposed to risks like cyberattacks, natural disasters, terrorism, and other threats. This growing complexity emphasizes the need for governments and organizations to prioritize the protection of these vital infrastructures (Clarke, 2011; Lowenthal, 2017; Brown, 2010).

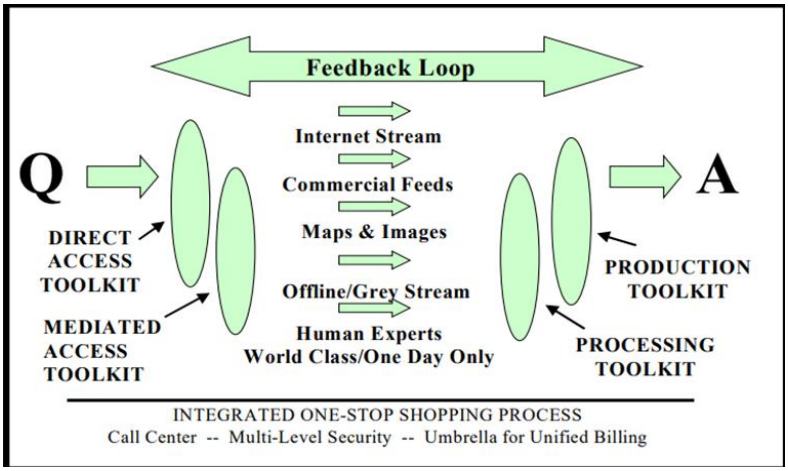

Fig. 1. OSINT collection process (Congressional Research Service, 2007; NATO, 2001)

The increasing complexity and interconnectedness of modern infrastructure. Open-Source Intelligence gathering and analyzing information that is publicly and legally available from sources such as the internet, social media, academic publications, government documents, and press releases. In the context of critical infrastructure security, OSINT plays a key role in identifying potential threats and vulnerabilities. It also brings to light often overlooked information that can help improve the security of these essential assets (Congressional Research Service, 2007; NATO, 2001; Lowenthal, 2017).

The use of OSINT has gained increasing acceptance in modern security practices, largely due to the vast amount of publicly available data. With the right tools, this data can be gathered quickly, enabling more effective risk management. OSINT complements traditional intelligence methods, enhancing situational awareness and enabling more accurate, forward-looking threat assessments (Lowenthal, 2017; Best, 2011; Mutschke, 2018).

Role of Open-Source Intelligence. OSINT, or Open-Source Intelligence, is a type of intelligence gathered by collecting and analyzing data from widely available sources. Comparing to classified intelligence, which relies on confidential data accessible to only a limited group, OSINT draws from sources like the news, social media platforms, government reports, academic research, and public records. What makes OSINT unique is that it's not just about gathering data – it's about processing and applying it to real-world situations (Congressional Research Service, 2007; NATO, 2001; Best, 2011).

In the security field, OSINT pulls information from a variety of sources, such as traditional media and social networks like Facebook, to help spot emerging risks or changes in the environment (NATO, 2001) and (Levytska, 2024; Lowenthal, 2017). By continuously monitoring and analyzing these sources, OSINT helps achieve security goals while staying within legal and ethical limits (Clarke, 2011; Best, 2011). As global infrastructure becomes more interconnected and complex, the importance of open-source intelligence is becoming increasingly important in modern security systems (Congressional Research Service, 2007; Lowenthal, 2017; Brown, 2010). The huge amounts of data available online, along with advances in technology, allow this information to be shared and accessed quickly (Best, 2011; Brown, 2010; Zegart, 2015).

These sources can include:

- News articles, television reports, and radio broadcasts (Lowenthal, 2017).
- Websites, blogs, forums, and online databases (Best, 2011).
- Media Platforms like Twitter (X), Instagram, Facebook LinkedIn, and others where users generate huge amounts of real-time data (Schafer, 2017; Knight, 2020).
- Official government publications, research, and statistical data released by governments.
- Academic papers, dissertations, and journals published by universities and research institutions.
- Reports and data collected and shared by Non-Governmental Organizations.
- Maps, satellite images, and geographic data (Lewis, 2021).

The goal of OSINT is to turn raw, unstructured public data into useful intelligence that can support a range of activities, from national security efforts to corporate risk management. By using OSINT, organizations can spot potential threats, uncover vulnerabilities, and gain valuable insights into security challenges (Brown, 2010; Harding, 2019; Knight, 2020).

Since OSINT relies solely on information that's publicly available, it operates within legal and ethical boundaries. This makes it a cost-effective and flexible option for gathering intelligence compared to more traditional methods (NATO, 2001; Clarke, 2011; Lowenthal, 2017). It's used across many fields, such as cybersecurity, defense, law enforcement, and corporate security, to keep an eye on and respond to emerging risks (Lowenthal, 2017; Harding, 2019; Knight, 2020).

What makes OSINT even more powerful is the use of advanced techniques like data mining, monitoring of social media platforms, and natural language processing (NLP). These help sort through and analyze large amounts of data (Mutschke, 2018; Johnson, 2019), allowing OSINT experts to find the most meaningful insights from the flood of

ISSN 2707-1758

information that's constantly being generated (Mutschke, 2018; Schafer, 2017; Johnson, 2019).

In today's highly connected world, where data is being created and shared every second, OSINT has become increasingly important in ensuring quick and effective risk management and security responses.

Methods

This Fig. 2 represents the process of using Open-Source Intelligence techniques to gather, analyze, and extract meaningful insights from publicly available information, especially for purposes like security analysis and investigative work.

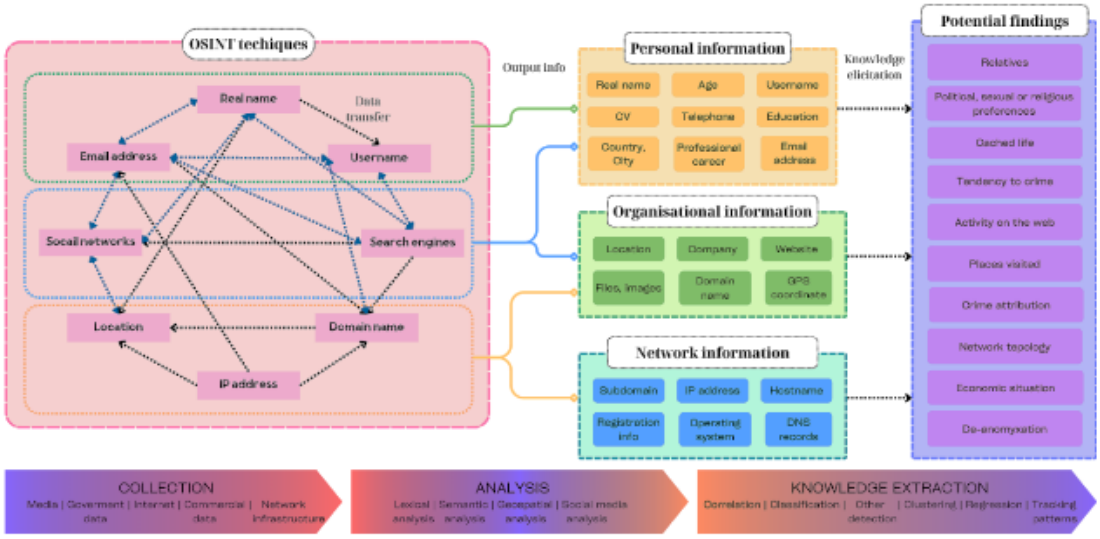

Fig. 2. OSINT collection process (Congressional Research Service, 2007; NATO, 2001)

OSINT Techniques and Data Collection

At the core of the Fig. 2, we can observe a network of interconnected OSINT techniques used to collect data from various sources. These techniques involve gathering details such as:

- Real names,
- Email addresses,
- Usernames,
- Social networks,
- Search engines,
- Location,
- Domain names, and IP addresses.

The Fig. 2 shows how these different pieces of information interact with one another, represented by arrows connecting the elements. For instance, a social network profile might reveal a person's real name or email address, while a search engine might help link a username to additional data, such as a social media profile or location information. Similarly, tracking an IP address might provide information about the user's location or the domain name they are associated with. This interplay highlights the richness of OSINT data, where one piece of information can lead to others, creating a web of connections that can be further explored.

Output Information

Once the data is collected, it is categorized into three main types of output information:

1. Sensitive Information, including details as an example person's real name, age, username, telephone number, education, email address, professional career, and location (city and country). This information is destructive for building profiles of individuals or groups.

2. Commersial Information, which relates to details about a company or organization, such as its location, website, domain name, GPS coordinates, and any associated files or images. Use such type of information can potentially help to understand an organization's structure, physical presence, and online footprint.

3. Network Information, which provides technical details, such as subdomains, IP addresses, hostnames, operating systems, DNS records, and registration information. This type of data is essential for building out the technical infrastructure of an person or an organization, and for understanding their presence in cyberspace.

Knowledge Elicitation and Potential Findings

The Fig. 2 further illustrates how the output information can be used for knowledge elicitation, producing a wide range of potential findings. These findings can reveal important insights, including:

- Personal connections, such as identifying relatives or close associates,
- Preferences, including political, sexual, or religious views,
- Cached life, referring to historical information that remains on the web,
- Tendency to commit crimes based on behavioral patterns,
- Web activity, identifying what individuals or groups are doing online,
- Places visited, through location data or travel histories,
- Crime attribution, linking individuals to potential criminal activities,
- Network topology, which helps understand the structure of a network,
- Economic situation, which can give insights into financial health or business activities,
- De-anonymization, which uncovers the identity of users who may be operating under the assumption of anonymity.

Analysis and Knowledge Extraction

At the bottom of the Fig. 2 we can observe outlined process of analysis, which involves several types of data processing:

- Lexical and semantic analysis focuses on understanding the meaning and context of textual data,
- Geospatial analysis uses geographic data, such as GPS coordinates, to track locations and movements,

- Social media analysis helps uncover relationships and patterns of behavior on platforms like Facebook, Twitter, or LinkedIn.

Finally, after the data has been analyzed, the process moves to knowledge extraction, where advanced techniques like correlation, classification, clustering, regression, and pattern tracking are used. This step involves extracting actionable intelligence by finding connections between evidently extraneous pieces of data, categorizing information, and identifying patterns over time. These methods allow investigators or security professionals to detect threats, track suspicious behavior, and make informed decisions based on OSINT findings.

Application to Critical Infrastructure Security

In the context of securing critical infrastructure, this process of OSINT monitoring and analysis can be instrumental. By gathering data from open sources such as social networks, websites, and public databases, security professionals can monitor for potential threats. For example, OSINT can help identify suspicious activity near sensitive infrastructure, uncover the digital footprints of individuals or organizations involved in planning attacks, or detect patterns in network behavior that indicate a cybersecurity breach. The ability to extract knowledge from OSINT enables authorities to respond proactively, strengthening the protection of vital systems.

This framework highlights the value of open-source intelligence in modern security operations, demonstrating how a variety of data sources and analysis techniques can be integrated to enhance situational awareness and threat detection.

Advanced OSINT Methodologies for Critical Infrastructure Security

What We Have Developed

In this research, we developed a mathematically rigorous approach to OSINT in the protection of critical infrastructure, improving on existing methods by providing a structured model for threat detection, vulnerability assessment, and risk calculation. The proposed method employs mathematical representations and probability functions, ensuring a more accurate analysis of threat information and vulnerability scoring. This advancement enables more precise mitigation strategies and better response coordination.

Comparison with Existing Methods

While existing OSINT methods rely heavily on unstructured data collection and analysis, our approach introduces a mathematical foundation for data gathering and threat evaluation, providing several key improvements:

Mathematical Representation of Data: Existing methods often involve ad hoc collection and manual filtering of data from open sources, which can lead to inaccuracies due to human error or noise. Our model formalizes the data collection process through the formula (1), ensuring that all relevant data points are systematically accounted for, reducing the possibility of missing critical information.

Probabilistic Threat Detection: Traditional threat detection methods may rely on keyword matching or expert analysis. However, these approaches do not quantify the likelihood of a true threat. We introduced a probability function (3.4.1) that mathematically evaluates the relevance of data to specific threats, offering a more reliable means of identifying real risks. This probabilistic approach reduces false positives and ensures a higher rate of accurate threat detection.

Vulnerability and Risk Assessment with Weighted Metrics: Current OSINT vulnerability assessments lack a formalized scoring system for infrastructure components. Our vulnerability scoring model (3.5.1) assigns specific vulnerability scores based on exposure to open-source threats, ensuring a quantitative and comparative analysis of different components. Furthermore, the risk score calculation (3.6.1) combines vulnerability and threat impact factors into a weighted function, allowing for more nuanced prioritization of critical risks.

To better understand the improvements offered by our method, we will now present the key mathematical models, visually on Fig. 3 and also mathematicaly below, that underpin our OSINT framework.

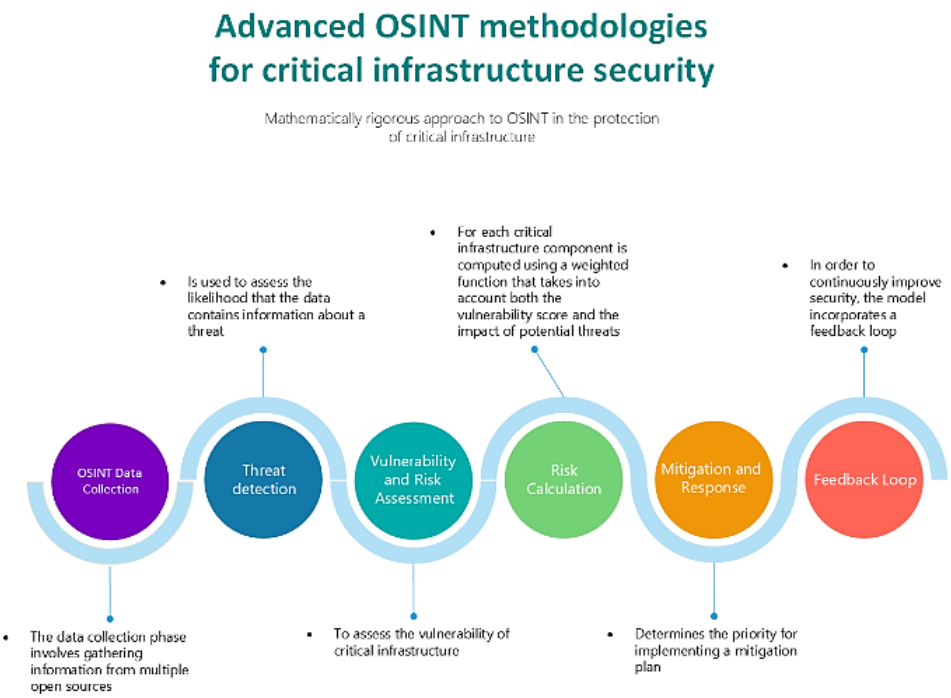

Fig. 3. Visual presentation of made-up method

ISSN 2707-1758

These models guide the data collection, threat detection, vulnerability assessment, and risk calculation processes:

Fig. 3: Conventional designations:

- C_1: Set of critical infrastructure components (e.g., power plants, water systems, communications networks).
- S_0: Set of OSINT sources (e.g., social media, government databases, websites, forums).
- D_0: Set of data extracted from OSINT sources.
- V_T: Set of threat vectors identified through OSINT analysis.
- A_t: Set of analysis techniques applied to the OSINT data (e.g., correlation, semantic analysis, geospatial analysis).
- R_s: Risk score calculated based on potential threats and vulnerabilities.
- P_M: Set of mitigation plans or responses.

OSINT Data Collection

The data collection phase involves gathering information from multiple open sources, which are mathematically represented on formula (1):

$$D_0 = \{d_1, d_2, ..., d_n\} \; where\_d_i \in S_0 . \quad (1)$$

Each piece of data d_i is associated with a source S_0 and a critical infrastructure component C_1. For example, imagining the situation when data collected about an organization's security policies could be linked to their communication systems.

Threat Detection

For each piece of data d_i, a probability function $P = (T/d_i)$ is used to assess the likelihood that the data contains information about a threat T represented on formula (2):

$$P(T \mid d_i) = \frac{\text{Re}\, levant\_threat - related\_keywords\_found\_in\_d_i}{Total\_data\_point s}. \quad (2)$$

Where $P(T \mid d_i) \in [0,1]$ represents the probability that the data point d_i contains information about a potential threat.

Vulnerability and Risk Assessment

To assess the vulnerability of critical infrastructure, we assign a vulnerability score $V(C_{ij})$ to each component C_{ij}, based on its exposure to open-source threats in the following formula (3):

$$V(C_{ij}) = f(D_0, V_t, A_t) . \quad (3)$$

This function f considers the data collected D_0, the threat vectors identified V_t, and the analysis techniques applied A_t. For instance, a high volume of OSINT data indicating a cyber threat against a power grid would increase its vulnerability score.

Risk Calculation

Once vulnerabilities have been assessed, the overall risk score $R_s(C_{ij})$ for each critical infrastructure component is computed using a weighted function that takes into account both the vulnerability score and the impact of potential threats showed in formula (4):

$$R_s(C_{ij}) = \alpha V(C_{ij}) + \beta I(T_j) . \quad (4)$$

Where $V(C_{ij})$ is the vulnerability score of the critical infrastructure component, $I(T_j)$ is the impact of the identified threat on that component, α and β are weighting factors based on the likelihood of a threat and the importance of the infrastructure.

Mitigation and Response

The risk score $R_s(C_{ij})$, presented at formula (5), determines the priority for implementing a mitigation plan. The mitigation strategies are represented by a set P_M, which are functions of the risk score:

$$P_M = g(R_s(C_1)). \quad (5)$$

Where g is a decision function that selects appropriate mitigation strategies based on the calculated risk. For example, if $R_s(C_{ij})$ is high, the mitigation plan might involve enhanced monitoring or deploying security patches.

Feedback Loop

In order to continuously improve security, the model incorporates a feedback loop where new data points D_0 and threat vectors V_T are constantly updated, and the risk scores V_T are recalculated:

$$\begin{aligned} D_0^{(t+1)} &= D_0^{(t)} + \Delta D, \\ V_T^{(t+1)} &= V_T^{(t)} + \Delta V, \\ R_S^{(t+1)} &= R_S^{(t)} + \Delta R. \end{aligned} \quad (6)$$

This feedback ensures that the model adapts to new information and evolving threats, keeping the critical infrastructure secure against potential risks.

Results

The study's findings underscore the value of a quantitative OSINT model in critical infrastructure security, demonstrating improvements in accuracy, speed, and decision-making. By reducing ambiguity through probabilistic risk assessments, the model minimizes unnecessary alerts and focuses on actionable threats. Scalability testing showed the model could handle large datasets effectively without overwhelming analysts. Finally, objective risk assessments were validated as enhancing decision-making processes, thus proving beneficial in real-time threat detection and mitigation. The model provides a solid foundation for continuously evolving OSINT practices and suggests potential for further optimization by minimizing risk and balancing mitigation efforts through a defined objective function.

The introduction of a mathematical foundation significantly improves the overall accuracy, efficiency, and reliability of OSINT for critical infrastructure security. Here are the key benefits:

- **Greater Precision**: By assigning probabilities and quantifying risks, our method minimizes the ambiguity inherent in traditional OSINT methods. This allows for more targeted threat mitigation, reducing unnecessary interventions.
- **Enhanced Speed**: Automating the data collection and threat evaluation process using mathematical

ISSN 2707-1758

formulas accelerates the analysis, enabling faster responses to emerging threats, a crucial factor in protecting critical infrastructure.

- **Scalability**: The structured approach is scalable, capable of processing vast amounts of data across multiple sources without overwhelming analysts. Existing methods struggle to handle large datasets effectively without risking data overload.
- **Objective Decision Making**: Our method removes much of the subjectivity involved in traditional OSINT threat assessments by introducing quantitative models, improving decision-making accuracy for infrastructure protection.

Discussion and conclusions

Also, in conclusion, after all conducted analytical works, we could definitely say that this mathematical model demonstrates how OSINT can be systematically used to enhance the security of critical infrastructure by assessing vulnerabilities, detecting threats, calculating risk, and applying targeted mitigation strategies. It leverages data collection from open sources, threat analysis, and continuous feedback to ensure that infrastructure systems are resilient to evolving risks.

In the metter of optimizing the processes from the persective of mathematical model, we'd recommend the following. The model can be further optimized using an objective function that minimizes risk across all infrastructure components while balancing resource allocation for mitigation in formula 4.1.

Author's contribution: Laryisa Dakova – conceptualization, methodology; Maryana Levytska – analysis of sources, preparation of literature review, theoretical foundations of the study; Katerina Havenko preparation of the laboratory for the study, conducting the study.

References

Best, R. A. Jr. (2011). Open Source Intelligence (OSINT). *Issues for Congress.* Congressional Research Service.

Brown, I. (2010). The changing role of open source intelligence in national security. *Intelligence and National Security*, 25(5), 699–722.

Clarke, R. A. (2011). *Cyber war: The next threat to national security and what to do about it.* HarperCollins Publishers.

Congressional Research Service. (2007, December 5). *Open Source Intelligence (OSINT).* A question for Congress.

Harding, T. (2019). *Open Source Intelligence techniques: Resources for searching and analyzing online information.* CreateSpace Independent Publishing Platform. https://doi.org/10.33896/SPolit.2019.54.11

Johnson, L. (2019). *Artificial intelligence in OSINT. A new frontier for intelligence agencies*. Taylor & Francis Group.

Knight, W. (2020). The impact of social media on intelligence gathering. *Journal of Public Intelligence*, 11(3), 45–56. https://www.researchgate.net/publication/259497232_Social_Media_and_Intelligence_Gathering

Lewis, J. (2021). Geospatial intelligence and OSINT. A convergence of tools and techniques. *Defense & Intelligence Review.*

Lowenthal, M. (2017). *Intelligence: From secrets to policy.* SAGE Publications (7th ed.).

Mutschke, P. (2018). Big data analytics for open source intelligence. New trends and applications. *Journal of Intelligence Studies.* https://ieeexplore.ieee.org/document/8954668

NATO. (2001, November). *NATO Open Source.* Intelligence Handbook.

Schafer, M. (2017). OSINT in the age of social media. *IEEE Access, Cybersecurity Journal*. https://doi.org/10.1109/ACCESS.2020.2965257.

Zegart, A. (2015). *Eyes on spies: Congress and the United States intelligence community.* Hoover Institution Press.

Отримано редакцією журналу / Received: 30.10.24
Прорецензовано / Revised: 27.11.24
Схвалено до друку / Accepted: 30.11.24

ISSN 2707-1758

Лариса ДАКОВА, канд. техн. наук, доц.
ORCID ID: 0000-0001-6104-8217
e-mail: dacova@ukr.net
Державний університет інформаційно-комунікаційних технологій, Київ, Україна

Мар'яна ЛЕВИЦЬКА, студ.
ORCID ID: 0009-0007-1617-029X
e-mail: levytskam@fit.knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Катерина ГАВЕНКО, студ.
ORCID ID: 0009-0005-7036-9318
e-mail: havenkok@fit.knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

ВИКОРИСТАННЯ ІНТЕЛЕКТУ З ВІДКРИТИМ КОРИСНИМ КОДОМ ДЛЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

В с т у п . ***Критична інфраструктура охоплює системи й активи, необхідні для функціонування сучасного суспільства й економіки. До них належать енергетика, транспорт, телекомунікації, охорона здоров'я та водопостачання – усі ці сектори мають вирішальне значення для національної безпеки та добробуту громадян. Збої в цих інфраструктурах можуть мати серйозні соціально-економічні наслідки.***

З розвитком технологій системи безпеки критичної інфраструктури стають дедалі складнішими та більш взаємопов'язаними. Інновації, такі як інтелектуальні мережі, автоматизовані транспортні системи та складні комунікаційні мережі, не лише підвищують ефективність, але і збільшують вразливість. Конвергенція цифрових і фізичних систем робить вказані сектори чутливішими до ризиків, зокрема і до кібератак, стихійних лих, тероризму й інших загроз. Це підкреслює необхідність для урядів і організацій приділяти особливу увагу захисту цих життєво важливих інфраструктур.

М е т о д и . ***Для захисту критичної інфраструктури розроблено математично точний підхід до використання OSINT (відкритих джерел інформації). Це вдосконалений метод, що включає структуровану модель для виявлення загроз, оцінювання вразливості та розрахунку ризику. Запропонований підхід базується на математичних моделях і ймовірнісних функціях, що дозволяє здійснювати точніший аналіз загроз та оцінювання вразливості. Це дає змогу розробляти ефективніші стратегії пом'якшення наслідків і покращити координацію реагування. На відміну від традиційних методів OSINT, які покладаються на збір і аналіз неструктурованих даних, наш підхід запроваджує математичну основу для збору даних і оцінювання загроз, забезпечуючи вдосконалене представлення даних і ймовірнісне виявлення загроз.***

Р е з у л ь т а т и . ***Результати дослідження підтверджують ефективність кількісної моделі OSINT для безпеки критичної інфраструктури. Вона демонструє поліпшення точності, швидкості прийняття рішень, мінімізуючи невизначеність завдяки ймовірнісному оцінюванню ризиків. Модель зменшує кількість непотрібних сповіщень і фокусується на загрозах, що мають практичне значення. Тестування на масштабованість показало, що система здатна ефективно обробляти великі обсяги даних, не перевантажуючи аналітиків. Об'єктивні оцінки ризиків підтвердили поліпшення процесу прийняття рішень і допомогли виявляти і пом'якшувати загрози в реальному часі. Модель також дає надійну основу для подальшого розвитку практик OSINT, з можливістю подальшої оптимізації через зменшення ризиків і збалансування зусиль щодо їхньої нейтралізації.***

В и с н о в к и . ***Результати дослідження показують, що запропонована математична модель є ефективним інструментом для систематичного застосування OSINT для підвищення безпеки критичної інфраструктури. Вона дозволяє здійснювати оцінювання вразливостей, виявлення загроз, розрахунок ризику та застосовувати цілеспрямовані стратегії пом'якшення. Завдяки використанню відкритих джерел даних, аналізу загроз і постійному зворотному зв'язку, модель забезпечує стійкість інфраструктури до мінливих ризиків.***

К л ю ч о в і с л о в а : ***OSINT, безпека критичної інфраструктури, кіберзагрози, оцінка вразливості, стійкість інфраструктури, публічні джерела, аналіз даних, кібербезпека, інформаційна безпека.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.

ISSN 2707-1758

УДК 004.056/.523:004.774REST API
DOI: https://doi.org/10.17721/ISTS.2024.8.56-59

Іван ПАРХОМЕНКО, канд. техн. наук, доц.
ORCID ID: 0000-0001-6889-9284
e-mail: ivan.parkhomenko@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Роман ОГІЄВИЧ, асп.
ORCID ID: 0009-0003-7948-1125
e-mail: r.ohiievych@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

МОДЕЛІ АВТОРИЗАЦІЇ ДЛЯ ВЗАЄМОДІЇ ВУЗЛІВ БЕЗ ДОВІРИ В ПУБЛІЧНИХ ДЕЦЕНТРАЛІЗОВАНИХ МЕРЕЖАХ

В с т у п . ***Децентралізовані мережі стали основою для нових технологій, що забезпечують безпеку та прозорість операцій без потреби в централізованих контролювальних органах. Вказані мережі дозволяють здійснювати взаємодію між вузлами без попередньої довіри. Проте забезпечення надійної та ефективної авторизації в таких мережах є викликом через відсутність єдиного авторизаційного центру. Це створює потребу в розробленні нових моделей, що дозволяють безпечно керувати доступом до ресурсів на основі взаємодії між вузлами. Однією з основних проблем є те, що кожен вузол може бути потенційно шкідливим, і традиційні моделі авторизації, що використовуються в централізованих системах, не можуть забезпечити належний рівень безпеки. Метою цієї роботи є дослідження нових підходів до авторизації в публічних децентралізованих мережах, які не потребують довіри між учасниками.***

М е т о д и . ***Досліджено моделі авторизації, засновані на репутації та доказах корисної роботи – Proof of Useful Work (PoUW), що перспективні для децентралізованих систем. Модель репутації передбачає надання прав доступу на основі попередньої активності вузла в мережі, де кожен вузол накопичує бали репутації за виконання певних завдань. Друга модель PoUW дозволяє вузлам отримувати авторизацію за кількість виконаних корисних обчислень. Це уможливлює не лише підвищення рівня безпеки мережі, але і стимулювання вузлів до виконання обчислювальних завдань, що мають практичну цінність для спільноти.***

Р е з у л ь т а т и . ***Моделювання показало, що обидві моделі дозволяють ефективно забезпечити безпеку та надійність взаємодії між вузлами. Вузли з високим рівнем репутації або ті, що виконали значний обсяг корисних обчислень, отримують доступ до критично важливих ресурсів мережі. Впровадження таких підходів дозволяє знизити ризик шкідливої активності, оскільки вузли, які не виконують корисних дій, обмежуються у правах доступу.***

В и с н о в к и . ***Запропоновані моделі авторизації на основі репутації та Proof of Useful Work продемонстрували високу ефективність у публічних децентралізованих мережах. Вони дозволяють здійснювати безпечну взаємодію між вузлами без потреби у довірі, що робить ці підходи перспективними для майбутнього впровадження в різних сферах. Використання цих моделей забезпечує динамічне керування доступом до ресурсів, мінімізуючи ризики шкідливої діяльності.***

К л ю ч о в і с л о в а : ***авторизація, децентралізовані мережі, репутація, Proof of Useful Work, безпека, взаємодія без довіри.***

Вступ

Сучасні публічні децентралізовані мережі, такі як блокчейн та peer-to-peer (P2P) системи, стають все популярнішими у багатьох сферах (Nakamoto, 2008, с. 1), зокрема й у фінансових операціях, керуванні даними й обчисленнях. Децентралізація забезпечує високий рівень безпеки та незалежності від централізованих органів (Buterin, 2014), однак, вона також створює значні виклики у сфері керування доступом до ресурсів і даних. Відсутність довіри між вузлами мережі означає, що традиційні моделі авторизації, засновані на централізованому контролі, не можуть бути ефективно застосовані в таких середовищах.

Однією з основних проблем, що виникають перед децентралізованими системами, є забезпечення безпечної та ефективної авторизації вузлів. Кожен вузол мережі може бути потенційно шкідливим або ненадійним, тому необхідно впроваджувати нові механізми авторизації, які не залежать від централізованих структур. У контексті цього дослідження особлива увага приділяється моделюванню авторизації на основі репутації вузлів та концепції Proof of Useful Work (PoUW), що дозволяють забезпечити безпеку взаємодії між вузлами без необхідності попередньої довіри.

Метою цієї статті є аналіз і розроблення нових моделей авторизації для децентралізованих систем, які зможуть розв'язати проблему довіри між вузлами та забезпечити безпечну і прозору взаємодію.

Методи

Децентралізовані мережі, такі як блокчейн та інші peer-to-peer системи, сприяли розвитку нових підходів до авторизації, які забезпечують безпечну взаємодію між вузлами без централізованого контролю (Nakamoto, 2008, с. 2). У цьому розділі розглянуто основні моделі авторизації, зокрема на основі репутації, Proof of Work (PoW), Proof of Stake (PoS) і Proof of Useful Work (PoUW).

PoW і PoS є основними моделями консенсусу в багатьох децентралізованих системах, включаючи Bitcoin та Ethereum. У PoW вузли виконують складні обчислювальні задачі для підтвердження транзакцій і забезпечення безпеки мережі, що дозволяє уникнути централізованого контролю, але вимагає значних енергетичних витрат (Bonneau et al., 2015, с. 106). У PoS, навпаки, вузли можуть підтверджувати транзакції на основі кількості криптовалюти, якою вони володіють, що значно зменшує енергоспоживання, але може призвести до централізації, оскільки вузли з більшими ресурсами мають більше повноважень (Buterin, 2014).

Один із найвідоміших протоколів PoS – це Ouroboros, який використовує різноманітні механізми для забезпечення безпеки та децентралізації. Цей протокол забезпечує високий рівень безпеки за рахунок розподілу прав верифікації залежно від часу утримання та кількості монет, що дозволяє створювати децентралізовані та надійні мережі (Kiayias et al., 2017, с. 360).

PoUW є інноваційною моделлю консенсусу, яка поєднує безпеку та корисну роботу. Відмінність PoUW від PoW полягає в тому, що вузли виконують не просто обчислення, а завдання з реальним практичним значенням, наприклад, оброблення наукових даних або великих обсягів інформації. Це дозволяє мережам

ISSN 2707-1758

використовувати ресурси раціональніше, надаючи вузлам можливість виконувати корисні завдання й одночасно забезпечувати безпеку мережі (Ball et al., 2017).

Цей підхід також стимулює вузли виконувати корисні для спільноти обчислення, зменшуючи ризики шкідливої активності та сприяючи ефективному розподілу ресурсів.

Репутаційні системи є альтернативним підходом для забезпечення авторизації в децентралізованих мережах. У репутаційних моделях кожен вузол накопичує бали репутації, що дозволяє оцінювати надійність вузла на основі його попередньої активності та взаємодії з іншими вузлами. Це дає можливість мережам працювати без централізованого контролю і стимулює вузли підтримувати високу репутацію для отримання доступу до ресурсів.

Дослідження також показують, що репутаційні моделі допомагають зменшити ризики шкідливої діяльності, оскільки вузли з низьким рівнем репутації мають обмежений доступ до важливих ресурсів мережі (Jøsang, Ismail, & Boyd, 2007, с. 618–644). Репутаційні системи широко використовують у соціальних мережах та інших онлайн-середовищах, де необхідно оцінювати надійність користувачів на основі їхньої поведінки.

Різні моделі авторизації відіграють важливу роль у керуванні доступом у децентралізованих мережах. Деякі дослідження свідчать, що такі мережі можуть працювати як "егалітарне суспільство" або ж як "доброзичлива диктатура", де вузли з високим рівнем репутації чи ресурсів отримують більші повноваження (Azouvi, Maller, & Meiklejohn, 2018, с. 127–143). Це дозволяє забезпечити стійкість і безпеку мережі, але вимагає ретельного балансування між децентралізацією та контролем для уникнення централізації.

Результати

У процесі дослідження проаналізовано дві моделі авторизації у публічних децентралізованих мережах: модель на основі репутації та модель Proof of Useful Work. Для кожної з них створено симуляційну мережу з 10 вузлів, де кожен вузол виконував певні завдання, за які отримував відповідні бали репутації або обчислювальні ресурси. В результаті вдалося отримати показники ефективності авторизації вузлів і динаміки зміни їхніх прав доступу до ресурсів мережі.

Модель авторизації на основі репутації передбачає, що кожен вузол накопичує бали репутації за виконання корисних дій для мережі, таких як оброблення транзакцій або надання обчислювальних ресурсів. Репутацію вузла розраховують за формулою

$$R_i = \sum_{j=1}^{n} \frac{W_j \cdot A_{ij}}{T_j}, \quad (1)$$

де R_i – репутація вузла *i*, A_{ij} – кількість виконаних дій вузлом і для вузла *j*, W_j – вага дії (важливість завдання для мережі), T_j – час, що минув з моменту виконання дії.

Ця формула дозволяє оцінити, наскільки важливими для мережі були виконані вузлом дії, і враховує як кількість дій, так і їхню важливість для загальної роботи системи.

Таблиця 1

Репутаційні значення вузлів до та після взаємодії

Вузол	Початкова репутація	Кінцева репутація
1	0.10	0.80
2	0.30	0.85
3	0.25	0.75
4	0.20	0.70
5	0.35	0.85
6	0.40	0.90
7	0.50	0.95
8	0.45	0.90
9	0.55	1.00
10	0.60	0.95

На основі результатів моделювання (табл. 1) можна дійти висновку, що вузли, які виконували більшу кількість завдань і взаємодіяли з іншими вузлами, отримали значно більше репутаційних балів і, відповідно, підвищили свій рівень авторизації. Репутація вузлів прямо корелює з їхньою активністю у мережі, що дозволяє зменшити ризики шкідливої активності з боку вузлів із низькою репутацією.

Модель PoUW базується на концепції, що вузли в децентралізованій мережі повинні виконувати обчислення, корисні для її функціонування, за що отримують права доступу до ресурсів. На відміну від традиційних моделей, таких як PoW, де вузли виконують обчислення, які мають обмежене практичне застосування (напр., пошук хеша для верифікації блока), PoUW стимулює вузли до виконання завдань, які приносять реальну користь спільноті (напр., обчислення наукових моделей, оброблення великих даних).

Основні принципи роботи моделі PoUW:

1. Корисні обчислення: вузли, замість витрачання ресурсів на розв'язання криптографічних задач виконують корисні для мережі обчислення. Ці обчислення можуть включати в себе наукові розрахунки, аналіз даних або інші задачі, що мають практичну цінність. Чим більше корисних обчислень виконав вузол, тим більше він отримує прав доступу до ресурсів мережі.
2. Рівень авторизації: авторизація вузла залежить від кількості виконаних ним корисних обчислень. Чим більше обчислень виконує вузол, тим вищий його рівень авторизації, що дозволяє йому доступ до більш критич-

но важливих ресурсів, таких як керування транзакціями, зберігання даних або підтвердження операцій.

Рівень авторизації визначається кількістю виконаних вузлом обчислень, що можна подати у вигляді формули

$$D_i = \frac{C_i}{C_{\max}}, \quad (2)$$

де D_i – рівень авторизації вузла i, C_i – кількість виконаних обчислень вузлом i, $C_{\max}$ – максимальна кількість обчислень, виконаних у мережі.

Ця формула забезпечує вузлам, які виконують більше корисних обчислень, вищий рівень авторизації. У свою чергу, вузли з меншою кількістю обчислень отримують менші права доступу, що гарантує рівний розподіл ресурсів відповідно до внеску кожного вузла.

Для аналізу стабільності роботи мережі та розподілу прав доступу проведено розрахунок показника Герста, що дозволяє оцінити, чи є динаміка репутаційної авторизації вузлів стійкою. Показник Герста розраховують за формулою

$$\frac{\log(R/S)}{\log(N)}, \quad (3)$$

де R/S – відношення амплітуди до стандартного відхилення, N – кількість даних.

Результати розрахунків показали, що для вузлів із високою репутацією показник Герста наближається до 0.9, що свідчить про їхню стабільність у накопиченні прав доступу. Вузли з низькою репутацією мали нижчі значення показника Герста (близько 0.5), що свідчить про нестабільність їхньої авторизації.

Дискусія і висновки

За результатами проведеного дослідження моделей авторизації вузлів у публічних децентралізованих мережах на основі репутації та PoUW можна зробити такі висновки.

Ефективність моделі авторизації на основі репутації: вузли, що активно виконували корисні для мережі дії, отримували значні покращення у рівні своєї репутації. Це забезпечувало їм доступ до більш критичних ресурсів мережі, таких як підтвердження транзакцій та управління обчислювальними завданнями. Зокрема, вузли з початково низькою репутацією, які виконали значну кількість завдань, змогли підвищити свою репутацію на 60–70 %. Це підтверджує, що модель на основі репутації є справедливим підходом до авторизації у децентралізованих мережах.

Модель PoUW забезпечує стимулювання активної участі вузлів: ця модель показала свою ефективність у забезпеченні високого рівня авторизації для тих вузлів, які виконують реальні обчислювальні завдання для мережі. Вузли, що виконали більше обчислень, отримали вищий рівень авторизації. Це дозволило їм доступ до критичних операцій, таких як зберігання важливих даних та керування транзакціями. У такий спосіб PoUW створює ефективний механізм мотивації вузлів до участі у корисній діяльності.

Динамічність і гнучкість авторизації: обидві моделі авторизації є динамічними, оскільки права доступу вузлів постійно коригуються залежно від їхньої активності та внеску у мережу. Це забезпечує справедливий розподіл ресурсів і захист від шкідливої діяльності з боку малоефективних або потенційно шкідливих вузлів. Вузли, які не виконують достатньої кількості завдань або порушують правила мережі, автоматично втрачають права доступу, що мінімізує ризик зловживань.

Безпека та стійкість мережі: за допомогою розрахунку показника Герста встановлено, що вузли з високою репутацією та значними обчислювальними ресурсами демонструють стабільну поведінку та високу стійкість у накопиченні прав доступу. Це свідчить про те, що мережа стає безпечнішою завдяки автоматичному відсіву вузлів із низькою активністю або недобросовісною поведінкою.

Мінімізація ризиків шкідливої активності: завдяки репутаційній моделі вузли з низькою активністю не можуть отримати високий рівень доступу до важливих ресурсів, що захищає мережу від можливих атак або недобросовісної поведінки. Модель PoUW, у свою чергу, стимулює вузли до виконання корисних обчислень, що також знижує ризики шкідливої активності, оскільки вузли-зловмисники не отримують достатньо прав доступу.

Запропоновані моделі можуть бути успішно інтегровані у різні типи децентралізованих систем, такі як блокчейн-платформи, peer-to-peer файлообмінники, децентралізовані обчислювальні системи тощо. Застосування репутаційної системи або PoUW дозволить підвищити надійність і безпеку таких систем, забезпечуючи справедливий розподіл ресурсів і захист від шкідливої активності.

Можливості для подальших досліджень: подальші дослідження можуть бути спрямовані на розширення можливостей моделей авторизації, зокрема й через упровадження додаткових механізмів захисту від маніпуляцій репутацією або обчислювальними ресурсами. Також є перспективи для інтеграції цих моделей з іншими підходами, що дозволить створити ще більш гнучкі та безпечні авторизаційні системи для публічних децентралізованих мереж.

Результати дослідження демонструють, що впровадження моделей авторизації на основі репутації та PoUW у публічних децентралізованих мережах значно підвищує рівень безпеки, стійкості та справедливості взаємодії між вузлами. Це дозволяє мережі функціонувати без централізованого контролю, забезпечуючи водночас прозорість і захист від шкідливої активності.

Внесок авторів: Іван Пархоменко – концептуалізація; методологія; аналіз джерел, підготування огляду літератури або теоретичних засад дослідження; Роман Огієвич – збір емпіричних даних та їх валідація; емпіричне дослідження.

Список використаних джерел

Azouvi, S., Maller, M., & Meiklejohn, S. (2018). Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance. *Financial Cryptography and Data Security*, 127–143. https://doi.org/10.1007/978-3-662-58387-6_9

Buterin, V. (2014). *Ethereum White Paper*. A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepaper

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *IEEE Symposium on Security and Privacy*, 104–121. https://doi.org/10.1109/SP.2015.14

Ball, M., Rosen, A., Sabin, M., & Vasudevan, P. (2017). *Proofs of Useful Work.* IACR Cryptology ePrint Archive. https://eprint.iacr.org

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2), 618–644. https://doi.org/10.1016/j.dss.2005.05.019.

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. *Annual International Cryptology Conference* (pp. 357–388). https://doi.org/10.1007/978-3-319-63688-7_12

ISSN 2707-1758

Nakamoto, S. (2008). Bitcoin. A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

References

Azouvi, S., Maller, M., & Meiklejohn, S. (2018). Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance. *Financial Cryptography and Data Security*, 127–143. https://doi.org/10.1007/978-3-662-58387-6_9

Buterin, V. (2014). *Ethereum White Paper*. A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepaper

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *IEEE Symposium on Security and Privacy*, 104–121. https://doi.org/10.1109/SP.2015.14

Ball, M., Rosen, A., Sabin, M., & Vasudevan, P. (2017). *Proofs of Useful Work.* IACR Cryptology ePrint Archive. https://eprint.iacr.org

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2), 618–644. https://doi.org/10.1016/j.dss.2005.05.019.

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. *Annual International Cryptology Conference* (pp. 357–388). https://doi.org/10.1007/978-3-319-63688-7_12

Nakamoto, S. (2008). *Bitcoin.* A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

Отримано редакцією журналу / Received: 01.10.24
Прорецензовано / Revised: 27.10.24
Схвалено до друку / Accepted: 13.11.24

Ivan PARKHOMENKO PhD, Assoc. Prof.
ORCID ID: 0000-0001-6889-9284
e-mail: ivan.parkhomenko@knu.ua
Taras Shevchenko National University of Kyiv, Ukraine

Roman OHIIEVYCH, PhD Student
ORCID ID: 0009-0003-7948-1125
e-mail: r.ohiievych@gmail.com
Taras Shevchenko National University of Kyiv, Ukraine

AUTHORIZATION MODELS FOR TRUSTLESS NODE INTERACTION IN PUBLIC DECENTRALIZED NETWORKS

Background. ***Decentralized networks, such as blockchain and peer-to-peer systems, have become the foundation for new technologies that ensure the security and transparency of operations without the need for centralized control authorities. These networks enable interaction between nodes without prior trust. However, ensuring reliable and efficient authorization in such networks presents a challenge due to the absence of a single authorization center. This creates the need to develop new models that allow secure access management based on the interaction between nodes. One of the main issues is that each node can potentially be malicious, and traditional authorization models used in centralized systems cannot provide the necessary level of security. The purpose of this study is to explore new approaches to authorization in public decentralized networks that do not require trust between participants.***

Methods. ***The research investigates reputation-based authorization models and Proof of Useful Work (PoUW) models, which show promise for decentralized systems. The reputation model grants access rights based on the node's previous activity in the network, where each node accumulates reputation points for completing specific tasks. The second model, PoUW, allows nodes to gain authorization based on the number of useful computations performed. This approach not only enhances network security but also incentivizes nodes to carry out computational tasks that have practical value for the community.***

Results. ***Modeling has shown that both models effectively ensure the security and reliability of interaction between nodes. Nodes with a high reputation level or those that have completed a significant volume of useful computations gain access to critical network resources. The implementation of such approaches reduces the risk of malicious activity, as nodes that do not perform useful actions are restricted in their access rights.***

Conclusions. ***The proposed authorization models based on reputation and Proof of Useful Work have demonstrated high efficiency in public decentralized networks. They enable secure interaction between nodes without the need for trust, making these approaches promising for future implementation in various fields. The use of these models provides dynamic access management to resources, minimizing the risks of malicious activity.***

Keywords: ***authorization, decentralized networks, reputation, Proof of Useful Work, security, trustless interaction.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.

УДК 004.056/.57:004.72REST API
DOI: https://doi.org/10.17721/ISTS.2024.8.60-65

Юрій ЩЕБЛАНІН, канд. техн. наук, ст. наук. співроб.
ORCID ID: 0000-0002-3231-6750
e-mail: shcheblanin.yurii@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Богдан СИДОРЕНКО, студ.
ORCID ID: 0009-0006-5646-333X
e-mail: sidorenko2002bogdan@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

Інна МИХАЛЬЧУК, канд. техн. наук,
ORCID ID: 0000-0002-1802-7653
e-mail: inna.mykhalchuk@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

БЕЗПЕКА REST API: ЗАГРОЗИ ТА МЕТОДИ ЗАХИСТУ

Вступ. *Зростання зловмисної активності в інформаційному просторі створює додаткові виклики для організацій, які використовують REST API в процесі передачі даних та організації взаємодії з клієнтами і партнерами. Згідно зі статистикою, більше 80 % сучасного вебтрафіка проходить через веб-API, що робить його привабливою мішенню для кіберзлочинців. Вразливість у механізмах автентифікації та авторизації REST API може призвести до витоку конфіденційної інформації, фінансових втрат і загроз репутації. Тому забезпечення безпеки REST API є критично важливим завданням для сучасних компаній, особливо тих, що працюють у галузях із високим рівнем ризику.*

Методи. *Застосовано методи аналізу загроз безпеці й оцінювання ризиків, що виникають у процесі використання REST API.*

Результати. *Організації інвестують значні ресурси у розвиток технологій захисту REST API, впроваджують токени для контролю доступу, шифрують передачу даних за допомогою TLS/SSL та інтегрують сучасні засоби захисту в свої додатки. Проте дослідження показує, що основні загрози безпеці все ще залишаються актуальними через недостатній рівень захищеності процесу валідації вхідних даних, слабкі паролі та відсутність багатофакторної автентифікації. Також встановлено, що значна кількість API не мають обмежень на частоту запитів, що робить їх вразливими до атак на виснаження ресурсів (DoS- і DDoS-атаки).*

Висновки. *Одним із ключових напрямів розв'язання проблеми безпеки REST API є впровадження системи управління безпекою API, до якої належить використання багаторівневого підходу до захисту. Це включає контроль доступу, застосування токенів для авторизації, регулярну перевірку систем на наявність вразливостей та обмеження швидкості запитів для зменшення ризику атак на відмову в обслуговуванні. До того ж упровадження сучасних практик безпеки, таких як багатофакторна автентифікація, допоможе мінімізувати ризики несанкціонованого доступу. Результати дослідження можуть бути використані для вдосконалення існуючих політик безпеки REST API й оптимізації підходів до управління загрозами в компаніях різного масштабу.*

Ключові слова: *REST API, інформаційна безпека, автентифікація, авторизація, загрози, інформаційна безпека.*

Вступ

Зростання зловмисної активності в інформаційному та кібернетичному просторах ставить перед керівниками підприємств і власниками компаній нові завдання щодо захисту своїх цифрових активів. Особливо вразливими є системи, що використовують REST API (Representational State Transfer Application Programming Interface) для обміну даними, оскільки вони стають мішенню для атак, спрямованих на отримання несанкціонованого доступу до конфіденційної інформації або порушення нормального функціонування систем.

Компрометація таких активів, як конфіденційні дані клієнтів, фінансова або інтелектуальна власність, може призвести до порушення безперервності бізнесу, фінансових втрат і втрати репутації компанії. У відповідь на ці виклики організації мають упроваджувати нові загрози та вразливості, характерні для архітектури REST.

З огляду на ці ризики підприємства та компанії мають оцінювати рівень зрілості процесів забезпечення безпеки своїх API та впроваджувати відповідні системи захисту, які враховують специфіку їхньої діяльності. Це питання стає критичним для залучення інвестицій, збереження довіри клієнтів і підтримки безперервної діяльності компанії в умовах сучасної кіберзагрози.

Зловмисники можуть використовувати різні методи атак, включаючи SQL-ін'єкції, атаки на автентифікацію та авторизацію, атаки на відмову в обслуговуванні (DoS, DDoS) та перехоплення даних. Ці атаки можуть призвести до несанкціонованого доступу до конфіденційної інформації, втрат фінансових ресурсів або порушення роботи системи.

Для захисту REST API необхідно впроваджувати комплексні заходи безпеки, які включають використання надійних механізмів автентифікації та авторизації, шифрування даних на транспортному рівні, валідацію вхідних даних та обмеження доступу до ресурсів. Відсутність цих заходів може призвести до серйозних наслідків для організації, включаючи втрату даних, фінансові збитки та порушення репутації.

Ця робота спрямована на аналіз сучасних загроз для безпеки REST API та розроблення підходів до підвищення рівня його захисту на основі сучасних технологій безпеки.

Мета статті – дослідити основні загрози безпеці REST API та проаналізувати методи захисту, які здатні забезпечити надійний захист даних, що передаються через ці інтерфейси.

Методи

Використано метод аналізу загроз безпеці й оцінювання ризиків, що виникають під час застосування REST API, а також системний підхід для комплексного дослідження архітектури REST API.

Результати

У сучасному цифровому середовищі REST API є ключовою складовою для забезпечення зв'язку між додатками, особливо у вебсервісах та мікросервісних архітектурах. Оскільки більшість інтернет-трафіка проходить через API, їхня безпека стає критично важливою для захисту даних і забезпечення стабільної роботи вебдодатків.

ISSN 2707-1758

REST API – це архітектурний стиль для створення легких і гнучких вебсервісів, що використовує стандартний протокол HTTP для передачі даних між клієнтом і сервером. REST API надає клієнтам доступ до певних ресурсів на сервері, дозволяючи отримувати або змінювати дані через стандартизовані запити. На відміну від інших архітектурних стилів, REST спирається на принципи простоти, ефективності та незалежності компонентів, що робить його ідеальним вибором для розподілених систем і мобільних додатків, де важлива швидка і стабільна передача даних.

Однією з ключових концепцій REST API є організація ресурсів за унікальними адресами. Кожен ресурс, наприклад, дані про користувача або продукт, доступний через визначений URL. Клієнт звертається до конкретного ресурсу через запит на сервер, який відповідає, обробляючи цей запит відповідно до правил REST. Щоб досягти цього, REST API використовує стандартні HTTP-методи, що описують дії, які клієнт може виконувати над ресурсами. Метод GET застосовують для отримання інформації про ресурси, POST – для створення нових записів, PUT – для оновлення існуючих даних, а DELETE – для видалення ресурсів (рис. 1).

Архітектурний стиль REST також базується на принципі динамічної взаємодії, що означає відсутність збереження стану між запитами клієнта. Це означає, що кожен запит обробляється незалежно від попередніх, що знижує навантаження на сервер, оскільки йому не потрібно зберігати інформацію про стан сеансу користувача. Завдяки цьому REST API добре масштабується і підходить для оброблення великої кількості запитів одночасно, що є важливим аспектом для вебдодатків і хмарних сервісів (Salva et al., 2024; Laptiev et al., 2022).

REST API часто передає дані у форматах JSON або XML (рис. 1), які легко обробляються більшістю мов програмування та забезпечують зручність взаємодії між різними типами клієнтів, такими як веббраузери, мобільні додатки або навіть інші сервери. Це робить REST API універсальним для різних платформ і значно спрощує інтеграцію нових компонентів у систему. Крім того, використання стандартних форматів передачі даних дозволяє швидко обробляти відповіді сервера і зменшує затримки під час передачі інформації (Zahynei et al., 2024; Syrotynskyi et al., 2024).

Щоб краще зрозуміти принцип роботи REST API, доцільно представити процес взаємодії між клієнтом і сервером у вигляді схеми. Клієнт, що може бути веб-додатком або мобільним пристроєм, формує HTTP – запит для отримання або зміни певних даних на сервері. Сервер приймає запит, перевіряє права доступу, виконує валідацію введених даних і, якщо запит коректний, звертається до бази даних або інших ресурсів для виконання необхідної операції. Після цього сервер формує відповідь із результатом і повертає її клієнту. Відповідь може містити дані у форматі JSON або XML, а також статус виконання запиту, що сигналізує клієнту про успішність операції або наявність помилок.

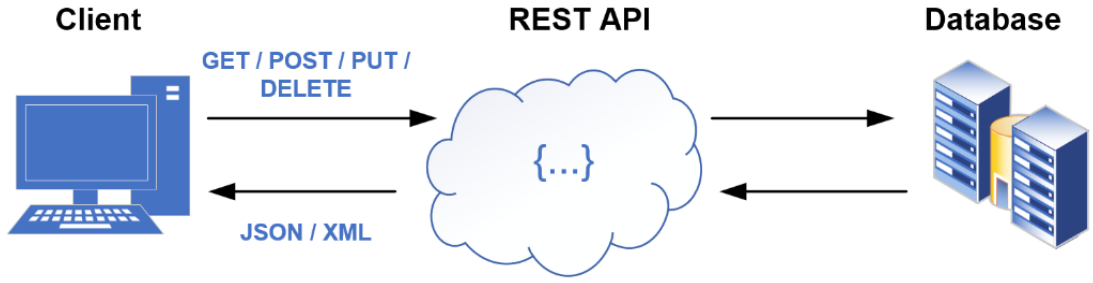

Рис. 1. Схема роботи REST API

Однак REST API схильні до численних загроз, що можуть поставити під загрозу конфіденційність і цілісність даних, а також загальну стабільність систем. Розуміння цих загроз й упровадження ефективних методів захисту є невід'ємною частиною побудови безпечних систем.

Основні загрози для REST API можна поділити на кілька категорій (OWASP API Security Top 10, 2023).

Перша категорія – це загрози пов'язані з недостатньою автентифікацією та авторизацією користувача. Якщо REST API не використовує належні механізми перевірки особи користувача, або процесу, це може дозволити несанкціонованим особам отримати доступ до конфіденційної інформації або навіть здійснювати небажані операції. Наприклад, зловмисники можуть використати слабкі або неправильно налаштовані механізми автентифікації, щоб отримати доступ до захищених ресурсів. Особливо небезпечною є ситуація, коли REST API не належно розмежовує доступ до різних рівнів даних для користувачів із різними ролями або рівнями доступу.

Другою загрозою є атаки типу Denial of Service (DoS, DDoS), які спрямовані на перевантаження серверів API численними запитами, що в кінцевому результаті може призвести до збоїв у роботі або зробити сервіс недоступним для легітимних користувачів. Атаки DoS і DDoS можуть бути надзвичайно руйнівними, оскільки їхня мета – повністю вивести з ладу систему, змушуючи сервер обробляти надмірну кількість запитів або споживати всі доступні ресурси.

Третьою загрозою є SQL-ін'єкції, коли зловмисники вводять шкідливий код у запити, що надсилаються до бази даних через API. Якщо REST API не фільтрує або належно не обробляє вхідні дані, це може призвести до виконання шкідливих команд на рівні бази даних, що відкриває доступ до конфіденційної інформації або дозволяє змінювати дані.

Четвертою загрозою є перехоплення даних. Якщо інформація, яка передається між клієнтом і сервером через REST API, не зашифрована, то зловмисники можуть перехоплювати її. Це особливо небезпечно, коли передають конфіденційні дані, такі як паролі,

особиста інформація або інші дані, які можуть бути використані для викрадення конфіденційної інформації або проведення фінансових махінацій.

До того ж REST API можуть бути вразливими до атак, які експлуатують вразливості програмного забезпечення, наприклад: неправильна обробка вхідних даних, використання застарілих бібліотек або фреймворків, що містять вразливості. Зловмисники можуть скористатися цими недоліками для компрометації системи та виконання шкідливих дій.

Основні методи захисту REST API спрямовано на мінімізацію вказаних загроз і забезпечення безпеки систем.

Одним із ключових методів захисту є використання токенів для автентифікації, зокрема і токенів на основі JSON Web Token (JWT). Цей підхід дає можливість забезпечити перевірку користувача у кожному запиті без необхідності зберігання стану сесії на сервері. Токени JWT включають зашифровану інформацію про користувача, що дозволяє серверу перевіряти права доступу і підтверджувати автентичність кожного запиту. Важливо також упроваджувати механізми оновлення та відкликання токенів, щоб уникнути їх несанкціонованого використання (Shcheblanin et al., 2023, pp. 266–271).

Другим важливим методом є шифрування даних за допомогою TLS/SSL. Це забезпечує захист даних під час передачі між клієнтом і сервером, знижуючи ризик перехоплення конфіденційної інформації зловмисниками. Використання HTTPS для всіх запитів REST API є обов'язковою практикою для забезпечення безпеки. Ще один важливий аспект захисту – валідація та фільтрація вхідних даних. REST API повинні ретельно перевіряти всі вхідні дані, щоб запобігти SQL-ін'єкціям та іншим типам атак на введення. Для цього використовують спеціальні анотації та механізми перевірки даних, що допомагають автоматизувати процес і запобігати поширеним вразливостям.

Обмеження доступу до ресурсів API є ще одним важливим заходом. Необхідно впроваджувати чіткі правила авторизації, що дозволяють обмежити доступ до певних частин API для різних груп користувачів. Це може бути реалізовано за допомогою ролей і привілеїв, що дозволяє контролювати, хто має доступ до певних функцій або даних.

Для захисту від атак типу DoS та DDoS важливо впроваджувати обмеження кількості запитів або використовувати механізми хешування, які дозволяють зменшити навантаження на сервер. Це допомагає знизити ймовірність перевантаження сервера та забезпечити стабільну роботу системи навіть під час великих обсягів запитів.

Отже, забезпечення безпеки REST API є комплексним процесом, який вимагає впровадження різних методів захисту для мінімізації загроз.

Інциденти з компрометацією API. Відомі інциденти, що сталися у великих компаніях, чітко ілюструють небезпеку недостатнього захисту REST API. Вони показують, до яких наслідків може призвести нехтування базовими принципами безпеки (OWASP API Security Project, 2021).

2019 р. через вразливість в API Facebook було викрадено особисті дані близько 50 мільйонів користувачів. Реалізація атаки стала можливою через вразливість у системі автентифікації, яка дозволяла зловмисникам отримати доступ до токенів користувачів і використовувати їх для входу в облікові записи без введення паролю.

Атака на API T-Mobile призвела до витоку даних близько 2 мільйонів користувачів. Ця атака була результатом недостатнього захисту інтерфейсів для сторонніх розробників, що дозволило зловмисникам отримати доступ до конфіденційної інформації користувачів, включаючи номери телефонів та адреси.

Компанія Uber зазнала атаки на свій REST API, що призвело до викрадення даних водіїв і пасажирів. Хакери скористалися помилками в API для отримання доступу до приватних інформаційних ресурсів, оскільки в API не було достатніх обмежень на доступ.

Рекомендації OWASP для підвищення рівня захищеності API. Організація OWASP (Open Web Application Security Project) створила список найпоширеніших загроз для API та рекомендацій щодо захисту від них (табл. 1). OWASP API Security Top 10 є основним орієнтиром для розробників, які прагнуть забезпечити безпеку своїх API.

Розглянемо детальніше захисні заходи для кожної загрози з OWASP API Security Top 10.

Broken Object Level Authorization (Порушення авторизації на рівні об'єктів). Однією з найбільших загроз для API є порушення авторизації на рівні об'єктів. Ця загроза виникає, коли користувачі отримують доступ до об'єктів, на які вони не мають прав. Щоб запобігти цьому, необхідно впроваджувати посилену авторизацію для кожного запиту до API. Кожен користувач повинен мати доступ лише до тих об'єктів, для яких йому надано дозволи. Важливим є використання контролю доступу на основі ролей (RBAC) або атрибутів (ABAC), що дозволяє точніше визначати права доступу. Журналювання всіх запитів до об'єктів допомагає відстежувати можливі порушення та забезпечувати належний рівень захисту (Schmidt, & Meier, 2020).

Broken Authentication (Недостатня автентифікація). Ненадійні або неправильно налаштовані механізми автентифікації можуть дозволити зловмисникам отримати доступ до API, видаючи себе за легітимних користувачів. Для захисту від цього рекомендується впроваджувати багатофакторну автентифікацію (2FA), яка забезпечує додатковий рівень безпеки. Використання токенів на основі JWT або OAuth2 допомагає уникнути проблем із зберіганням сесій і спрощує процес автентифікації. Варто також обмежити кількість спроб входу для запобігання атакам типу "груба сила". Надійне хешування паролів за допомогою алгоритмів є ще одним критично важливим заходом для захисту паролів від підбору (Stallings, 2020; Subhadeep et al., 2024).

Excessive Data Exposure (Надмірна передача даних). Однією з поширених проблем є надмірне розкриття даних через API, коли відповідь містить більше інформації, ніж потрібно клієнту. Для уникнення цього необхідно фільтрувати дані на рівні відповіді, щоб віддавати клієнту лише ту інформацію, яка йому необхідна для виконання запиту. Використання механізмів форматування відповіді на стороні сервера дозволяє контролювати, які дані можуть бути відправлені клієнту, запобігаючи надмірному розкриттю.

Lack of Resources & Rate Limiting (Відсутність обмежень на використання ресурсів). Відсутність обмежень на кількість запитів може призвести до атак на виснаження ресурсів сервера, таких як DoS- та DDoS-атаки. Для захисту від цього рекомендують упроваджувати обмеження швидкості запитів (Rate Limiting), що дозволить обмежити кількість запитів від одного клієнта за одиницю часу. Крім того,

ISSN 2707-1758

використання хешування може допомогти зменшити навантаження на сервер, особливо для повторюваних запитів. Важливо також упроваджувати моніторинг аномальної активності, щоб своєчасно виявляти підозрілу поведінку і вживати відповідних заходів.

Таблиця 1

Топ-10 загроз OWASP для безпеки API

Номер	Загроза	Опис
API 1	Broken Object Level Authorization	Недостатній контроль доступу до об'єктів, що дозволяє зловмисникам отримати доступ до чужих ресурсів
API 2	Broken Authentication	Недостатньо захищені або неправильно налаштовані механізми автентифікації можуть дозволити компрометацію
API 3	Excessive Data Exposure	API може віддавати занадто багато інформації через недостатнє обмеження на рівні відповіді
API 4	Lack of Resources & Rate Limiting	Відсутність обмежень на кількість запитів може призвести до атак на виснаження ресурсів або DoS- та DDoS-атак
API 5	Broken Function Level Authorization	Недостатній контроль доступу до певних функцій API може дозволити користувачам виконувати заборонені дії
API 6	Mass Assignment	Зловмисники можуть змінювати атрибути об'єктів, які не повинні бути доступні через API
API 7	Security Misconfiguration	Неправильна конфігурація безпеки API, включаючи відсутність шифрування або слабкі налаштування доступу
API 8	Injection	Вразливості до ін'єкцій дозволяють упроваджувати шкідливий код через вхідні дані
API 9	Improper Assets Management	Недостатнє управління ресурсами API може призвести до розкриття конфіденційної інформації
API 10	Insufficient Logging & Monitoring	Відсутність належного журналювання та моніторингу ускладнює виявлення атак або реагування на них

Broken Function Level Authorization (Недостатня авторизація на рівні функцій). Недостатня авторизація на рівні функцій може дозволити користувачам отримувати доступ до функцій, які для них не призначені. Щоб запобігти цьому, потрібно впроваджувати строгий контроль доступу до кожної функції. Використання правил авторизації, заснованих на ролях користувачів, дозволяє ефективно розмежовувати доступ до різних функцій API. Також важливо перевіряти права доступу до кожної функції перед її виконанням (Rzaieva et al., 2024; Sobchuk, Zelenska, & Laptiev, 2023).

Mass Assignment (Масове призначення). Масове призначення відбувається, коли API дозволяє клієнтам передавати більше даних, ніж потрібно, і в такий спосіб змінювати критичні атрибути. Щоб цього уникнути, необхідно явно визначати поля, які можуть бути змінені через API-запити. Крім того, важливо перевіряти дозволи на зміну кожного окремого поля, щоб уникнути несанкціонованих змін важливих даних.

Security Misconfiguration (Неправильна конфігурація безпеки). Неправильна конфігурація безпеки API, така як відсутність шифрування або використання застарілих бібліотек, може стати серйозною загрозою. Для уникнення цього важливо регулярно оновлювати компоненти API та використовувати актуальні версії бібліотек із виправленими вразливостями. Стандартизація конфігурацій безпеки допомагає уникнути помилок у налаштуваннях. Проводьте періодичні аудити безпеки, щоб виявляти можливі слабкі місця та вразливості (Rzaieva et al., 2024, pp. 27–38).

Injection (Ін'єкція). Атаки ін'єкції, наприклад SQL-ін'єкції, виникають, коли шкідливий код впроваджується у запити API. Щоб запобігти цьому, слід використовувати параметризовані запити або ORM (Object-Relational Mapping) для безпечної взаємодії з базами даних. Фільтрація і екранування вхідних даних також допомагають запобігти впровадженню небезпечних символів у запити.

Improper Assets Management (Неправильне керування активами). Недостатнє керування ресурсами API, такими як застарілі версії API, може створити додаткові вразливості. Для уникнення цього необхідно регулярно проводити інвентаризацію API і вимикати застарілі версії, які більше не використовуються. Важливо переконатися, що доступ до застарілих API обмежений або повністю вимкнений (Atlidakis, Godefroid, & Polishchuk, 2019).

Insufficient Logging & Monitoring (Недостатнє журналювання та моніторинг). Відсутність належного журналювання та моніторингу може ускладнити виявлення атак або реагування на них. Щоб уникнути цього, рекомендують упроваджувати повне журналювання критичних подій, таких як спроби автентифікації або доступ до конфіденційних ресурсів. Налаштування сповіщень дозволяє оперативно реагувати на підозрілі дії або порушення безпеки. Регулярний аналіз журналів подій допомагає вчасно виявляти підозрілу активність і запобігати можливим атакам (Barabash et al., 2023, pp. 177–192).

Отже, упровадження захисних заходів, рекомендованих OWASP, дозволить суттєво знизити ризик компрометації API і підвищити загальний рівень безпеки додатків. Їх дотримання забезпечить захист від найпоширеніших загроз та атак на рівні API, що критично важливо для сучасних вебдодатків і мікросервісних архітектур.

Дискусія і висновки

Безпека REST API є однією з найважливіших складових розроблень сучасних вебдодатків і мікросервісних

архітектур. Використання API для передачі даних між різними сервісами та системами значно підвищує ефективність розроблення, але також відкриває нові вектори для потенційних атак. В роботі розглянуто найпоширеніші загрози безпеці API, визначені в OWASP API Security Top 10, і запропоновано заходи для їхньої мінімізації.

Ключовим аспектом захисту API є впровадження багаторівневої системи безпеки, яка включає не лише базові механізми шифрування й автентифікації, але й контроль доступу на рівні об'єктів і функцій, захист від ін'єкцій, а також моніторинг активності. Одним із найважливіших кроків для забезпечення безпеки є впровадження посиленої авторизації, що дозволяє запобігати доступу до даних користувачів, яким ці дані не призначені. Це також включає використання механізмів багатофакторної автентифікації (2FA) та токенів, таких як JWT, для забезпечення надійного процесу автентифікації.

Досвід великих компаній, таких як Facebook, Uber та T-Mobile, демонструє серйозність наслідків, до яких може призвести нехтування належними заходами безпеки. Компрометація API у цих випадках призвела до витікання конфіденційної інформації мільйонів користувачів, що підкреслює важливість дотримання найкращих практик захисту API. Сучасні реалії вимагають від розробників не тільки впровадження традиційних методів безпеки, але й застосування таких інструментів, як автоматизоване тестування безпеки в межах підходу DevSecOps.

Згідно з рекомендаціями OWASP, основними захисними заходами є обмеження кількості запитів (Rate Limiting), належне журналювання подій, шифрування трафіка та використання сучасних методів захисту від ін'єкцій, таких як параметризовані запити. Регулярні аудити безпеки й оновлення компонентів системи також відіграють ключову роль у підтриманні надійної безпеки.

Зазначимо, що комплексне впровадження захисних заходів, визначених OWASP, допоможе значно знизити ризик компрометації REST API. Дотримання цих рекомендацій гарантуватиме, що система буде захищена від найпоширеніших загроз, а її функціональність залишатиметься стабільною та безпечною. Зростання популярності REST API вимагає від розробників постійного вдосконалення підходів до безпеки, впровадження автоматизованих рішень і готовності швидко реагувати на нові виклики у сфері кібербезпеки.

Внесок авторів: Богдан Сидоренко – концептуалізація, методологія, аналіз джерел, підготування огляду літератури, розробка захисних заходів для REST API; Юрій Щебланін – збір емпіричних даних, їхня валідація, участь у розробці методології дослідження; Інна Михальчук – огляд літератури, редагування рукопису, участь у розробці методології дослідження.

Список використаних джерел

Atlidakis, V., Godefroid, P. & Polishchuk M (2019). RESTler: Stateful REST API Fuzzing. *41st ACM/IEEE International Conference on Software Engineering (ICSE'2019)*. Montreal, QC, Canada. https://ieeexplore.ieee.org/document/8811961

Barabash, O., Sobchuk, V., Musienko, A., Laptiev, O., Bohomia, V., & Kopytko, S. (2023). *System Analysis and Method of Ensuring Functional Sustainability of the Information System of a Critical Infrastructure Object* (pp. 177–192). https://doi.org/10.1007/978-3-031-37450-0_11

Laptiev, O.,Sobchuk, V., Subach, I., Barabash, A. & Salanda, I. (2022). The Method of Detecting Radio Signals Using the Approximation of Spectral Function. *CEUR Workshop Proceedings*, 3384, 52–61.

OWASP API Security Project (2021). OWASP Foundation. Retrieved from: https://owasp.org/www-project-api-security/.

OWASP API Security Top 10. (2023). OWASP Foundation. https://owasp.org/www-project-api-security/.

Rzaieva, S., Rzaiev D., Kostyuk Y., Hulak H., & Shcheblanin O. (2024). *Methods of Modeling Database System Security* (short paper). CPITS 2024: 384–390.

Schmidt, T., & Meier, M. (2020). Secure API Design and Development: Practices for Building Robust APIs. *API Security Journal*, 5(2), 43–57.

Shcheblanin, Y., Oliinyk, B., Kurchenko, O., Toroshanko O., Korshun, & N. (2023). Research of Authentication Methods in Mobile Applications. *CPITS-2023*, 3421, 266–271.

Sobchuk, V., Zelenska, I., & Laptiev, O. (2023). Algorithm for solution of systems of singularly perturbed differential equations with a differential turning point. *Bulletin of the Polish Academy of Sciences Technical Sciences*, 71(3), Article number: e145682. https://doi.org/10.24425/bpasts.2023.145682 WoS.

Stallings, W. (2020*). Cryptography and Network Security. Principles and Practice.* Pearson Education.

Subhadeep C., Sainath C., Pinnarwar S., & Sandosh S. (2024). Real-Time Threat Detection and Mitigation in Web API Development. *International Conference on Electrical Electronics and Computing Technologies (ICEECT)*, 1 (pp. 1–9). Greater Noida, India.

Zahynei A., Shcheblanin Y, Kurchenko O., Anosov A., & Kruglyk V. (2024). *Method for Calculating the Residual Resource of Fog Node Elements of Distributed Information Systems of Critical Infrastructure Facilities (short paper).* CPITS 2024: p. 432-439.

References

Atlidakis, V., Godefroid, P. & Polishchuk M (2019). RESTler: Stateful REST API Fuzzing. *41st ACM/IEEE International Conference on Software Engineering (ICSE'2019)*. Montreal, QC, Canada. https://ieeexplore.ieee.org/document/8811961

Barabash, O., Sobchuk, V., Musienko, A., Laptiev, O., Bohomia, V., & Kopytko, S. (2023). *System Analysis and Method of Ensuring Functional Sustainability of the Information System of a Critical Infrastructure Object* (pp. 177–192) https://doi.org/10.1007/978-3-031-37450-0_11

Laptiev, O.,Sobchuk, V., Subach, I., Barabash, A. & Salanda, I. (2022). The Method of Detecting Radio Signals Using the Approximation of Spectral Function. *CEUR Workshop Proceedings*, 3384, 52–61.

OWASP API Security Project (2021). OWASP Foundation. Retrieved from: https://owasp.org/www-project-api-security/.

OWASP API Security Top 10. (2023). OWASP Foundation. https://owasp.org/www-project-api-security/.

Rzaieva, S., Rzaiev D., Kostyuk Y., Hulak H., & Shcheblanin O. (2024). *Methods of Modeling Database System Security* (short paper). CPITS 2024: 384–390.

Schmidt, T., & Meier, M. (2020). Secure API Design and Development: Practices for Building Robust APIs. *API Security Journal*, 5(2), 43–57.

Shcheblanin, Y., Oliinyk, B., Kurchenko, O., Toroshanko O., Korshun, & N. (2023). Research of Authentication Methods in Mobile Applications. *CPITS-2023*, 3421, 266–271.

Sobchuk, V., Zelenska, I., & Laptiev, O. (2023). Algorithm for solution of systems of singularly perturbed differential equations with a differential turning point. *Bulletin of the Polish Academy of Sciences Technical Sciences*, 71(3), Article number: e145682. https://doi.org/10.24425/bpasts.2023.145682 WoS.

Stallings, W. (2020*). Cryptography and Network Security. Principles and Practice.* Pearson Education.

Subhadeep C., Sainath C., Pinnarwar S., & Sandosh S. (2024). Real-Time Threat Detection and Mitigation in Web API Development. *International Conference on Electrical Electronics and Computing Technologies (ICEECT)*, 1 (pp. 1–9). Greater Noida, India.

Zahynei A., Shcheblanin Y, Kurchenko O., Anosov A., & Kruglyk V. (2024). *Method for Calculating the Residual Resource of Fog Node Elements of Distributed Information Systems of Critical Infrastructure Facilities (short paper).* CPITS 2024: p. 432-439.

Отримано редакцією журналу / Received: 05.11.24
Прорецензовано / Revised : 27.11.24
Схвалено до друку / Accepted : 01.12.24

ISSN 2707-1758

Yurii SHCHEBLANIN, PhD (Engin.), Senior Researcher
ORCID ID: 0000-0002-3231-6750
e-mail: shcheblanin.yurii@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Bohdan SYDORENKO, Student
ORCID ID: 0009-0006-5646-333X
e-mail: sidorenko2002bogdan@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Inna MYKHALCHUK, PhD (Engin.), Assist.
ORCID ID: 0000-0002-1802-7653
e-mail: inna.mykhalchuk@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

SECURITY OF REST API: THREATS AND PROTECTION METHODS

Background. ***The increase in malicious activity in the information space creates additional challenges for organizations that use REST APIs to transfer data and facilitate interactions with clients and partners. According to statistics, over 80% of modern web traffic goes through web APIs, making them an attractive target for cybercriminals. Vulnerabilities in REST API authentication and authorization mechanisms can lead to data breaches, financial losses, and reputational risks. Therefore, ensuring REST API security is a critical task for modern companies, especially those operating in high-risk industries.***

Methods. ***Threat analysis and risk assessment methods were used to evaluate the security challenges associated with REST APIs.***

Results. ***Organizations are investing significant resources in the development of REST API security technologies, implementing tokens for access control, encrypting data transmission via TLS/SSL, and integrating modern security measures into their applications. However, research shows that major security threats remain relevant due to insufficient input validation processes, weak passwords, and the lack of multi-factor authentication. It was also found that a significant number of APIs lack rate limiting, making them vulnerable to resource exhaustion attacks (DoS/DDoS attacks).***

Conclusions. ***One of the key approaches to addressing REST API security issues is the implementation of an API security management system that uses a multi-layered approach to protection. This includes access control, token-based authorization, regular system vulnerability checks, and rate limiting to reduce the risk of denial-of-service attacks. In addition, implementing modern security practices, such as multi-factor authentication, will help minimize the risk of unauthorized access. The research findings can be used to improve existing REST API security policies and optimize threat management approaches in companies of various sizes.***

Keywords: ***REST API, information security, authentication, authorization, threats, cybersecurity.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.

ISSN 2707-1758

УДК 004.056/.57.4:681.5
DOI: https://doi.org/10.17721/ISTS.2024.8.66-73

Лариса МИРУТЕНКО, канд. техн. наук, доц.
ORCID ID: 0000-0003-1686-261X
e-mail: myrutenko.lara@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

Олексій ШАЙНА, асп.
ORCID: 0009-0003-5707-0544
e-mail: p.papyge@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

Дмитро ПАЛКО, асп.
ORCID ID: 0000-0002-2886-1975
e-mail: palko.dmytro@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

ПРОТОКОЛИ БЕЗПЕКИ В КІБЕРФІЗИЧНИХ СИСТЕМАХ

Вступ. ***Кіберфізичні системи займають важливе місце у сучасних технологіях, оскільки вони поєднують фізичні об'єкти та криптографічні механізми захисту для забезпечення надійної роботи мережних пристроїв, зокрема й у фінансовій галузі, Інтернеті речей і промисловому Інтернеті речей. Основна проблема таких систем полягає у забезпеченні надійного й ефективного захисту даних у разі обмежених ресурсів обчислювальної потужності й енергоспоживання. Криптографічні протоколи, що використовуються у кіберфізичних системах, повинні бути високоефективними, адже від їхньої роботи залежить як безпека, так і загальна продуктивність систем. У цій статті досліджено шляхи підвищення ефективності криптографічних протоколів у кіберфізичних системах.***

Результати. ***Під час дослідження встановлено, що використання протоколів MTLS підвищує рівень захисту даних, але водночас потребує значно більшої кількості ресурсів кіберфізичної системи порівняно з TLS та SSL. До того ж TLS усе ще використовує більшу спроможність кіберфізичних систем аніж SSL, чим підвищує вартість пристроїв кіберфізичних систем. Оптимізація алгоритмів шифрування та дешифрування в протоколі TLS може допомогти зменшити вартість пристроїв і підвищити швидкість передачі даних.***

Висновки. ***Отримані результати показують, що підвищення ефективності криптографічних протоколів у кіберфізичних системах можливе завдяки використанню ефективніших алгоритмів шифрування. Оптимізація протоколів безпеки може значно покращити швидкість передачі даних і продуктивність кіберфізичних систем, особливо у середовищах з обмеженими ресурсами. Варто звернути увагу на концепцію використання існуючих протоколів безпеки, які об'єднують у собі використання симетричних та асиметричних алгоритмів шифрування. В подальшому саме швидкість шифрування та розшифрування відіграватиме визначну роль у підвищенні ефективності. Оскільки саме цей чинник зменшить витрачення ресурсів у кіберфізичних системах, а також отримає перевагу в часі, за рахунок передачі більшої кількості інформації за одиницю часу, не втрачаючи криптостійкості. Подальші дослідження можуть бути зосереджені на розробленні власного протоколу криптографічного протоколу.***

Ключові слова: ***кіберфізична система, асиметричний алгоритм, симетричний алгоритм, протокол безпеки.***

Вступ

Кіберфізичні системи (КФС) займають важливе місце у сучасних технологіях, оскільки вони поєднують фізичні об'єкти та криптографічні механізми захисту для забезпечення надійної роботи мережних пристроїв, зокрема й у фінансовій галузі, Інтернеті речей (IoT) і промисловому Інтернеті речей (IIoT). Основна проблема таких систем полягає у забезпеченні надійного й ефективного захисту даних за обмежених ресурсів обчислювальної потужності та енергоспоживання. Криптографічні протоколи, що використовуються у кіберфізичних системах, мають бути високоефективними, адже від їхньої роботи залежить як безпека, так і загальна продуктивність систем. Ця стаття спрямована на дослідження шляхів підвищення ефективності криптографічних протоколів у КФС.

Метою статті є аналіз існуючих криптографічних протоколів, що використовуються в кіберфізичних системах, та розроблення підходів до підвищення їхньої ефективності. Основну увагу приділено зменшенню енергоспоживання, підвищенню швидкодії алгоритмів шифрування та розробленню методів оптимізації для середовищ з обмеженими ресурсами. Дослідження також охоплює аспекти безпеки, стійкості до фізичних атак і захисту персональних даних.

Результати

Під час дослідження встановлено, що використання протоколів MTLS підвищує рівень захисту даних, але водночас потребує набагато більшої кількості ресурсів КФС порівняно з TLS (Transport Layer Security) та SSL (Secure Sockets Layer). Зазначимо, що TLS усе ще використовує більшу спроможність кіберфізичних систем аніж SSL, чим підвищує вартість пристроїв КФС. Оптимізація алгоритмів шифрування та дешифрування в протоколі TLS може допомогти зменшити вартість на пристрої та підвищити швидкість передачі даних.

Безпека кіберфізичних пристроїв є критично важливою через те, що вони часто працюють у відкритих мережах, й існує ризик перехоплення даних. Для забезпечення безпечного з'єднання між складовими КФС широко використовують криптографічні протоколи, наприклад, TLS, SSL, MTLS.

КФС можуть представляти собою різні IoT-пристрої, з окремою архітектурою безпеки. Для захисту зв'язку між складовими цих девайсів застосовують протоколи безпеки, що шифрують мережний трафік.

Як приклад розглянимо такі КФС.

Смарт-колонки Google Home, Amazon Echo. Смарт-колонки Google Home і Amazon Echo використовують TLS для захисту даних під час їхньої передачі на хмарні сервери, де обробляються голосові команди користувачів.

Фітнес-трекери (Fitbit, Apple Watch). Багато фітнес-трекерів використовують TLS для захисту з'єднань із мобільними додатками або хмарними сервісами для зберігання даних про здоров'я та активність.

Розумні лічильники (Smart Meters). Більшість енергетичних компаній використовують розумні лічильники для моніторингу споживання електроенергії або газу. Ці лічильники використовують TLS для захищеної передачі даних про споживання на центральні сервери компаній.

ISSN 2707-1758

Системи "розумного дому" (Nest, Philips Hue). Системи керування освітленням та опаленням також використовують TLS для забезпечення безпеки у процесі взаємодії із хмарними сервісами або додатками. Усі ці КФС застосовують TLS-протокол для захисту зв'язку. Щоб зрозуміти недоліки та переваги цього протоколу, потрібно розглянути ще два протоколи безпеки – SSL та MTLS. SSL, схема якого зображена на рис. 1 (Tencent Cloud HTTPS) – це попередник TLS, але нині використовується зрідка через вразливості старих версій протоколу (SSL 2.0, SSL 3.0). Більшість сучасних КФС застосовують надійніший протокол TLS замість SSL. Проте раніше SSL використовували в таких системах, як ранні моделі розумних камер відеоспостереження. Деякі моделі камер мали SSL для захисту відеопотоку під час передачі на сервер або мобільний додаток. SSL досі зустрічається на деяких старих або менш оновлених КФС, але більшість сучасних систем перейшли на TLS, оскільки SSL вважається небезпечним.

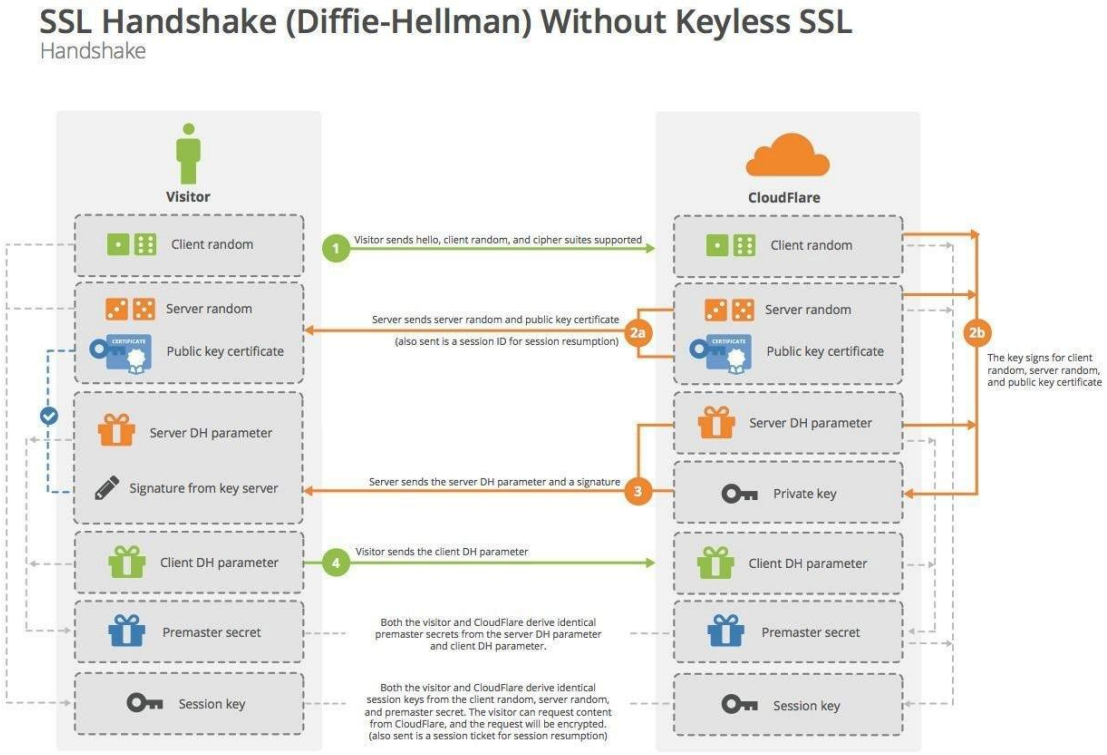

Рис. 1. Схема роботи SSL

Тепер розглянемо приклади використання протоколу MTLS у сучасних КФС. Нині цей протокол захисту з'єднання зустрічається в таких системах: *медичні пристрої* (Smart Health Devices). Деякі медичні IoT-пристрої, такі як пристрої для моніторингу серцевого ритму, інсулінові помпи або інші життєво важливі пристрої, використовують MTLS для забезпечення захищеної передачі медичних даних між пристроєм і медичним сервером. Це важливо для запобігання несанкціонованому доступу до конфіденційних даних пацієнтів. *Індустріальні КФС (IIoT).* У промислових застосуваннях, таких як автоматизовані системи управління заводами, сенсори та контролери часто використовують MTLS для автентифікації серверів і забезпечення безпеки обміну даними. Це допомагає запобігти атакам, які можуть скомпрометувати критичні системи виробництва. *Банкомати та платіжні термінали.* Банківські термінали використовують MTLS для безпечної передачі транзакційних даних між терміналом і сервером банку. Це запобігає атакам типу "людина посередині" (MitM), гарантуючи, що і термінал, і сервер банку є автентичними. *Розумні транспортні системи.* Розумні автомобілі та транспортні системи використовують MTLS для безпечного з'єднання між автомобілем та інфраструктурою (напр., зарядні станції, системи навігації). Це дозволяє зменшити ризики зловмисних втручань у системи автомобіля (Stallings, 2017).

На основі прикладів використання указаних протоколів можна зробити висновок: застосування MTLS у КФС, доречне тільки тоді, коли прилад має великий обсяг електронного ресурсу, що по суті робить такий прилад більш вартісним і габаритним. Варто зазначити, що TLS-протокол використовують безпосередньо в будь-яких кіберфізичних системах, тому що це потребує менший ресурс для його імплементації. Відповідно протокол SSL теж досі зустрічається і потребує ще менших характеристик до приладу на відміну від MTLS і TLS. Розглянемо детальніше наведені протоколи, відмінності між ними та проаналізуємо доцільність їхнього використання в тій чи інший КФС. Основні переваги цих протоколів насамперед у тому, що вони шифрують усі дані, які передаються між клієнтом і сервером, а це запобігає перехопленню або зловмисним змінам даних. Також TLS і особливо MTLS забезпечують і серверу, і клієнту впевненість у справжності кожного з них, що запобігає атакам типу "людина посередині" та несанкціонованому доступу. На додачу протоколи гарантують, що дані не були змінені під час їх передачі (Koblitz, 1987).

Проблеми використання даних систем безпеки полягають у тому, що КФС часто мають обмежену

обчислювальну потужність, пам'ять та енергетичні ресурси. Шифрування й обчислення, пов'язані з TLS і MTLS, можуть бути важкими для таких пристроїв, тому важливо використовувати оптимізовані криптографічні алгоритми (напр., ECC замість RSA). Скажімо, взаємна автентифікація в MTLS вимагає керування цифровими сертифікатами і для серверів, і для клієнтів, що може бути складним і ресурсомістким процесом для великих мереж КФС. Для КФС, які часто мають обмежені мережні ресурси, час установлення захищеного з'єднання може бути критичним. Тому використання легких криптографічних алгоритмів і протоколів, таких як DTLS (легка версія TLS для UDP), може бути кращим варіантом для деяких КФС (Stallings, 2017). Щоб зрозуміти, чому вказані протоколи потребують збільшених ресурсів для пристроїв, пропоную розглянути кожен протокол окремо (Menezes, Van Oorschot, & Vanstone, 1996).

TLS працює на транспортному рівні моделі OSI, як зображено на рис. 2 (OpsFlow Blogs, Mastering HTTPS), і використовується для захисту даних, що передаються між клієнтом (напр.,браузером) і сервером (напр., вебсайтом або хмарним сервісом). Основними функціями TLS є:

- шифрування – захист переданих даних від перехоплення;
- цілісність – гарантування, що дані не були змінені під час передачі;
- автентифікація – підтвердження, що клієнт і сервер є довіреними сторонами.

Тепер пропонуємо розглянути основні етапи роботи цього протоколу: рукостискання (Handshake) – це перший етап, під час якого клієнт і сервер домовляються про параметри з'єднання: привітання від клієнта Client Hello: клієнт ініціює з'єднання, надсилаючи список підтримуваних алгоритмів шифрування, протоколів і версій (Rivest, Shamir, & Adleman, 1978). Привітання від сервера (Server Hello): сервер вибирає підтримуваний клієнтом алгоритм шифрування і надсилає свій сертифікат (цифровий сертифікат SSL/TLS), який містить його публічний ключ (Boneh, & Franklin, 2003). Перевірка сертифіката: клієнт перевіряє сертифікат сервера, щоб переконатися в його справжності. Якщо сертифікат довірений (зазвичай перевіряється за допомогою інфраструктури публічних ключів – PKI (Public Key Infrastructure)), клієнт приймає його. Генерація сесійного ключа: клієнт генерує сесійний ключ для шифрування подальшої комунікації і надсилає його серверу. Цей ключ зашифрований публічним ключем сервера. Захищений обмін: сервер використовує свій приватний ключ для розшифрування сесійного ключа, після чого клієнт і сервер починають використовувати цей ключ для шифрування та розшифрування всіх подальших повідомлень. Шифрування даних (Data Encryption). Після завершення рукостискання весь трафік між клієнтом і сервером шифрується сесійним ключем. TLS підтримує кілька алгоритмів шифрування, таких як AES, ChaCha20, RC4, та інші, які можна використовувати залежно від конфігурації (Boneh, & Franklin, 2003). Перевірка цілісності (Data Integrity): TLS використовує хеш-функції, такі як HMAC Hash-based Message Authentication Code, для перевірки цілісності даних. Це дозволяє виявляти, чи були повідомлення змінені під час передачі (Diffie, & Hellman, 1976). Шифрування даних (Data Encryption): після завершення рукостискання весь трафік між клієнтом і сервером шифрується сесійним ключем. TLS підтримує кілька алгоритмів шифрування, наприклад AES, ChaCha20, RC4, та інші, які можуть використовуватися залежно від конфігурації (Giovanni et all, 2018).

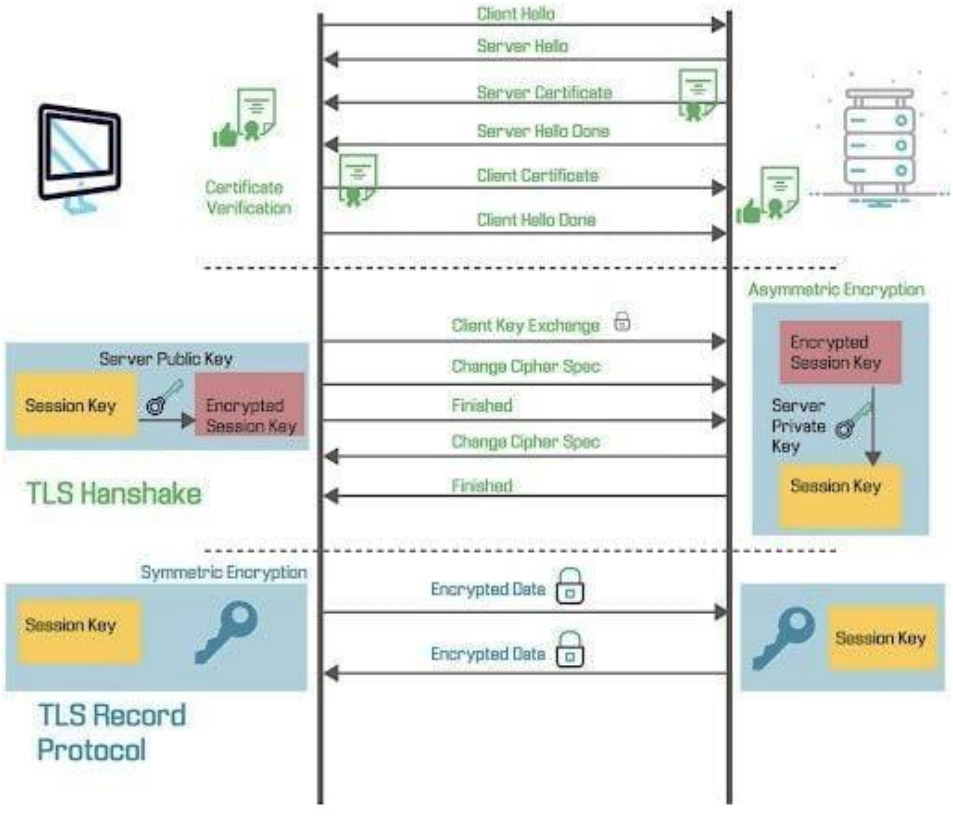

Рис. 2. Схема роботи протоколу TLS

ISSN 2707-1758

Перевірка цілісності (Data Integrity): TLS використовує хеш-функції, такі як HMAC (Hash-based Message Authentication Code), для перевірки цілісності даних. Це дозволяє виявляти, чи були повідомлення змінені під час передачі. Закриття з'єднання (Connection Closure): після завершення передачі даних з'єднання закривається. Це робиться за допомогою спеціальних повідомлень, які підтверджують, що передачу завершено і з'єднання можна безпечно закрити. Чому TLS вимагає більше ресурсів, ніж SSL: TLS підтримує новіші та складніші криптографічні алгоритми, що підвищують безпеку, але також збільшують обчислювальне навантаження. Наприклад, у TLS використовують алгоритми AES і SHA-256, які є надійнішими, але вимагають більше ресурсів, ніж старіші алгоритми, які застосовували в SSL. Покращене рукостискання: у TLS реалізовано покращені механізми рукостискання, які гарантують надійність автентифікації та обміну ключами (Rives, 1978). В TLS відбувається обмін сесійним ключем за допомогою алгоритмів, таких як Diffie-Hellman або його версія на основі еліптичних кривих (ECDH), що забезпечує захист від атак, на зразок "людина посередині". Однак цей процес є обчислювально складнішим порівняно з простішими алгоритмами в SSL. Покращена цілісність даних: SSL використовував слабкіші хеш-функції (напр., MD5 або SHA-1), які були пізніше визнані небезпечними. TLS перейшов на новіші, більш стійкі до колізій функції, такі як SHA-256 або SHA-384. Хоча ці функції значно підвищують безпеку, їхня обчислювальна складність також є вищою. Захист від атаки повторного використання сесій (Replay Attack): TLS забезпечує захист від Replay Attack, яка була слабкіше реалізована в SSL. Це додатковий механізм безпеки, який вимагає більше ресурсів для перевірки послідовності й автентичності кожного пакета. Використання прямих секретів (Perfect Forward Secrecy, PFS): у TLS впроваджено підтримку PFS, це означає, що компрометація одного сесійного ключа не призведе до компрометації всіх попередніх сесій і досягається застосуванням алгоритмів обміну ключами, таких як Diffie-Hellman. Однак PFS вимагає більше обчислювальних ресурсів для генерації нових ключів під час кожного з'єднання. Щоб краще зрозуміти, в чому саме перевага вдосконаленої криптографії, необхідно розглянути різницю між криптографічними алгоритмами DES, AES та SHA-1, SHA-256 відповідно. Спочатку розглянемо основні параметри та структуру SHA-1 та SHA-256, оскільки саме ці функції хешування використовують у протоколах TLS та SSL (Menezes, Van Oorschot, & Vanstone, 1996): алгоритм SHA-1. Ініціалізують п'ять 32-бітових значень:

$$H0 = 0x67452301, H1 = 0xEFCDAB89, H2 = 0x98BADCFE, H3 = 0x10325476, H4 = 0xC3D2E1F0.$$

Кожен 512-бітовий блок ділиться на 16 слів по 32 біти: $W0, W1, \ldots, W15$, де для розширення слів, генерується 80 слів за допомогою розширення вхідних слів:

$$Wt = (Wt-3 \oplus Wt-8 \oplus Wt-14 \oplus Wt-16) \ll 1.$$

Формула для кожного раунду така:

$$T = (A \ll 5) + ft(B,C,D) + E + Wt + Kt,$$
$$E = D, D = C, C = B \ll 30\ C\ =\ B \backslash ll\ 30C = B \ll 30, B = A, A = T.$$

Оновлення значень *H*, після оброблення кожного блока значення $H0, H1, H2, H3, H4$ змінюються:

$$H0 = H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D, H4 = H4 + E.$$

Результат хешування: після оброблення всіх блоків результатом є конкатенація значень $H0, H1, H2, H3, H4,$ що утворюють 160-бітовий хеш. Алгоритм SHA-256 встановлює вісім 32-бітових початкових значень:

$$H0 = 0x6a09e667, H1 = 0xbb67ae85, H2 = 0x3c6ef372, H3 = 0xa54ff53a\ ,$$
$$H4 = 0x510e527f, H5 = 0x9b05688c, H6 = 0x1f83d9ab, H7 = 0x5be0cd19.$$

Розбиття повідомлення на блоки по 512 бітів, де кожен блок розбивається на 16 слів по 32 біти, розширюються для створення 64 слів за такою формулою:

$$Wt = \sigma 1(Wt-2) + Wt-7 + \sigma 0(Wt-15) + Wt-16,$$

де

$$\sigma 0(x) = (x \gg 7) \oplus (x \gg 18) \oplus (x \gg 3),$$
$$\sigma 1(x) = (x \gg 17) \oplus (x \gg 19) \oplus (x \gg 10).$$

Оброблення блока даних (64 раунди):

$$T1 = H + \Sigma 1(E) + Ch(E,F,G) + Kt + Wt,$$
$$T2 = \Sigma 0(A) + Maj(A,B,C).$$

Оновлення значень:

$$H = G, G = F, F = E, E = D + T1,$$
$$D = C, C = B, B = A, A = T1 + T2.$$

Оновлення значень хеша:

$$H0 = H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D,$$
$$H4 = H4 + E, H5 = H5 + F, H6 = H6 + G, H7 = H7 + H.$$

ISSN 2707-1758

Результат хешування: після оброблення всіх блоків вихідним значенням є конкатенація $H0, H1, \ldots, H7$, що утворює 256-бітовий хеш. Довжина хеша: SHA-1: повертає 160-бітове хеш-значення (20 байтів). SHA-256: повертає 256-бітове хеш-значення (32 байти). Більша довжина хеша в SHA-256 робить його стійкішим до атак за принципом "дня народження" (birthday attack), оскільки кількість можливих комбінацій збільшується з 21602160 (SHA-1) до 22562256 (SHA-256). Для атаки колізій на SHA-256 необхідно обчислити 21282128 хешів, у той час як для SHA-1 потрібно обчислити 280280 хешів. Стійкість до колізій: SHA-1: підтримує теоретичну стійкість до колізій на рівні 280280 (що є вразливим у сучасних умовах). SHA-256: має теоретичну стійкість до колізій на рівні 21282128, що набагато безпечніше для сучасних обчислювальних ресурсів. Рівень криптостійкості: SHA-1 використовує 80 раундів оброблення даних, тоді як SHA-256 застосовує 64 раунди, але на довших 32-бітових блоках. SHA-256 також використовує складнішу структуру та різноманітні константи, що ускладнює відновлення вхідних даних. Теоретична криптостійкість у просторі можливих хешів: SHA-1: 21602160 можливих хешів. SHA-256: 22562256 можливих хешів. Для SHA-1 імовірність знайти колізію (тобто два різних блоки вхідних даних, що дають однаковий хеш) значно більша через менший розмір хеша. Теоретично атака на колізію для SHA-1 потребує 280280 операцій, що вже під силу сучасним суперкомп'ютерам, тоді як атака на колізію SHA-256 потребує 21282128 операцій, що робить її надзвичайно складною і практично неможливою. Атака на обчислення обернення (preimage attack): SHA-1: потребує в середньому 21602160 обчислень для знаходження вхідних даних, що відповідають певному хеша. SHA-256: потребує 22562256 обчислень для тієї самої задачі. Така різниця в обчисленнях робить SHA-256 значно стійкішим до brute-force атак. Рівень ентропії: довший хеш у SHA-256 надає більший рівень ентропії, що значно ускладнює криптоаналітичні атаки. Оскільки кожен біт у хеші SHA-256 має більше можливих варіантів, передбачити вихідне значення або підібрати колізію стає значно складніше.

Переваги SHA-256 над SHA-1. Складніша структура: SHA-256 використовує більшу кількість операцій із довшими блоками, що створює надійнішу хеш-функцію, стійку до сучасних методів криптоаналізу. Стійкість до сучасних обчислень: навіть із розвитком квантових обчислень SHA-256 матиме суттєву перевагу в безпеці порівняно із SHA-1, як зазначено у порівняльній таблиці на рис. 3.

Параметр	SHA-1	SHA -256
Довжина хеша	160 біт	256 біт
Блок повідомлення	512біт	512 біт
Кількість раундів	80	64
Структура	Меркле-Демгард	Меркле-Демгард
Колізійна стійкість	Знижена (ефективність атаки)	Висока
Безпека	Скомпрометований	Сучасний стандарт

Рис. 3. Порівняльна таблиця алгоритмів SHA-1 та SHA-256

Як було зазначено, блокові шифри також використовують у протоколах SSL і TLS, тому слід розглянути відмінність між DES і AES, аби зрозуміти що в сучасних алгоритмах більше не використовують шифр DES. Алгоритм DES:

$$Li + 1 = Ri,$$
$$Ri + 1 = Li \oplus F(Ri, Ki),$$

$F(Ri, Ki)$ – функція раунду, яка залежить від правої частини Ri і підключа Ki для цього раунду. $\oplus$ – операція XOR.

$$Ri \to E(Ri),$$

де E – функція розширення, яка перетворює 32 біти Ri на 48 бітів за допомогою додавання бітів за певною схемою XOR із підключем

$$B = E(Ri) \oplus Ki.$$

B ділиться на 8 частин по 6 бітів, кожна частина обробляється *S*-блоком:

$$S(Bj) \to 4 \text{ біт}.$$

Результати конкатенуються у 32-бітове значення.

Відбувається заміна P:

$$P(S(B)) \to F(Ri, Ki)$$

Фінальний результат: після 16 раундів результати *L* та *R* об'єднуються, і до них застосовується кінцева перестановка FP. Алгоритм AES: 128-бітовий вхідний блок перетворюється на матрицю state розміром 4×4 байти. Введений ключ обробляється для отримання підключів для кожного раунду. SubBytes**:** заміна байтів із використанням *S*-блока.

$$state[i, j] = S(state[i, j]).$$

MixColumns**:** перемішування колонок множенням на фіксовану матрицю в полі Галуа GF(2^8):

$$C(x) = state[i, j] \cdot M,$$

де *M* – фіксована матриця: $M = \begin{matrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{matrix}$

ISSN 2707-1758

AddRoundKey: XOR із підключем раунду:

$$state = state \oplus RoundKey.$$

Формула ключового розкладу: AES генерує підключі для кожного раунду за допомогою функції розширення ключа:

$$W[i] = W[i-4] \oplus T(W[i-1]),$$

де *T* включає *S*-блок і операцію Rcon, яка додає змінну залежність для кожного раунду. Довжина ключа: DES: використовує ключ завдовжки 56 бітів (хоча початково є 64 біти, 8 із них застосовують для перевірки парності).

AES: підтримує три довжини ключа – 128, 192, і 256 біт. Короткий ключ DES значно зменшує рівень безпеки, оскільки потребує лише 256256 операцій для повного перебору, тоді як навіть для найкоротшого 128-бітового ключа AES потрібно 21282128 спроб. Розмір блока: DES: працює з блоками по 64 біти. AES: використовує 128-бітові блоки. Більший розмір блока AES робить його стійкішим до атак, які базуються на шаблонах (patterns), а також підвищує ефективність оброблення великих обсягів даних. Структура алгоритму: DES: використовує 16 раундів обробки з Feistel-структурою, де кожен раунд здійснює операції з підключами. AES: залежно від довжини ключа має 10 (128-бітовий ключ), 12 (192-бітовий ключ), або 14 (256-бітовий ключ) раундів. AES базується на замінно-перестановочній мережі (SP-network), яка містить такі основні етапи: заміну байтів (SubBytes), зсув рядків (ShiftRows), змішування стовпців (MixColumns) і додавання підключа (AddRoundKey). Структура SP-мережі, на відміну від Feistel-структури, забезпечує кращу дифузію та заплутування даних, що підвищує стійкість AES до атак. Повний перебір ключів (Brute-force): DES: із ключем у 56 бітів є вразливим до повного перебору, оскільки сучасні обчислювальні потужності можуть перебрати всі можливі ключі за лічені години чи навіть хвилини. AES: найменший ключ у 128 бітів потребує 21282128 можливих комбінацій, що значно перевищує можливості навіть найпотужніших сучасних обчислювальних систем. Криптоаналіз: DES: вразливий до атаки, відомої як "диференційний криптоаналіз" і "лінійний криптоаналіз". Крім того, є атакована версія – 3DES, яка використовує три послідовні операції DES (шифрування-дешифрування-шифрування) для підвищення безпеки, але навіть вона починає поступатися AES через обмежену стійкість і вимоги до потужності (Koblitz, 1987). AES: стійкий до всіх відомих атак, включаючи лінійний і диференційний криптоаналіз. Його структура SP-мережі і більший розмір ключів роблять AES надійним проти методів криптоаналізу, спрямованих на пошук шаблонів і регулярностей у процесі шифрування. Ефективність та швидкість: DES: вимагає менше ресурсів і є швидшим на застарілому обладнанні, але вже не відповідає сучасним вимогам безпеки. AES: швидший та ефективніший на сучасному обладнанні, особливо на процесорах, які мають апаратну підтримку AES (напр., AES-NI).

Переваги AES над DES. Криптостійкість: завдяки довшим ключам і складнішій структурі AES є більш захищеним від сучасних атак. Стійкість до квантових атак: жоден симетричний алгоритм не є повністю захищеним від квантових обчислень, але AES із більшими ключами має більшу криптостійкість порівняно з DES. Універсальність і швидкість: AES є ефективним як на програмному, так і на апаратному рівні, що робить його універсальним стандартом для захисту даних. Порівняння двох блокових шифрів представлено на рис. 4.

Параметр	DES	AES
Довжина блока	64 біти	256 біт
Блок повідомлення	56 біт	512 біт
Кількість раундів	16	64
Структура	Feistel network	Substitution-Permutation Network
Колізійна стійкість	Вразливий до атак на перебір	Висока, захищений від багатьох атак
Безпека	Скомпрометований	Сучасний стандарт

Рис. 4. Порівняльна таблиця алгоритмів DES та AES

Отже, можна зробити висновок, що вдосконалюючи криптографічні алгоритми, можна покращити рівень безпеки протоколу TLS над SSL, але водночас виникає потреба в більших ресурсах, тим самим підвищується вартість девайсу через його характеристики. Тепер розглянемо протокол MTLS детальніше. MTLS – це розширення стандартного протоколу TLS, яке забезпечує взаємну автентифікацію обох сторін з'єднання: і клієнта, і сервера. У той час як стандартний TLS забезпечує автентифікацію лише сервера, MTLS дозволяє також переконатися, що клієнт є довіреною стороною (Luo, Xu, & Zheng, 2020). Це робить MTLS безпечнішим, але також потребує більше ресурсів для встановлення та підтримання з'єднання. У стандартному протоколі TLS клієнт перевіряє автентичність сервера за допомогою сертифіката X.509, який видає сертифікаційний центр (CA). Відтак клієнт шифрує дані для передачі серверу. Однак сервер не перевіряє, хто є клієнтом, і не знає, чи є він довіреним. MTLS розв'язує цю проблему, вимагаючи автентифікації з обох сторін (Luo, Xu, & Zheng, 2020). Основні етапи роботи такі.

Клієнт і сервер обмінюються сертифікатами: у випадку MTLS і клієнт, і сервер повинні надати цифрові сертифікати під час процесу рукостискання. Це дозволяє серверу перевірити автентичність клієнта і переконатися, що він є довіреною стороною (Schneier,

2000). Автентифікація обох сторін: після обміну сертифікатами клієнт перевіряє сертифікат сервера, щоб переконатися, що він справжній і виданий надійним сертифікаційним центром. Сервер, зі свого боку, перевіряє сертифікат клієнта, якщо обидва сертифікати є дійсними, сторони продовжують встановлення сесії. Шифрування з'єднання: як і у звичайному TLS, MTLS використовує сесійний ключ для шифрування всіх подальших даних після встановлення автентифікації клієнта і сервера. Це забезпечує конфіденційність, цілісність і захист даних від перехоплення. Перевірка сертифікатів через PKI: взаємна автентифікація потребує інфраструктури публічних ключів для керування сертифікатами як клієнта, так і сервера. Кожна сторона повинна мати чинний сертифікат, підписаний сертифікаційним центром, якому довіряють обидві сторони.

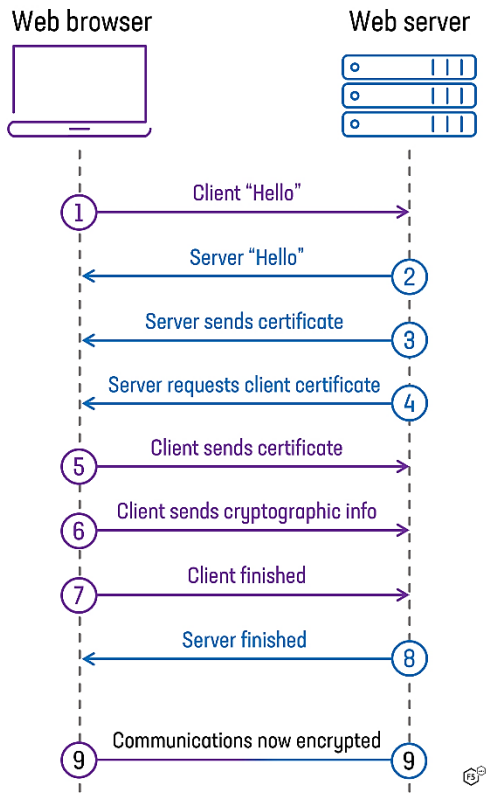

Рис. 5. Схема роботи MTLS

Тепер розглянемо, чому MTLS, схема якого зазначена на рис. 5, вимагає більшої ресурсоспроможності від КФС: додаткова автентифікація клієнта: у MTLS сервер має перевіряти автентичність клієнта за допомогою його сертифіката, що вимагає додаткових обчислювальних ресурсів. Процес перевірки сертифіката включає валідацію сертифіката, перевірку його терміну дії, пошук відмічених сертифікатів у списку відкликаних сертифікатів (CRL) або через протокол OCSP (Online Certificate Status Protocol). Вимога сертифікатів з обох сторін: на відміну від звичайного TLS, де сертифікат надає лише сервер, у MTLS клієнт також повинен мати чинний сертифікат. Це додає оброблення на стороні клієнта, що може бути критичним для пристроїв з обмеженими ресурсами, таких як IoT або КФС. Більший обсяг рукостискання: процес рукостискання в MTLS складніший і включає більше етапів, ніж у стандартному TLS. Кожна сторона повинна обмінятися сертифікатами і виконати обчислювальні операції для перевірки автентичності, що збільшує час установлення з'єднання і вимагає більше обчислювальних ресурсів для оброблення цього процесу. Керування сертифікатами: MTLS покладається на інфраструктуру PKI для керування сертифікатами клієнта і сервера. Це вимагає додаткових зусиль для керування сертифікатами, їхнього видання, поновлення та відкликання. Керування великими обсягами сертифікатів може бути складним і ресурсомістким процесом, особливо в середовищах із великою кількістю клієнтів (напр., у корпоративних мережах або середовищах КФС) (Perez, & Garcia, 2019). З огляду на це можна сказати, що для того, щоб використовувати той чи інший протокол безпеки з'єднання в системах із малою пропускною здатністю, можна спробувати покращити взаємодію симетричних та асиметричних алгоритмів шифрування. Тому необхідно також розглянути можливість зміни складних математичних алгоритмів на легші, що дозволить покращити швидкість шифрування та дешифрування, знизить вартість КФС. Причому потрібно звернути увагу на доцільність використання складних алгоритмів шифрування в кіберфізичних системах, в яких швидкість відіграє визначальну роль. Наприклад, використання складних алгоритмів шифрування в таких КФС, як FPV-дрони, може негативно впливати на роботу самого пристрою та обмін даними між клієнтом і пристроєм. Потрібно враховувати специфіку вказаного девайсу у процесі проєктування аріхтектури безпеки.

Дискусія і висновки

Щоб використовувати той чи інший протокол безпеки з'єднання в системах із малою пропускною здатністю, необхідно покращити взаємодію симетричних та асиметричних алгоритмів шифрування. Запропоновано розглянути можливість зміни складних математичних алгоритмів на легші, що покращить швидкість шифрування та дешифрування, знизить вартість КФС. Варто звернути увагу на концепцію використання існуючих протоколів безпеки, які об'єднують в собі використання симетричних та асиметричних алгоритмів шифрування. В подальшому саме швидкість шифрування та розшифрування відіграватиме визначальну роль у підвищенні ефективності, оскільки саме цей чинник зменшить витрачання ресурсів у КФС, а також отримає перевагу в часі, за рахунок передачі більшої кількості інформації за одиницю часу, майже не втрачаючи у криптостійкості. Подальші дослідження можуть бути зосереджені на розробці власного криптографічного протоколу.

Внесок авторів: Олексій Шайна – збір та аналіз даних про наявні системи захисту в кіберфізичних системах; Лариса Мирутенко – огляд існуючих проблем у протоколах безпеки та пропозиція щодо поліпшення наявних криптографічних протоколів; Дмитро Палко – концептуалізація, аналіз теоретичних засад дослідження.

Список використанних джерел

Boneh, D., & Franklin, M. (2003). Identity-based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3), 586–615.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6).

Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.

Schneier, B. (2000). *Secrets and lies. Digital security in a networked world*. Wiley.

Menezes, A., Van Oorschot, P., & Vanstone, S. (1996). *Handbook of applied cryptography*. CRC Press.

ISSN 2707-1758

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177), 203–209.

Luo, J., Xu, L., & Zheng, P. (2020). Security analysis of network protocols in industrial cyber-physical systems. *Journal of Industrial Information Integration*, 17, 100–110.

Perez, R., & Garcia, S. (2019). Application of cryptography in IoT and cyber-physical systems. Current state. *Sensors*, 19(4).

References

Boneh, D., & Franklin, M. (2003). Identity-based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3), 586–615.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6).

Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.

Schneier, B. (2000). *Secrets and lies. Digital security in a networked world.* Wiley.

Menezes, A., Van Oorschot, P., & Vanstone, S. (1996). *Handbook of applied cryptography*. CRC Press.

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.).Pearson.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177), 203–209.

Luo, J., Xu, L., & Zheng, P. (2020). Security analysis of network protocols in industrial cyber-physical systems. *Journal of Industrial Information Integration*, 17, 100–110.

Perez, R., & Garcia, S. (2019). Application of cryptography in IoT and cyber-physical systems. Current state. *Sensors*, 19(4).

Отримано редакцією журналу / Received: 20.11.24
Прорецензовано / Revised: 27.11.24
Схвалено до друку / Accepted: 13.12.24

Larisa MYRUTENKO, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0003-1686-261X
e-mail: myrutenko.lara@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Oleksii SHAINA, PhD Student
ORCID ID: 0009-0003-5707-0544
e-mail: p.papyge@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Dmytro PALKO, PhD Student
ORCID ID: 0000-0002-2886-1975
e-mail: palko.dmytro@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

EXISTING SECURITY PROTOCOLS IN CFS

Background. ***Cyber-Physical Systems (CPS) play an important role in today's technology, as they combine physical objects and cryptographic security mechanisms to ensure the secure operation of networked devices, particularly in the financial industry, the Internet of Things (IoT), and the Industrial Internet of Things (IIoT). The main problem of such systems is to ensure reliable and effective data protection with limited resources of computing power and energy consumption. Cryptographic protocols used in cyber-physical systems must be highly efficient, because both the security and the overall performance of the systems depend on their operation. This article is aimed at researching ways to improve the efficiency of cryptographic protocols in KFS.***

Results. ***During the research, it was established that: the use of MTLS protocols increases the level of data protection, but at the same time requires a much larger amount of CFS resources compared to TLS and SSL. At the same time, TLS still uses more capacity of cyber-physical systems than SSL, which increases the cost of CFS devices. Optimizing encryption and decryption algorithms in the TLS protocol can help reduce device costs and increase data transfer speeds.***

Conclusions ***The obtained results show that increasing the efficiency of cryptographic protocols in cyber-physical systems is possible by using more effective encryption algorithms. Optimizing security protocols can significantly improve the data transfer rate and performance of cyber-physical systems, especially in resource-constrained environments. It is worth paying attention to the concept of using existing security protocols that combine the use of symmetric and asymmetric encryption algorithms. In the future, it is the speed of encryption and decryption that will play a significant role in increasing efficiency. Since it is this factor that will reduce the use of resources in the CFS and will also gain an advantage in time, due to the transfer of more information per unit of time, with almost no loss in crypto-resistance. Further research may focus on the development.***

Keywords: ***cyberphysical system, asymmetric algorithm, symmetric algorithm, security protocol.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

КОМП'ЮТЕРНІ НАУКИ

UDC 519.87:550.34+53.082.4:[69.058:271.2-788(477.411)]
DOI: https://doi.org/10.17721/ISTS.2024.8.74-84

Vasyl MOSTOVYY, DSc (Phys. & Math.), Leading Researcher
ORSID ID: 0000-0002-1759-1893
e-mail: vasyl.mostovyy@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

MATHEMATICAL MODEL OF THE SIGNAL EMISSION DYNAMICS IN SEISMIC-ACOUSTIC MONITORING SYSTEMS OF BUILDING STRUCTURES

Background. *The paper presents a mathematical model of automated systems of seismoacoustic monitoring of building structures to assess the dynamics of crack formation in building structures to prevent the destruction of the objects under investigation. The seismoacoustic field generated by the research objects is reflected in the matrix of informative parameters, the dynamics of which characterize the dynamics of the object's state. To assess the dynamics of high-frequency signals generated by cracks that occur during the operation of the structure, it is advisable to use the dynamics of emissions that generate these signals. For this, from the point of view of physical practicality, it makes sense to choose a model that characterizes the dynamics of the high-frequency range of the spectrum. Namely, the work presents an algorithm based on a theorem for stationary processes in a broad sense.*

Methods. *The aging process can be reflected in the feature space, which can be reduced to parameters characterizing the elastic properties of the materials that form the objects under study. Since the propagation velocities and the shape of longitudinal and transverse waves in the material depend on the elastic parameters of these materials (Poisson's ratio and Young's modulus), the change in these parameters leads to changes in the spectral characteristics of the emission signals that occur in the aging material. Any redistribution of energy in the material is accompanied by the appearance of signals that generate emission. The dynamics of the parameters of the emission signal reflect the change in the elastic properties of the object under study. Possible reasons for changes in the internal structure are the appearance and growth of cracks, phase transitions in monolithic materials, and loosening of components. This means that changes in the dynamic parameters of emission signals are related to the dynamic characteristics of this object.*

Results. *A mathematical model of building structure aging is proposed. This model of aging of the object must consider the nature of external influences on the object and the nature of its reaction to external disturbances. Given stochastic background noise during monitoring, only the statistical nature of this dependence should be accepted in the model. This model is implemented in building № 3 (cell) of the Kyiv Pechersk Lavra.*

Conclusions. *Two stages of the study of the emission dynamics of building № 3 of the Kyiv Pechersk Lavra showed that during the given time interval, the change in the emission characteristics of this object is within the measurement error. Thus, for an adequate assessment of the emission dynamics generated by cracks that arise during the KPL hull No. 3 operation, it is necessary to collect statistics over a time interval of several decades. To solve this problem, it is essential to carry out permanent seismoacoustic monitoring of the building structure.*

Keywords: *seismoacoustic monitoring, seismoacoustic emission, mathematical model, seismoacoustic signal, matrix of informative parameters of the model, aging of structures.*

Background

The dynamics of emission signal parameters reflect changes in the elastic properties of the object under investigation. This means that changes in the dynamic parameters of emission signals are related to the dynamic characteristics of this object. Given the presence of stochastic background noise during monitoring, only the statistical nature of this dependence should be accepted in the model. The key issue is the selection of informative parameters for the space of signs, in which it is necessary to carry out a dynamic analysis of their behavior, on the basis of which to build a decisive rule for forecasting the state of the object (Mostovyy, V., 2013). There is a problem of choosing the space of signs of aging and fatigue. Since we have only indirect information about the state of the object in the form of the characteristics of the emitted signals, we will be able to make only indirect measurements related to the propagation of emission waves. Dynamic changes of these waves are reflected in the dynamics of their spectral characteristics. The space of spectral characteristics is based on parameters statistically related to the characteristics of the object. The stochastic characteristics of such a component random process reflect the process of changing the elastic characteristics of the material. The task of estimating the parameters of the analyzed random process is reduced to estimating their posterior probability, the dynamics of which reflect fatigue and the aging process of the object.

Passive seismic-acoustic monitoring of construction objects is understood as routine observation of parameters of the natural background of the investigated object. The natural background of the object is a superposition of emission signals caused by natural changes of the object under study (the appearance of microcracks, etc.) and the object's response to external disturbance (wind loads, the impact of transport, seismic events, soil vibrations caused by the vibrations of objects of various nature, the reaction of these objects to external actions, etc.). The mathematical model of object aging should consider the nature of external influences on the object and the nature of its reaction to external disturbances.

Passive seismic-acoustic monitoring will be used to observe the dynamics of the parameters of the mathematical model of the research process and assess the state of aging of the object under study.

Methods

The aging process, a crucial aspect in the life cycle of building structures, is reflected in the feature space. This space can be reduced to a set of parameters characterizing the elastic properties of the materials. Understanding how changes in these parameters lead to changes in the spectral characteristics of the emission signals is key to predicting and managing structural health.

ISSN 2707-1758

The natural frequencies of the investigated objects were in the seismic frequency range. In the stationary state of the object, steady migration of the vector characterizing the state of the object was observed in the space of features within the ellipsoid of rotation of a relatively small volume as passive monitoring. This circumstance is related to the stochastic nature of the monitoring process. This state, crucially, is observed before the onset of fatigue. From the point of view of materials science, fatigue is local structural damage that develops and occurs during cyclic loads on the material. The maximum stress values in the cycle are less than the highest stress limit and below the stress limit for the given material.

The structural failure of the material, a critical event, consists in the loss of the load-bearing capacity of the element or directly of the entire structure. It begins when the stresses in the material approach the limit, causing excessive deformations, when the material in the process of a complete cycle returns to its initial state, i.e., the phenomenon of hysteresis is manifested. Any energy redistribution in the material, a key factor, is accompanied by the emergence of emitted signals. Emission signals, the focus of our study, are voltage waves generated by a sudden internal redistribution of voltage in the material caused by changes in the internal structure.

Possible reasons for changes in the internal structure: the appearance and growth of cracks, phase transitions in monolithic materials and loosening of components.

Structural analysis and identification of dynamic parameters of building structures and their components whose spectral characteristics lie in the seismic and lower part of the acoustic ranges are extremely important in their monitoring to predict significant changes in dynamic characteristics. By geometric dimensions, they are large artificial and natural objects. The method of dynamic identification provides an opportunity to investigate the dynamic behavior of this structure with the help of non-destructive tests and, therefore, allows us to assess the "health" of the structure and the possible need for more detailed monitoring. The method of examination of the response of the structure to the dynamic load is analyzed, which can be any environmental (wind, sea waves, traffic, etc.) or artificially caused using test pulses.

Of particular interest is the passive monitoring of objects with sources of emission signals, the parameters of which are subject to determination and characteristic of the structure. The emission can be both irregular and regular. In the latter case, it can be modeled as a flow with probabilistic characteristics to be determined (Mostovyy, V., 2013).

A change in the condition of building structures during their operation can lead to undesirable and sometimes even catastrophic consequences. The cause of destruction of engineering structures and their components is most often structural changes of composite materials, under which destruction occurs in operational loads and natural aging (Schijve, 2003). An example of such consequences can be the well-known, relatively recent collapses of building structures in Germany, Japan, France, Latvia, and the USA (such as the collapse of the city archive building in Cologne on March 3, 2009, the collapse of a car tunnel near Tokyo on December 2, 2012, the collapse of the terminal at Charles de Gaulle Airport on 05/24/2004, the collapse of the Maxim center in Riga on 11/21/2013, the collapse of a residential building in Miami, Florida, USA on 06/24/2021) and many other countries. In Ukraine, an example of such a disaster can be the collapse of a building on the street. Hrushevsky in the city of Drohobych, 28.08.2019, the bridge's destruction in Kharkiv on 30.08. 2019, and others. Continuous seismic-acoustic monitoring makes it possible to evaluate the dynamics of the strength characteristics (Young's modulus and shear modulus) of the object under investigation to forecast its condition (Tassios, 2010).

To study the dynamics of parameters characterizing the strength parameters of building structures, a new concept of seismic-acoustic monitoring of natural and building objects is proposed, in which the object under investigation is mapped into an n-dimensional vector of the Euclidean space of informative parameters using a physically feasible parametric model. For seismic-acoustic monitoring of building structures, a mathematical model (Mostovyy, V., 2013) was used within the framework of this concept in order to assess the dynamics of the object's parameters characterizing its strength (Mostovyy, V., 2013).

The monitoring concept was based on the following physical principles. Since the speed of propagation and the form of longitudinal and transverse waves in the material depend on the elastic parameters of these materials, the change in these parameters leads to changes in the spectral characteristics of the emission signals that occur in the aging material. The emission refers to the redistribution of energy in the material, accompanied by the appearance of emitted signals. Signal emissions are stress waves generated by a sudden internal redistribution of stress in the material caused by changes in the internal structure, i.e., material fatigue. The emission is caused by the redistribution of energy in the material. Any energy redistribution in the material is accompanied by the emergence of emitted signals. The superposition of such signals generates an emission field (Tassios, 2010).

From the point of view of material science, fatigue is developing, and local structural damage occurs during cyclic loads on the material (Suresh, 2004). Cyclic stress should lead to material fatigue. Fatigue leads to irreversible deformations of the material, that is, to its aging. The aging process in the proposed models is a change in material parameters that are reflected in the feature space. Parameterization of the analyzed process takes place using its approximation of a parametric model with free parameters. Thus, the process of seismic-acoustic monitoring of natural and building structures is reduced to regular observations of the free parameters of the selected model.

The physical principles of seismic-acoustic monitoring presented above in an actual embodiment require the researcher to solve complex mathematical problems. From the registration of the implementation of the emission field to the estimation of the free parameters of the model, a complex mathematical apparatus is used, which is based on such mathematical disciplines as the theory of random processes, functional analysis, the theory of the function of a complex variable, linear algebra, optimization methods and the theory of decision making (Timoshenko, & Gere, 1961), which is presented in the study of the dynamics of the state of building structures.

Since the propagation velocity of longitudinal and transverse waves are functions of the characteristics of the medium's strength, namely Young's modulus and the shear modulus, respectively, it is physically appropriate to use the medium's spectral characteristics as informative parameters of the mathematical model of the object under study.

Thus, wave propagation dynamics characterize the dynamics of the strength characteristics, and a change in the state of the research object itself causes the departure from the stationarity of the spectral characteristics (Mostovoy, V., & Mostovoy, S., 2023).

Mathematical model of the signal emission dynamics. To assess the dynamics of high-frequency signals generated by cracks that arise during the operation of the structure, it is advisable to use the dynamics of emissions that generate these signals. For this, from the point of view of physical practicality, it makes sense to choose a model that characterizes the dynamics of the high-frequency range of the spectrum. Namely, the algorithm is based on a theorem for stationary in the sense of processes. If a stationary process in a broad sense has a completely entirely continuous spectrum and the spectral density of the process allows the representation

$$f(\omega) = (h(i\omega)^2 \quad (1)$$

here

$$h(i\omega) = \int_0^\infty b(\tau) \cdot \exp(-i \cdot \omega \cdot \tau) d\tau,$$

$$\int_0^\infty (b(\tau)(^2 \cdot d\tau \angle \infty. \quad (2)$$

then the process is the response of a physically feasible filter $a(t)$ and

$$h(i\omega) = \sqrt{\frac{1}{2 \cdot \pi}} \cdot \int_0^\infty a(\tau) \cdot \exp(i \cdot \omega \cdot \tau) \cdot d\tau. \quad (3)$$

The detection algorithm follows from this. On the prehistory T, under the assumption of stationarity in the broad sense of a stochastic process $n(t)$ we estimate its spectral density $h(i\omega)$ and map it into a vector of the n-dimensional parameter $\vec{h}$ space, for example, by calculating the energy of the spectral density $h(i\omega)$ in n subbands (ω_i, ω_{i+1}) $i = \overline{1,n}$, and then estimate in the Euclidean metric the deviation of the vector $\vec{h}_t$ calculated in the sliding window from $\vec{h}$:

$$\left\| \vec{h}_t - \vec{h} \right\| \le H. \quad (4)$$

If this expression is correct, a decision is made about the absence of negative dynamics of the research object. Otherwise, the fragment of the process $(t, t+T)$ characterizes the negative dynamics of the aging process. The setpoint level H is determined by the researcher, who determines the setpoint level in terms of its probability of false alarm and target miss.

Application of a mathematical model to assess the impact of emission processes on the dynamics of the state of building № 3 (cell) of the Kyiv Pechersk Lavra. Seismic-acoustic monitoring of the microseismic background of critical points of the objects under investigation is conducted to obtain the spectral characteristics of the building № 3 (cell) of the Kyiv Pechersk Lavra under investigation and to analyze the observed data to forecast the dynamics of the object under investigation. A specialized seismic recorder, ZIR-2, developed and produced by the Ukrainian company "Roden", was used to record vibrations. The spectral ranges of the sensors are 0.5–600 Hz. It should be noted that the spectrum of the object under study is its stable characteristic, which changes when the mechanical parameters of the structure change, and it can be used to detect "age-related" changes in the structure during its life. It can be assumed that the fixed spectral characteristics of the structure can further be used as the set starting values for detecting the moment of its "aging", which can change during the monitoring process in case of accumulation of local damages.

The work's purpose is to evaluate the dynamics of high-frequency signals generated by cracks that occur during the operation of a building № 3 (cell) of the Kyiv Pechersk Lavra structure.

To evaluate the dynamics of high-frequency signals generated by cracks that occur during the operation of the building structure under investigation. To evaluate the dynamics of high-frequency signals generated by cracks that occur during the operation of the building structure under investigation, let us compare two observations of registered data. A significant change in the model parameters for two dimensions indicates a strong cracking emission, which can lead to undesirable consequences for the operation of the building structure under study.

The first observation. To assess the dynamics of the emission intensity generated by cracking in the observation area, we will carry out the first observations using the parametric model (1–4), Fig. 1–4. The dynamics of the parameters of this model will characterize the dynamics of emission of crack formation in the structure of building # 3 (cell) of the Kyiv Pechersk Lavra under study.

The first observation of the building № 3 (cell) of the Kyiv Pechersk Lavra is given below.

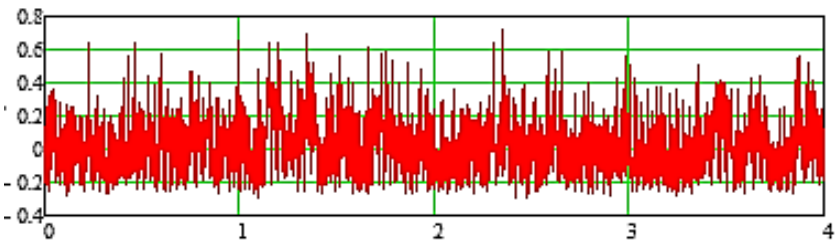

Fig. 1. A fragment of the recording of the first observation (duration 4 seconds) of the building's reaction to the natural background. The abscissa shows time in seconds. Along the ordinate axis, the function of the acceleration of the structure's oscillations in m/sec^2 is plotted with precision to the multiplier

Data registration during seismic-acoustic monitoring is accompanied by simultaneous additive interference caused by external factors. This study used frequency filtering for data preprocessing (Mostovoy, S., & Mostovoy, V., 2011).

Figures 1 and 2 show fragments of the recording of the first observation lasting 4 seconds, the response of the building № 3 (cell) of the Kyiv Pechersk Lavra to the natural background, unfiltered (Fig. 1) and filtered (Fig. 2).

ISSN 2707-1758

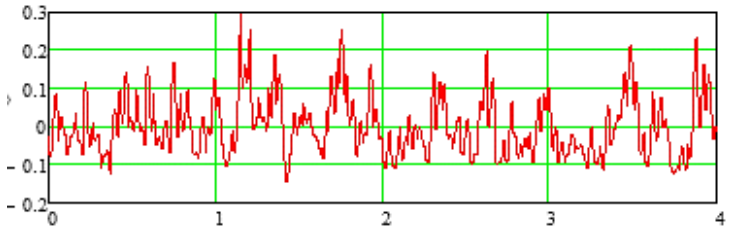

Fig. 2. A fragment of a filtered recording of the first observation (duration 4 seconds) of the building's reaction to the natural background. On the abscissa axis, the time is present in seconds. Along the ordinate axis, the function of the acceleration of oscillation of the structure m/sec^2 is plotted with precision to the multiplier

The Figure 3 shows the Amplitude of the module of the Fourier spectrum of the low-pass filtered data of building № 3 (cell) of the Kyiv Pechersk Lavra seismic records.

The frequency range was from 90 Hz to 500 Hz. It was divided into five equal quantiles (4), each into five equal subranges.

The Figure 4 shows the Fourier amplitude of the filtered data of the first range of the first observation of building № 3 (cell) of the Kyiv Pechersk Lavra. The energy of each of the twenty sub bands was presented in a matrix of the first observation 5×5.

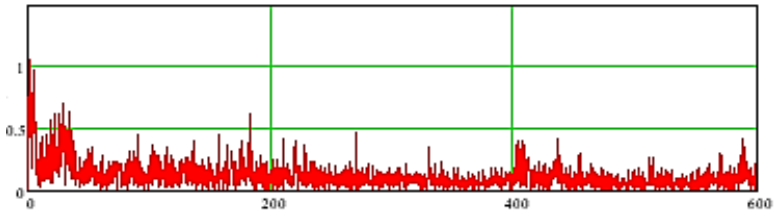

Fig. 3. The amplitude of the module of the Fourier spectrum of the filtered data of the first observation in relative units, in the frequency range from 0 to 600 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

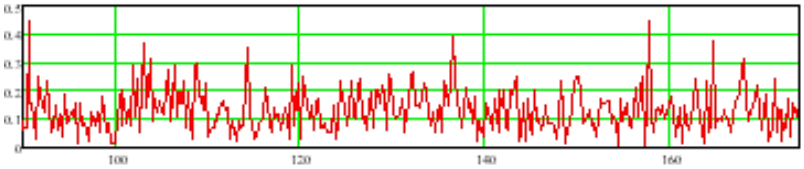

Fig. 4. The amplitude of the module of the Fourier spectrum of the filtered data of the first range in relative units, in the frequency range from 90 to 170 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 5 shows the amplitude of the module of the Fourier spectrum of the filtered data of the first subband of the first band presented in relative units, in the frequency range from 90 to 105 Hz.

The Figure 6 shows the amplitude of the module of the Fourier spectrum of the filtered data of the second subband of the first band presented in relative units, in the frequency range from 105 to 125 Hz.

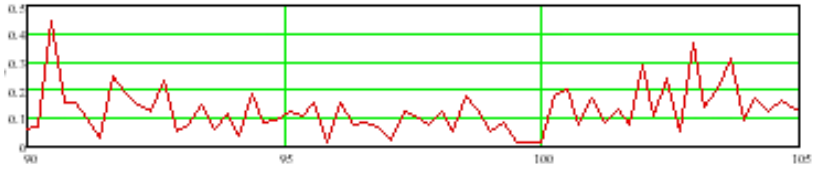

Fig. 5. The amplitude of the module of the Fourier spectrum of the filtered data of the first subband of the first band in relative units, in the frequency range from 90 to 105 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

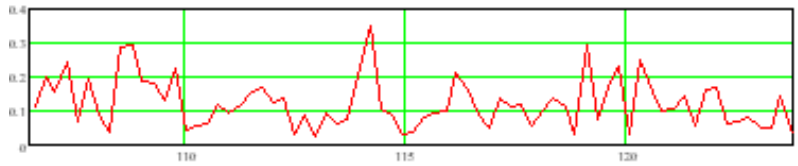

Fig. 6. The amplitude of the module of the Fourier spectrum of the filtered data of the second subband of the first band in relative units, in the frequency range from 105 to 125 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 7 shows the amplitude of the module of the Fourier spectrum of the filtered data of the third subband of the first band presented in relative units, in the frequency range from 125 to 140 Hz.

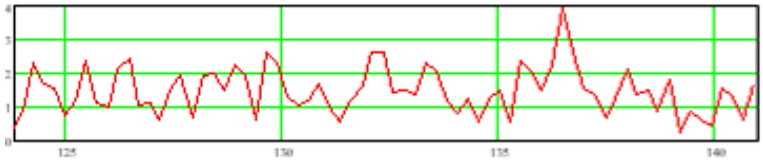

Fig. 7. The amplitude of the module of the Fourier spectrum of the filtered data of the third subband of the first band in relative units, in the frequency range from 125 to 140 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 8 shows the amplitude of the module of the Fourier spectrum of the filtered data of the fourth subband of the first band presented in relative units, in the frequency range from 140 to 155 Hz.

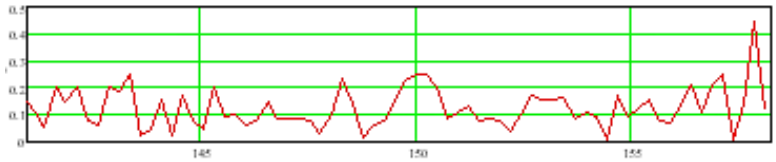

Fig. 8. The amplitude of the module of the Fourier spectrum of the filtered data of the fourth subband of the first band in relative units, in the frequency range from 140 to 155 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 9 shows the amplitude of the module of the Fourier spectrum of the filtered data of the fourth subband of the first band presented in relative units, in the frequency range of 155 to 170 Hz.

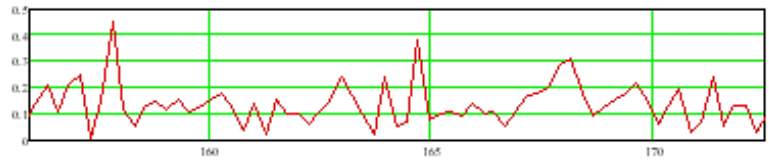

Fig. 9. The amplitude of the module of the Fourier spectrum of the filtered data of the fourth subband of the first band in relative units, in the frequency range from 155 to 170 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 10 shows the Fourier amplitude of the filtered data of the first range of the first observation. The energy of each of the twenty subbands was presented in a matrix of the first observation 5×5.

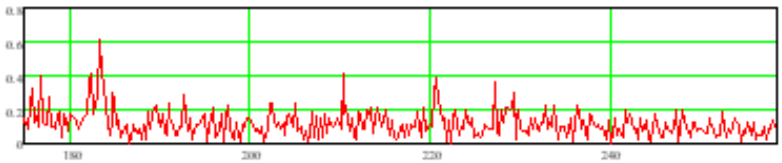

Fig. 10. The amplitude of the module of the Fourier spectrum of the filtered data of the second range of first observation in relative units, in the frequency range. from 170 to 250 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 11 shows the Fourier amplitude of the filtered data of the first range of the first observation. The energy of each of the twenty subbands was presented in a matrix of the first observation 5×5.

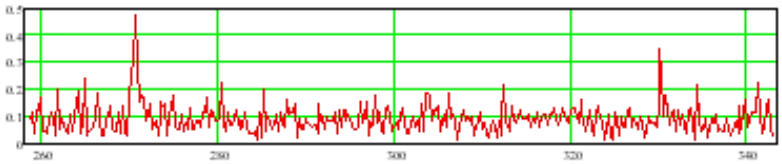

Fig. 11. The amplitude of the module of the Fourier spectrum of the filtered data of the second range of first observation in relative units, in the frequency range from 250 to 330 0 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

ISSN 2707-1758

The Figure 12 shows the Fourier amplitude of the filtered data of the first range of the first observation. The energy of each of the twenty subbands was presented in a matrix of the first observation 5×5.

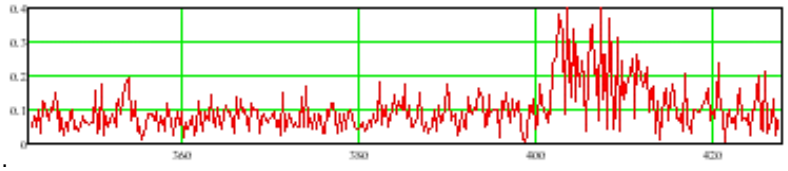

Fig. 12. The amplitude of the module of the Fourier spectrum of the filtered data of the second range of first observation in relative units, in the frequency range from 340 to 420 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 13 shows the amplitude of the module of the Fourier spectrum of the filtered data of the second range of first observation in relative units, in the frequency range from 420 to 500 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units.

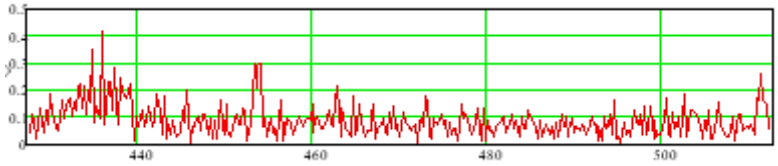

Fig. 13. shows the Fourier amplitude of the filtered data of the first range of the first observation. The energy of each of the twenty subbands was presented in a matrix of the first observation 5×5

The Figure 14 shows the Fourier amplitude of the filtered data of the first range of the first observation. The energy of each of the twenty subbands was presented in a matrix of the first observation 5×5.

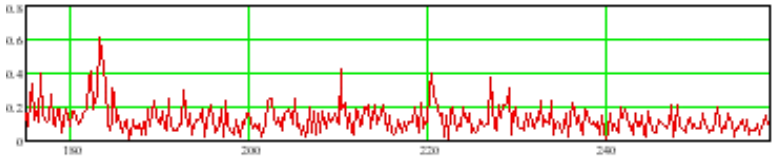

Fig. 14. The amplitude of the module of the Fourier spectrum of the filtered data of the second range of first observation in relative units, in the frequency range from 170 to 250 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 15 shows the Fourier amplitude of the filtered data of the first range of the first observation. The energy of each of the twenty subbands was presented in a matrix of the first observation 5×5.

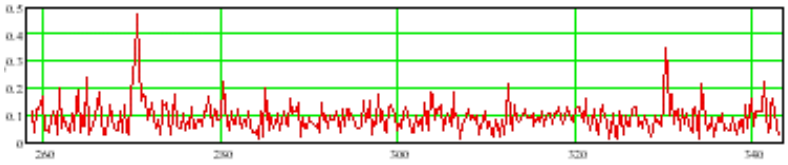

Fig. 15. The amplitude of the module of the Fourier spectrum of the filtered data of the second range of first observation in relative units, in the frequency range from 250 to 330 0 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 16 shows the Fourier amplitude of the filtered data of the first range of the first observation. The energy of each of the twenty subbands was presented in a matrix of the first observation 5×5.

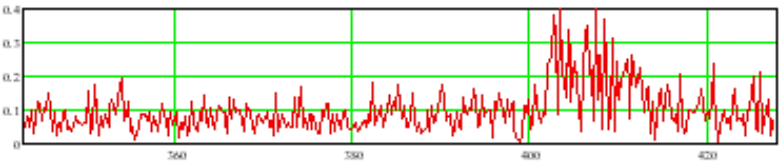

Fig. 16. The amplitude of the module of the Fourier spectrum of the filtered data of the second range of first observation in relative units, in the frequency range from 340 to 420 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 17 shows the Fourier amplitude of the filtered data of the first range of the first observation. The energy of each of the twenty subbands was presented in a matrix of the first observation 5×5. The energy of each of the twenty sub bands was presented in a matrix 5×5, table 1.

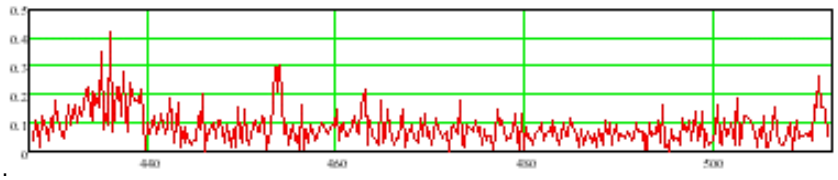

Fig. 17. The amplitude of the module of the Fourier spectrum of the filtered data of the second range of first observation in relative units, in the frequency range from 420 to 500 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

Table 1

Matrix of energy size 5×5 of quintiles of all 25 subbands of the first observation of the first observation

2.3054	2.7727	1.8019	1.2790	2.1570
2.1405	1.8973	1.4254	1.2361	1.5053
2.5438	2.2818	1.5132	1.3459	1.3412
2.1597	2.0464	1.4520	2.7071	1.0495
2.2884	1.5792	1.5325	1.6143	1.2925

The second observation. To assess the dynamics of the emission intensity generated by cracking in the observation area, we will carry out the second observations using the parametric model (1–4) to study building № 3 (cell) of the Kyiv Pechersk Lavra.

The second observation of the building № 3 (cell) of the Kyiv Pechersk Lavra is given below.

Data registration during seismic-acoustic monitoring is accompanied by simultaneous additive interference caused by external factors. This study used frequency filtering for data preprocessing (Mostovoy, S., & Mostovoy, V., 2011).

Figures 18 and 19 show fragments of the recording of the second observation lasting 4 seconds, the response of the building to the natural background, unfiltered (Fig.18) and filtered (Fig. 19).

On the Figure 20 the Amplitude of the module of the Fourier spectrum of the low-pass filtered data is shown.

The frequency range was from 90 Hz to 500 Hz. It was divided into five equal quantiles (4), each into five equal subranges.

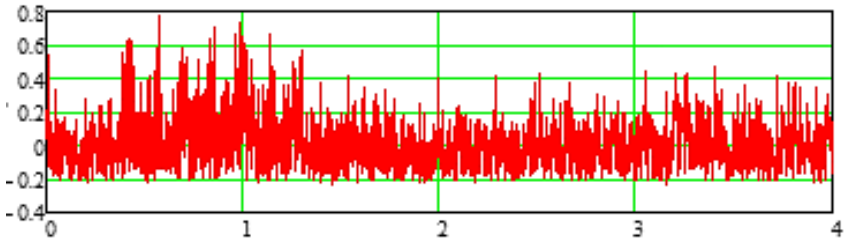

Fig. 18. A fragment of the recording of the second observation (duration 4 seconds) of the building's reaction to the natural background. The abscissa shows time in seconds. Along the ordinate axis, the function of the acceleration of the structure's oscillations in m/sec^2 is plotted with precision to the multiplier

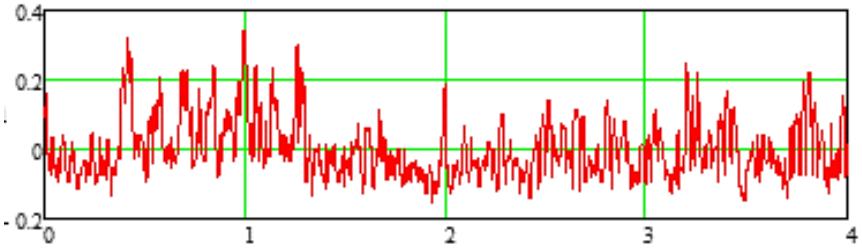

Fig. 19. A fragment of a filtered recording of the second observation (duration 4 seconds) of the building's reaction to the natural background. On the abscissa axis, the time is present in seconds. Along the ordinate axis, the function of the acceleration of oscillation of the structure m/sec^2 is plotted with precision to the multiplier

ISSN 2707-1758

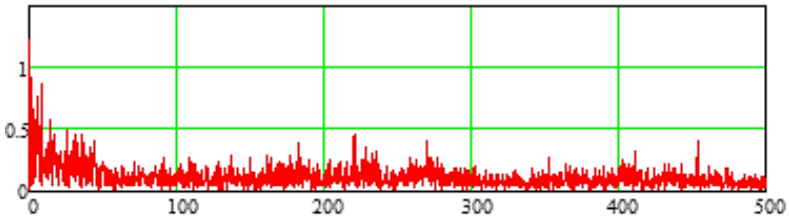

Fig. 20. The amplitude of the module of the Fourier spectrum of the filtered data of the second observation in relative units, in the frequency range from 0 to 600 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 21 shows the Fourier amplitude of the filtered data of the first range of the first observation. The energy of each of the twenty sub bands was presented in a matrix of the first observation 5×5.

Fig. 21. The amplitude of the module of the Fourier spectrum of the filtered data of the first range of the second observation in relative units, in the frequency range from 90 to 170 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 22 shows the amplitude of the module of the Fourier spectrum of the filtered data of the first subband of the first band presented in relative units, in the frequency range from 90 to 105 Hz.

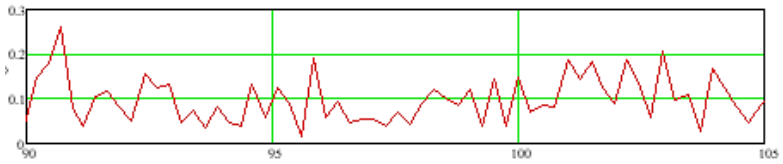

Fig. 22. The amplitude of the module of the Fourier spectrum of the filtered data of the first subband of the first band in relative units, in the frequency range from 90 to 105 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 23 shows the amplitude of the module of the Fourier spectrum of the filtered data of the second subband of the first band presented in relative units, in the frequency range from 105 to 125 Hz.

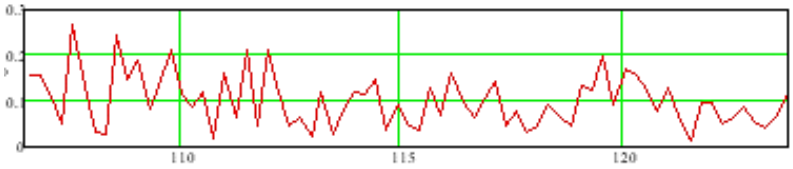

Fig. 23. The amplitude of the module of the Fourier spectrum of the filtered data of the second subband of the first band in relative units, in the frequency range from 105 to 125 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 24 shows the amplitude of the module of the Fourier spectrum of the filtered data of the third subband of the first band presented in relative units, in the frequency range from 125 to 140 Hz.

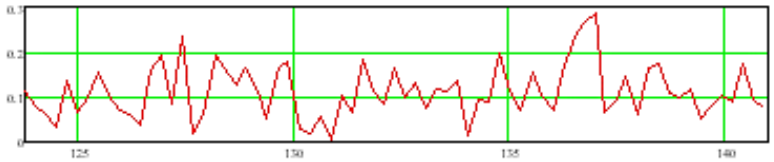

Fig. 24. The amplitude of the module of the Fourier spectrum of the filtered data of the third subband of the first band in relative units, in the frequency range from 125 to 140 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 25 shows the amplitude of the module of the Fourier spectrum of the filtered data of the fourth subband of the first band presented in relative units, in the frequency range from 140 to 155 Hz.

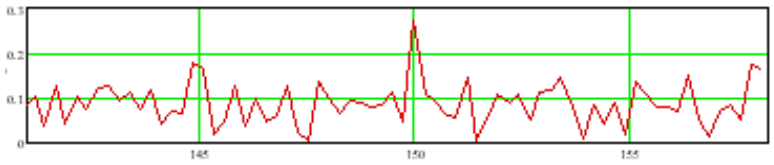

Fig. 25. The amplitude of the module of the Fourier spectrum of the filtered data of the fourth subband of the first band in relative units, in the frequency range from 140 to 155 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 26 shows the amplitude of the module of the Fourier spectrum of the filtered data of the fourth subband of the first band presented in relative units, in the frequency range of 155 to 170 Hz.

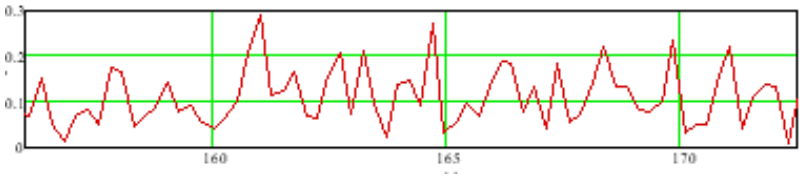

Fig. 26. The amplitude of the module of the Fourier spectrum of the filtered data of the fourth subband of the first band in relative units, in the frequency range from 155 to 170 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 27 shows the Fourier amplitude of the filtered data of the first range of the second observation. The energy of each of the twenty subbands was presented in a matrix of the first observation 5×5.

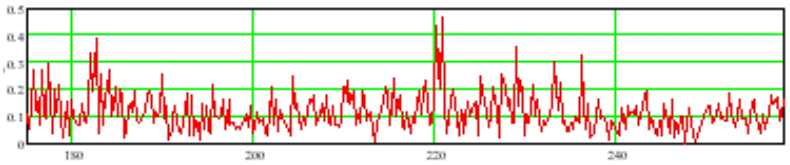

Fig. 27. The amplitude of the module of the Fourier spectrum of the filtered data of the second range of first observation in relative units, in the frequency range from 170 to 250 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 28 shows the Fourier amplitude of the filtered data of the first range of the second observation. The energy of each of the twenty subbands was presented in a matrix of the first observation 5×5.

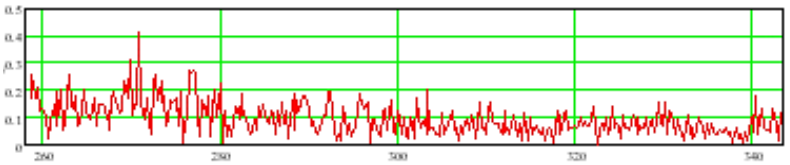

Fig. 28. The amplitude of the module of the Fourier spectrum of the filtered data of the second range of first observation in relative units, in the frequency range from 250 to 330 0 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

The Figure 29 shows the Fourier amplitude of the filtered data of the first range of the second observation. The energy of each of the twenty subbands was presented in a matrix of the first observation 5×5.

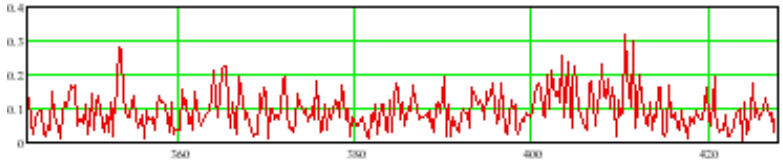

Fig. 29. The amplitude of the module of the Fourier spectrum of the filtered data of the second range of first observation in relative units, in the frequency range from 340 to 420 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

ISSN 2707-1758

The Figure 30 shows the Fourier amplitude of the filtered data of the first range of the second observation. The energy of each of the twenty subbands was presented in a matrix of the first observation 5×5, table 2.

Similarly, the energy matrix of 25 subbands was obtained for the second recording fragment.

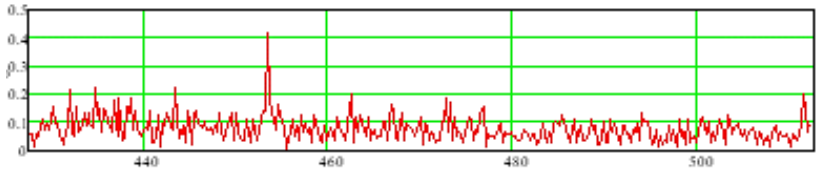

Fig. 30. The amplitude of the module of the Fourier spectrum of the filtered data of the second range of first observation in relative units, in the frequency range from 420 to 500 Hz. The frequency in Hertz is given on the abscissa. The y-axis shows the range amplitude in relative units

Table 2

Matrix of the energy size 5×5 of the quantiles of all 25 subbands of the second fragment of the recording Fig. 14

2.2574	2.7012	1.7931	1.3520	2.2752
2.0735	1.9259	1.4074	1.2935	1.4875
2.4780	2.2015	1.4257	1.3129	1.4590
2.2745	2.6549	1.9350	2.0250	1.1487
2.3582	1.6940	1.7253	1.1542	1.9537

Discussion and conclusions

The strength characteristics of any object depend on its spectral characteristics, that is, the possibility of propagation of elastic waves with different parameters. The structural failure of the material consists in the loss of the load-bearing capacity of the element or directly of the entire structure. It begins when the stresses in the material approach the limit, causing excessive deformations, when the material does not return to its initial state during the entire cycle. Cyclic stresses should lead to material fatigue. Fatigue leads to irreversible deformations. The aging process in the proposed model is a change in material parameters reflected in the feature space.

It is advisable to use emission dynamics to assess the dynamics of high-frequency signals generated by cracks that arise during the structure's operation. For an adequate assessment of the emission dynamics generated by microcracks, it is natural to use an algorithm based on the theorem for processes that are stationary in the sense of (1)–(3). Two stages of the study of the dynamics of the emission of the building are generated by the occurrence of microcracks using the algorithm based on the theorem for processes that are stationary in the sense of (1)–(3). Showed that for a given time interval, the change in emission characteristics was reflected in the energy size matrix of the quantiles of all 25 subbands of each of the two research fragments, Fig. 1, 2.

For an adequate assessment of the emission dynamics generated by cracks that occur during the operation of the structure, it is necessary to collect statistics on a time interval of decades. To solve this problem, it is necessary to carry out permanent seismшс-acoustic monitoring of the building structure.

The authors acknowledge the funding received by the National Research Foundation of Ukraine from the state budget 2022.01/0209 "Complex research of the geoecological state of preservation of the historical and cultural heritage objects of the National Reserve "Kyiv-Pechersk Lavra" in the conditions of military operations" (NRFU Competition "Science for the Recovery of Ukraine in the War and Post-War Periods").

References

Mostovoy, S., & Mostovoy, V. (2011). Problems of filtration at geophysical information processing. *Geoinfomatika*, 2, 48–52 [in Ukranian]. [Мостовой, С., & Мостовой, В. (2011). Проблеми фільтрації при обробці геофізичної інформації. *Геоінфоматика*, 2, 48–52].

Mostovoy, V., & Mostovoy, S. (2023). Models of optimization of dynamic parameters of the object in passive monitoring. *Cybersecurity: Education, Science, Technology,* 28(5), 112–123 [in Ukranian]. [Мостовой, В., & Мостовой, С. (2023). Моделі оптимізації динамічних параметрів об'єкта при пасивному моніторингу. *Кібербезпека: освіта, наука, техніка,* 28(5), 112–123].

Mostovyy, V. (2013). *Models of geophysical field monitoring systems* [Dissertation for the degree of Doctor of Physical and Mathematical Sciences] Kyiv National University of Construction and Architecture [in Ukranian]. [Мостовий, В. (2013). Моделі систем геофізичного моніторингу поля [Дис. д-ра фіз.-мат. наук] Київський національний університет будівництва і архітектури.

Schijve, J. (2003). Fatigue of structures and materials in the 20th century and the state of the art. *International Journal of Fatigue*, 25(8), 679–702.

Suresh, S. (2004). *Fatigue of Materials*. Cambridge University Press.

Tassios T. (2010). Seismic engineering of monuments. *Bulletin of earthquake engineering*, 8(6), 1231–1265.

Timoshenko, S., & Gere, J. (1961). *Theory of elastic stability* (2nd ed). McGraw-Hill.

Отримано редакцією журналу / Received: 01.12.24
Прорецензовано / Revised: 05.12.24
Схвалено до друку / Accepted: 08.12.24

Василь МОСТОВИЙ, д-р фіз-мат. наук, провід. наук. співроб.
ORSID ID: 0000-0002-1759-1893
e-mail: vasyl.mostovyy@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

МАТЕМАТИЧНА МОДЕЛЬ ДИНАМІКИ ВИПУСКАННЯ СИГНАЛУ В СИСТЕМАХ СЕЙСМОАКУСТИЧНОГО МОНІТОРИНГУ БУДІВЕЛЬНИХ КОНСТРУКЦІЙ

В с т у п . ***Представлено математичну модель автоматизованих систем сейсмоакустичного моніторингу будівельних конструкцій, яка дозволить оцінити динаміку утворення тріщин у будівельних конструкціях із метою попередження руйнування досліджуваних об'єктів. Сейсмоакустичне поле, яке генерують об'єкти дослідження, відображається в матрицю інформативних параметрів, динаміка якої характеризує динаміку стану об'єкта. Для оцінювання динаміки високочастотних сигналів, які генеруються тріщинами, що виникають у процесі експлуатації споруди, доцільно використовувати динаміку емісії, яку породжують ці сигнали. Для цього, з погляду фізичної доцільності, має сенс вибору моделі, яка характеризує динаміку високочастотного діапазону спектра. А саме, в роботі представлено алгоритм, заснований на теоремі для стаціонарних у широкому сенсі процесів.***

М е т о д и . ***Процес старіння може бути відображений у простір ознак, який може бути зведений до множини параметрів, що характеризують пружні властивості матеріалів, які формують досліджувані об'єкти. Оскільки швидкості розповсюдження та форма поздовжніх і поперечних хвиль у матеріалі залежать від пружних параметрів цих матеріалів (коефіцієнта Пуассона та модуля Юнга), то зміна вказаних параметрів призводить до змін спектральних характеристик емісійних сигналів, які виникають у старіючому матеріалі. Будь-який перерозподіл енергії у матеріалі супроводжується виникненням сигналів, що генерують емісію. Динаміка параметрів сигналу емісії відображає зміну пружних властивостей досліджуваного об'єкта. Можливі причини змін внутрішньої структури – це виникнення та збільшення тріщин, фазові переходи в монолітних матеріалах і розпушення складових. Це означає, що зміни динамічних параметрів сигналів емісії пов'язані з динамічними характеристиками вказаного об'єкта.***

Р е з у л ь т а т и . ***Запропоновано математичну модель старіння будівельної конструкції. Ця модель старіння об'єкта має враховувати природу зовнішніх впливів на об'єкт і природу його реакції на зовнішні збурення. З урахуванням наявності стохастичного фонового шуму під час моніторингу, у моделі слід прийняти лише статистичний характер цієї залежності. Вказану модель реалізовано на корпусі № 3 (келії) Києво-Печерської лаври.***

В и с н о в к и . ***Два етапи дослідження динаміки емісії корпусу № 3 Києво-Печерської лаври показали, що за даний інтервал часу зміна характеристик емісії цього об'єкта перебуває в межах похибки вимірювання. Отже, для адекватного оцінювання динаміки емісії, що генерується тріщинами, які виникають у процесі експлуатації корпусу № 3 Києво-Печерської лаври, необхідно використовувати статистику на інтервалі часу в кілька десятиліть. Для розв'язання цієї задачі необхідно проводити постійний сейсмоакустичний моніторинг будівельної конструкції.***

К л ю ч о в і с л о в а : ***сейсмоакустичний моніторинг, сейсмоакустична емісія, математична модель, сейсмоакустичний сигнал, матриця інформативних параметрів моделі, старіння конструкцій.***

Автор заявляє про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The author declares no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.

Наукове видання

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

№ 2(8)/2024

Редактор *Л. Магда*

Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, економіко-статистичних даних, власних імен та інших відомостей. Редколегія залишає за собою право скорочувати та редагувати подані матеріали.

Оригінал-макет виготовлено Видавничо-поліграфічним центром "Київський університет"
Виконавець *В. Гаркуша*

Формат 60x84$^{1/16}$. Обл.-вид. арк. 9,8. Ум. друк. арк. 10,0. Наклад 100. Зам. № 225-11257.
Гарнітура Times New Roman. Папір офсетний. Друк офсетний. Вид. № Іт2.
Підписано до друку 21.03.2025

Видавець і виготовлювач
ВПЦ "Київський університет",
б-р Тараса Шевченка, 14, м. Київ, 01601, Україна
☎ (38044) 239 32 22; (38044) 239 31 72; тел./факс (38044) 239 31 28
e-mail: vpc_div.chief@univ.net.ua; redaktor@univ.net.ua
http: vpc.knu.ua
Свідоцтво суб'єкта видавничої справи ДК № 1103 від 31.10.02