

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

22 листопада 2024 року



КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

**МАТЕРІАЛИ
V МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

**МАТЕРІАЛИ V МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

22 листопада 2024 року, м. Одеса

Одеса, 2024

**MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity**

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

**MATERIALS OF THE V INTERNATIONAL
SCIENTIFIC AND PRACTICAL CONFERENCE**

November 22, 2024, Odesa

Odesa, 2024

УДК 340.12:316.3**Відповідальній редактор:**

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій,
кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу
несуть учасники конференції, їхні наукові керівники,
які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 25.11.2024 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 22 листопада 2024 р.). Одеса, 2024. 289 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

Редакційна колегія:

ГОРБАЧЕНКО Станіслав, д.е.н., професор

СОКОЛОВ Артем, д.т.н., професор

АХМАМЕТЬЄВА Ганна, к.т.н., доцент

РАЗІНКІН Нікіта, асистент кафедри

UDC 340.12:316.3**Editor-in-chief:**

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/25/2024)

Materials of the International Scientific and Practical Conference «Cybersecurity in the
Modern World: Current Challenges» (Odessa, November 22, 2024). Odesa, 2024. 289 p.

The conference was attended by students, postgraduates, young scientists, teachers
and researchers. The conference is held at the National University «Odesa Law
Academy».

Editorial Board:

GORBACHENKO Stanislav, Doctor of Economics, Professor

SOKOLOV Artem, Doctor of Engineering, Professor

AKHMAMETYEVA Anna, Candidate of Engineering, Associate Professor

RAZINKIN Nikita, Assistant

V Міжнародна науково-практична конференція**«Кібербезпека в сучасному світі:
актуальні виклики»****22 листопада 2024 року****ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:****Секція 1. Алгоритмічні та технічні аспекти кібербезпеки****Секція 2. Штучний інтелект та інформаційні технології в задачах кібербезпеки****Секція 3. Управлінські, соціальні та психологічні аспекти кібербезпеки****Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації****СКЛАД ПРОГРАМНОГО КОМІТЕТУ КОНФЕРЕНЦІЇ:****Доц. Дикий О.В.**, НУ “Одеська юридична академія”, Україна**Проф. Горбаченко С.А.**, НУ “Одеська юридична академія”, Україна**Проф. Казакова Н.Ф.**, НУ “Одеська юридична академія”, Україна**Доц. Соколов А.В.**, НУ “Одеська юридична академія”, Україна**Проф. Евсеев С.П.**, НТУ «Харківський політехнічний інститут», Україна**Проф. Ткач Ю.М.**, НУ “Чернігівська політехніка”, Україна**Проф. Опірський І.Р.**, НУ “Львівська Політехніка”, Україна**Проф. Шелест М.Є.**, НУ “Чернігівська політехніка”, Україна**Проф. Mikolaj Karpinski**, University of the National Education Commission, Польща**Проф. Немкова О.А.**, НУ “Львівська Політехніка”, Україна**E-mail: kiberprostirconf@gmail.com (Для питань та тез)**

V International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

22 November 2024 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies in cybersecurity tasks

Section 3. Management, social and psychological aspects of cybersecurity

Section 4. Regulatory and legal principles of cybersecurity and information protection

PROGRAM COMMITTEE OF THE CONFERENCE:

Assoc. Prof. **Dykyi O.V.**, NU "Odesa Law Academy", Ukraine

Prof. **Gorbachenko S.A.**, NU "Odesa Law Academy", Ukraine

Prof. **Kazakova N.F.**, NU "Odesa Law Academy", Ukraine

Assoc. Prof. **Sokolov A.V.**, NU "Odesa Law Academy", Ukraine

Prof. **Evseev S.P.**, National Technical University "Kharkiv Polytechnic Institute", Ukraine

Prof. **Tkach Yu.M.**, Chernihiv Polytechnic National University, Ukraine

Prof. **Opirskyi I.R.**, Lviv Polytechnic National University, Ukraine

Prof. **Shelest M.E.**, Chernihiv Polytechnic National University, Ukraine

Prof. **Mikolaj Karpinski**, University of the National Education Commission, Poland

Prof. **Nemkova O.A.**, Lviv Polytechnic National University, Ukraine

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

**Шановні учасники щорічної
Міжнародної науково-практичної конференції
«Кібербезпека в сучасному світі:
актуальні виклики» !**

Сьогодні, коли минуло вже тисяча днів з початку повномасштабного вторгнення ми, як ніколи, усвідомлюємо важливість кібербезпеки. Кіберпростір, що раніше сприймався переважно як технічний інструмент чи канал обміну інформацією, перетворився на стратегічну арену, де інформаційні впливи та технологічні рішення визначають майбутнє безпеки, управління і соціального розвитку. Нові загрози національній безпеці також, все частіше пов'язані саме зі швидким розвитком технологій. І вони потребують консолідації знань, інноваційних підходів і міжнародного співробітництва.

Сьогодні ми стикаємося з новими, нетиповими загрозами національній та глобальній безпеці, пов'язаними зі швидкою трансформацією технологій, кібератаками на критично важливі інфраструктури, порушенням інформаційних прав людей та поширенням дезінформації, здатної підривати довіру до державних інституцій та суспільних цінностей. Ця багатовимірність проблем спонукає нас переосмислити кібербезпеку, виходячи за межі вузького технічного бачення, залучаючи правові, економічні, соціально-психологічні та управлінські підходи.

Прагнення адаптуватися до нових реалій в умовах війни та глобальних викликів, що постають у XXI столітті, вимагає консолідації міжнародних зусиль та розвитку міждисциплінарних досліджень. Від технічних фахівців, що розробляють інноваційні протоколи захисту інформаційних систем, до науковців-юристів, котрі формують правові стандарти регулювання цифрового простору, від економістів, які аналізують вартість кібератак для бізнесу та держави, до психологів, що досліджують вплив кіберзагроз на суспільну свідомість – усі вони мають працювати спільно. Лише так можна створити комплексну систему протидії тим викликам, котрі надходять із безмежного та динамічного кіберпростору.

Наше місто, Одеса, здавна славиться потужним інтелектуальним, науковим та культурним потенціалом, а також динамічним ІТ-сектором. Національний університет «Одеська юридична академія», як впливовий центр науки і освіти, пропонує платформу для об'єднання зусиль дослідників і практиків із різних країн та галузей.

Ми сподіваємося на подальшу плідну роботу, обмін знаннями, ідеями та досвідом, як з боку представників наукової спільноти, так і від фахівців-практиків щодо максимально ефективного захисту кіберпростору.

*Президент Національного університету
«Одеська юридична академія»,
академік НАПрН України, академік НАПН України
доктор юридичних наук, професор,
Заслужений юрист України*

Сергій КІВАЛОВ

Секція 1. АЛГОРИТМІЧНІ ТА ТЕХНІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ

АНАЛІЗ СТІЙКОСТУ ПОТОЧНОГО ШИФРУ RC4

Щербина Юрій

*доцент кафедри інформаційних технологій Національного університету
«Одеська юридична академія»*

Казакова Надія

*професор кафедри кібербезпеки Національного університету
«Одеська юридична академія»*

Фразе-Фразенко Олексій

*доцент кафедри кібербезпеки Національного університету
«Одеська юридична академія»*

Постановка проблеми

Алгоритм потокового шифрування RC4 було запропоновано Рональдом Рівестом у 1987 році для компанії RSA Data Security. Достатньо довго він був популярним стандартом шифрування і використовувався у схемі Wireless Equivalency Protection (WEP), а також у деяких версіях специфікації SSL. Цей шифр забезпечував високу швидкість шифрування, був простим у розумінні та програмній реалізації і, в той же час, не висував ніяких специфічних вимог до апаратного забезпечення. Не зважаючи на те, що виявлені в ньому слабкі місця, не дозволяють використовувати його в сучасних системах з високими вимогами до захисту, його модифіковані версії до цієї пори залишаються криптографічно безпечними для великої кількості програмних застосунків.

Особливістю потокового шифру RC4 є те, що для генерації шифруючої гами він використовує ключове слово, довжина якого може мінятися від 40 до 256 бітів, а сам процес шифрування зводиться до звичайного гамування відкритого тексту послідовністю, створеною на основі оригінального власного генератора псевдовипадкових чисел.

Ціль дослідження

Для виявлення меж використання, все ще популярного шифру RC4, необхідно провести аналіз відомих описаних типів атак на його слабкі місця та визначити можливі способи протидії, зроблять його використання безпечним.

Атаки на шифр RC4 та способи захисту від них

Як відомо, алгоритм шифрування RC4 складається з двох частин: алгоритму планування ключів (key-scheduling algorithm або KSA) та ініціалізації S-блоку а також алгоритму генерації шифруючої гами (pseudo-random generation algorithm або PRGA) [1]. Спочатку на основі введеного ключа фор-

мується масив S великої довжини, а потім, використовуючи спеціальну перестановку, з нього відбирають вихідні байти, що утворюють псевдовипадкову послідовність для гамування. Саме простота цього алгоритму та висока якість вихідної шифруючої гами до цих пір забезпечують популярність цього шифру.

Першою вразливістю шифру RC4, що була знайдена Андрю Рузом, є кореляція байтів шифруючої гами з першими байтами ключа та їх лінійними комбінаціями. В середині 2000 років було запропоновано алгоритм, який використовуючи цю залежність, дозволяє відновити ключ без будь яких даних про його можливе значення. Але проблема полягає в тому, що час на його реалізацію, складає корінь квадратний від складності повного перебору [2].

Іншою модифікацією цієї вразливості є залежність перших байтів ключового потоку від змісту введеного ключа. Якщо ключ використовується не одноразово, то його значення з високою долею ймовірності може бути визначене на основі аналізу великої кількості перехоплених повідомлень [3]. Саме це слабке місце було використано під час вдалої атаки на протокол стандарту бездротових мереж IEEE 802.11, що й вимусило вносити відповідні зміни для підвищення безпеки інформаційного обміну. Саме в цій роботі автори запропонували відкидати початкову частину зформованої генератором шифруючої гами.

Для виконання атаки, побудованої на використанні цього типу вразливості шифру, необхідно знати перше вихідне псевдовипадкове слово K та m байтів вхідного ключа. Це дає можливість отримати $m + 1$ байт ключа. Ітераційно повторюючи цю процедуру можна отримати весь ключ.

В роботі [4] було зроблено спробу обґрунтувати на основі теорії випадкових перестановок спосіб оцінки кількості байтів, що мають бути відкинутими для забезпечення захисту від атак описаного типу. А саме було вказано, що кількість відкинутих байтів має складати величину не меншу за 512 байт.

В роботі [5] було запропоновано більш досконалий тип описаної вище ітераційної атаки, що також дозволяє визначати зміст використаного ключа, а також були наведені пропозиції щодо підвищення захищеності самого алгоритму RC4, а саме було запропоновано використання зворотного алгоритму ключового розкладу.

Висновки

Сьогодні існує велика кількість робіт, присвячених описанню слабкості шифру RC4, але більшість з них мають, скоріш за все, теоретичний характер. Враховуючи, що шифр є поточним і використовується здебільшого в реальному масштабі часу, наприклад в мобільному зв'язку, організація в такому режимі на нього описаних атак, стає майже не реальною через те, що для цього необхідні неприйнятно високі обчислювальні ресурси. Зазвичай вони

займають не менше 2000 годин, а це зовсім неприйнятно. Саме через це по оцінкам експертів, до 30% сеансів зв'язку по протоколу TLS захищається шифром RC4. Те саме можна сказати й про інші варіанти використання цього шифру в реальних масштабах часу, з високими вимогами до швидкодії та криптографічної стійкості.

Список використаних джерел:

1. Bruce Schneier. Applied Cryptography. 20th Anniversary Hardcover: ISBN 978-1-119-09672-6. 784 Pages. URL : <https://www.schneier.com/books/applied-cryptography/>.
2. Andrew Roos. Weak keys in RC4. Date: 07.11.2012. Message-ID: <44ebge\$If@hermes.is.co.za> Organization: Vironix-ZA URL: <https://web.archive.org/web/20120618200629/http://marcel.wanda.ch/Archive/WeakKeys>.
3. Scott Fluhrer, Itsik Mantin, Adi Shamir. Weaknesses in the Key Scheduling Algorithm of RC4. Conference series: International Workshop on Selected Areas in Cryptography. 20 December 2001. pp 1 – 24. URL : https://link.springer.com/chapter/10.1007/3-540-45537-X_1.
4. Mironov I. (Not so) random shuffles of RC4 (неопр.) // Lecture Notes in Computer Science. – 2002. – Т. 2442. – pp 304 – 319. – doi:10.1007/3-540-45708-9_20. 19.01.2010. URL: <https://eprint.iacr.org/2002/067.pdf>.
5. Klein A. Attacks on the RC4 stream cipher. Designs, codes and cryptography. – 2008. – Т. 48, № 3. – pp. 269-286. – doi:10.1007/s10623-008-9206-6. 02.04.2015. URL: <https://www.networklife.net/images/wep-rc4/RC4.pdf>.

Ключові слова: Симетричне шифрування, поточні шифри, шифр RC4, мобільний трафік.

Key words: Symmetric encryption, current ciphers, RC4 cipher, mobile traffic.

МОДЕЛЬ ВПЛИВУ КІБЕРЗАГРОЗ ТА КІБЕРАТАК НА ВІДНОВЛЕННЯ ФУНКЦІОНАЛЬНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ

Бойко Віктор

*доцент кафедри кібербезпеки Національного університету
«Одеська юридична академія», кандидат технічних наук*

Інформаційно-комунікаційна мережа (information communication network – ICN) з доступом до глобального інфопростору практично безперервно піддається несприятливим впливам і вражаючим факторам, істотну роль серед яких займають кібератаки та кіберзагрози різного роду та характеру [1]. При цьому сучасні ІКС апіорі є вразливими - що підтверджується довгим списком прецедентів, описаних у [2]. Практика захисту та відновлення функціонування ICN показує, що загальна тенденція до ускладнення, централізації, ієрархізації та недостатньо продуманих рішень при плануванні архітектури глобальних ICN призвели до того, що сучасні ICN втратили істотну частину своєї

гнучкості та здатності протистояти зовнішнім та внутрішнім впливам. Ускладнення також призвело до того, що на сучасному етапі однією зі складних проблем захисту ICN є не максимізація стійкості ICN до несприятливих впливів і вражаючих факторів, а мінімізація часу відновлення функціональності та працездатності ICN після інциденту. Найбільш показовим є випадок “Київстар”, який зміг відновити повну функціональність своєї мережі лише через 7 днів (з 12 до 20 грудня 2023 року [3], [4]).

Процес відновлення працездатності ICN являє собою поєднання різних факторів, що часто слабо піддаються оцінці. При відновленні працездатності обслуговуючий персонал може стикатися з проблемами різної природи та генези - недоліком запасних частин, дефіцитом дублюючих потужностей тощо, тощо. Можуть виникати важкопередбачувані вторинні ефекти, які мультиплікують загальні збитки та викликають вторинні за своєю природою збої в роботі, що ще більше ускладнює відновлення системи. Це особливо характерно для так званих мереж масового обслуговування, окремим випадком яких є ICN.

Приклад такого вторинного ефекту виникає в таких мережах при виході з ладу деякої кількості вузлів мережі. Оскільки мережа є гнучкою за своєю природою, то вихід одного або декількох вузлів не призводить до загального виходу з ладу мережі безпосередньо, однак, призводить до того, що користувачі, які втратили точки обслуговування, перенаправляють свої запити на інші вузли мережі. Загальне навантаження на ці вузли зростає, що насправді є “мирним” варіантом атаки на відмову (DDoS атаки). Якщо мережа спроектована без урахування цього ефекту, збільшення навантаження може призвести до відмови нових вузлів, що вціліли при первинному впливі. Вторинні відмови, у свою чергу, призводять до того, що зростає навантаження на вузли мережі, що залишилися - що веде до нової серії відмов. І так далі – процес може розвиватися аж до повної відмови мережі. У разі, якщо несприятливим впливам піддаються інформаційні системи, що обслуговують індустріальні та промислові комплекси, ризики та масштаби збитків багаторазово збільшуються [5].

У статті [2] було описано модель живучості мережі, яка ґрунтується на представленні мережі у вигляді сукупності віртуального або реального обладнання, які в рамках завдання розглядаються як граф вузлів, пов'язаних з'єднаннями різного характеру. Ці зв'язки між елементами можуть розглядатися як зв'язок по ресурсу, що відповідає категоріям живучості системи (“енергія” – “інформація” – “речовина”), а сама модель має структурно/функціональний акцент (“мережевий” за термінологією [1]). Також у моделі передбачено використання спеціальних, “віртуальних” вузлів, які моделюють причинно-наслідкові залежності та відносини між компонентами [6]). Це дозво-

ляє доповнити модель елементами багатофакторного аналізу. Кожен із вузлів системи може бути частиною ICN, її елементом, або окремим робочим компонентом робочої підсистеми. При цьому цей вузол в рамках моделі має характеристики, що включають час і характер відновлення елемента. У статті пропонувалась методика оцінки часу відновлення використовує безрозмірні позамасштабні оцінки “важливості”, “уразливості” елемента з точки зору загальної задачі мінімізації часу відновлення системи в цілому. Така оцінка традиційно спирається на критерій Бірнбаума [7] та ідеї, викладені в [8].

У роботі [8] розглянуто модель відновлення функціональності системи, в якій функція відновлення працездатності описана за допомогою диференціальних рівнянь. Рішення таких рівнянь для інтервалу часу, меншого, ніж чверть періоду рішення ($0; \pi/2$), в залежності від отриманих коефіцієнтів можна розділити на три основні категорії, кожна з яких відповідатиме режиму відновлення добре підготовленої, середньо підготовленої та погано підготовленої системи. При цьому добре підготовлена система описується експоненціальним законом, середньо підготовлена система – лінійним, погано підготовлена – тригонометричним – не дуже добре підготовлена система. При цьому під тригонометричним законом мається на увазі залежність, що відповідає першій чверті повного періоду синусоїдальної функції – на ділянці ($0; \pi/2$). Істотним моментом використання такої моделі є можливість як оцінки часу відновлення, і розгляд різних сценаріїв розвитку подій - зокрема каскадного виходу мережі з ладу, описаного вище.

У цій доповіді пропонується доповнити модель, щоб розширити її можливості щодо оцінки вторинних сценаріїв та наслідків кіберзагроз, додавши фактор контрольованого ризику виходу з ладу окремих компонентів системи. Для цього характеристики вузлів когнітивно-імітаційної моделі доповнюються спеціальною характеристикою, яка моделює ризик виходу з ладу компонента на кожному кроці моделювання процесу усунення несправностей та відновлення працездатності системи. Ця величина в залежності від цілей і завдань моделювання може характеризуватись різними за характеристиками розподілу (Нормальне, Вейбулла різних порядків), а в спрощеній моделі може бути представлена математичним очікуванням.

Список використаних джерел:

1. Bi W., MacAskill K., Schooling J. Old wine in new bottles? Understanding infrastructure resilience: Foundations, assessment, and limitations // *Transportation Research Part D: Transport and Environment*. — Elsevier BV, 2023. — Vol. 120. — P. 103–793.
2. Бойко В., Василенко М., Слатвінська В. Моделювання живучості та відновлення інформаційно-комунікаційних мереж в умовах дії кіберзагроз // *Інформаційні технології та суспільство*. — 2024. — Іс. 1 (12). — P. 13–19.

3. Олена К. Збій у роботі мережі київстар — оновлення та рекомендації для абонентів [Online]. — 2023. — URL: <https://biz.nv.ua/ukr/tech/zbiy-u-roboti-merezhi-kijivstar-onovlennya-ta-rekomendaciji-dlya-abonentiv-50375659.html> (accessed: 06.11.2024).
4. Олена К. У київстарі розповіли про наслідки кібератаки на 3,6 млрд грн [Online]. — 2024. — URL: <https://biz.nv.ua/ukr/markets/u-kijivstari-rozpovili-pro-naslidki-kiberataki-na-3-6-mlrd-grn-50419968.html> (accessed: 06.11.2024).
5. Boyko V., Vasilenko M., Slatvinska V. Survivability and sustainability of smart city information system components // Municipal economy of cities. — O.M.Beketov National University of Urban Economy in Kharkiv, 2021. — Vol. 6, no. 166. — P. 20–27.
6. Бойко В. Д. Моделювання кібернетичної складової живучості складних технічних систем / Матеріали міжнародної науково-практичної конференції "інформаційні управляючі системи та технології" (ІУСТ-одеса-2014), 23 – 25 вересня 2014 року. — Одеса, 2014. — P. 239–241.
7. Rausand M., Høyland A. System reliability theory: Models, statistical methods, and applications, second edition / 2nd ed. — Wiley-Interscience, 2003. — P. 636.
8. Cimellaro G. P., Reinhorn A. M., Bruneau M. Framework for analytical quantification of disaster resilience // Engineering Structures. — Elsevier BV, 2010. — Vol. 32, no. 11. — P. 3639–3649.

Ключові слова: моделювання відновлення, живучість, інформаційно-комунікаційні системи, кібератаки, кібербезпека, кіберзагроза, кіберзагрози, когнітивно-імітаційна модель, стійкість.

Keywords: cognitive simulation model, cyberattacks, cybersecurity, cyberthreats, information and communication systems, modeling, recovery resilience, survivability.

ВДОСКОНАЛЕННЯ ПРОЦЕСУ ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Кіх Михайло

*аспірант і асистент кафедри безпеки інформаційних технологій
Національного університету «Львівська Політехніка»*

Нємкова Олена

*професор кафедри безпеки інформаційних технологій Національного
університету «Львівська Політехніка», доктор технічних наук, професор*

Генерація псевдовипадкових послідовностей є важливою складовою багатьох комп'ютерних систем та програм, що використовують випадковість для різних цілей, від криптографії до індустрії комп'ютерних ігор [1–5]. Однак існують деякі проблеми та виклики, пов'язані з процесом генерації псевдовипадкових чисел, які потребують уваги та вирішення. Одна з ключових проблем — недостатня якість та безпека псевдовипадкових чисел, яка може призвести до вразливостей систем та недостатньої стійкості криптографічних протоколів [1, 3]. Інші проблеми включають недостатню швидкість гене-

рації, обмеженість доступних ресурсів, а також недостатню випадковість у деяких сценаріях використання.

Для вирішення цих проблем потрібно розглянути різні шляхи покращення до процесу генерації псевдовипадкових послідовностей, включаючи впровадження більш надійних алгоритмів, вибір оптимальних початкових значень, перевірку на відповідність стандартам, моніторинг та аудит системи генерації, а також оптимізацію швидкості та продуктивності.

Використання кращих алгоритмів. Використання криптографічно стійких генераторів псевдовипадкових чисел (КСГПВЧ) значно покращує безпеку та випадковість послідовностей. Алгоритми, такі як Fortuna, Yarrow, Blum Blum Shub (BBS), та ISAAC, створюють складно передбачувані послідовності, що робить їх ідеальними для застосувань із підвищеними вимогами до безпеки, як-от генерація ключів шифрування та цифрові підписи. КСГПВЧ проходять ретельні тестування на стійкість та відповідають міжнародним стандартам. Алгоритм Fortuna, наприклад, забезпечує багаторівневу надійність і стійкість до компрометації, що робить його популярним у криптографічних системах [1].

Вибір оптимальних початкових значень. Оптимальний вибір початкових значень (seed) критично важливий для якості та безпеки псевдовипадкових послідовностей. Правильні значення підвищують випадковість, захищають від атак і забезпечують стабільну роботу системи [2]. Основні етапи:

1. Початкові значення повинні мати високу ентропію, щоб унеможливити передбачення. Варто використовувати надійні джерела: системні події, час виконання.

2. Потрібно поєднувати ентропію з незалежних джерел (час запуску системи або активність користувача).

3. Варто забезпечити унікальність та непередбачуваність значень для уникнення повторень.

4. Потрібно регулярно оновлювати початкові значення.

5. Варто підбирати розмір значення відповідно до вимог генератора, наприклад, 256 біт [2].

Перевірка на відповідність стандартам. Перевірка відповідності стандартам є ключовим етапом для підвищення якості генерації псевдовипадкових послідовностей. Основні кроки:

1. Потрібно обирати стандарти, які відповідають вимогам безпеки, наприклад, NIST SP 800-90A/B/C, FIPS 140-2/140-3, ISO/IEC 18031, ANSI X9.82 .

2. Варто переконатися, що обрані алгоритми відповідають криптографічним стандартам [3].

3. Потрібно тестувати генератор відповідно до стандартів, застосовуючи набори тестів: NIST Statistical Test Suite, Diehard, або TestU01 [3].

4. Варто використовувати бібліотеки з сертифікацією безпеки (FIPS 140-2).

5. Потрібно регулярно оновлювати алгоритми й процедури для відповідності останнім стандартам безпеки.

Моніторинг та аудит системи генерації. Постійний моніторинг та аудит процесу генерації псевдовипадкових чисел допомагають виявляти проблеми та вразливості, що можуть знизити випадковість і безпеку. Основні етапи:

1. Потрібно визначити метрики безпеки, такі як кількість згенерованих чисел, ентропія, результати тестів на стійкість, виявлення аномалій.

2. Варто налаштувати систему для відстеження ключових параметрів, подій та збереження журналів [4].

3. Потрібно проводити регулярний аудит для перевірки відповідності стандартам.

4. Варто створити механізми виявлення аномалій та реагування на них [4].

5. Потрібно навчити персонал користуванню інструментами моніторингу та аудиту.

6. Варто удосконалювати процеси моніторингу та аудиту на основі зворотного зв'язку.

Оптимізація швидкості та ефективності. Оптимізація алгоритмів може покращити швидкість і ефективність генерації псевдовипадкових чисел. Основні кроки:

1. Потрібно використовувати швидкі алгоритми з низькою обчислювальною складністю [5].

2. Варто застосовувати апаратне прискорення, наприклад, SIMD у процесорах.

3. Потрібно використовувати багатопотоковість та паралелізацію (GPU) для прискорення.

4. Варто зменшувати накладні витрати, наприклад, оптимізуючи пам'ять і алгоритми [5].

5. Потрібно використовувати кешування та попереднє обчислення, щоб уникнути повторних розрахунків.

6. Варто оптимізувати код, використовуючи ефективні алгоритми та вбудовані функції.

7. Потрібно регулярно тестувати і вдосконалювати генератор для підтримки високої швидкості.

Результати досліджень. Результати досліджень покращення процесу генерування псевдовипадкових послідовностей за допомогою вибору оптимальних початкових значень, перевірки на відповідність стандартам, моніто-

рингу та аудиту системи генерації, оптимізації швидкості та ефективності відображені у таблиці 1. Визначено стратегії застосування і переваги кожного методу для покращення процесу генерування. Важливо також враховувати пріоритети різних методів для їх комбінації та послідовності використання.

Таблиця 1. Методи покращення: стратегії, переваги і пріоритети

Метод покращення	Стратегія	Переваги	Пріоритет
Вибір оптимальних початкових значень	1. Забезпечення високої ентропії. 2. Збір ентропії з різних джерел. 3. Захист від прогнозування початкових значень. 4. Регулярне оновлення початкових значень. 5. Вибір відповідного розміру початкових значень.	1. Захист від атак. 2. Якість випадкових послідовностей. 3. Унікальність послідовностей (Уникнення повторів). 4. Стійкість до криптоаналізу. 5. Запобігання прогнозуванню. 6. Ефективне використання ресурсів. 7. Асинхронність в системах з багатьма генераторами.	Високий
Перевірка на відповідність стандартам	1. Вибір відповідних стандартів. 2. Використання криптографічно стійких алгоритмів. 3. Тестування на відповідність стандартам. 4. Використання сертифікованих бібліотек та інструментів. 5. Оновлення та перевірка стандартів.	1. Забезпечення безпеки. 2. Гарантія випадковості. 3. Забезпечення сумісності. 4. Довіра користувачів. 5. Забезпечення якості. 6. Захист від юридичних та регуляторних ризиків.	Високий
Моніторинг та аудит системи генерації	1. Визначення метрик безпеки. 2. Налаштування системи моніторингу. 3. Реалізація аудиту безпеки. 4. Виявлення та реагування на аномалії. 5. Навчання персоналу. 6. Постійне вдосконалення.	1. Виявлення аномалій. 2. Попередження про вразливості. 3. Забезпечення відповідності. 4. Покращення якості генерації. 5. Підвищення довіри. 6. Реагування на інциденти.	Середній
Оптимізація швидкості та ефективності	1. Використання оптимізованих алгоритмів. 2. Використання апаратного прискорення. 3. Багатопотоковість та паралелізація. 4. Зменшення накладних витрат. 5. Кешування та попереднє обчислення. 6. Оптимізація коду. 7. Тестування та оптимізація швидкості.	1. Підвищення продуктивності. 2. Зменшення затримок. 3. Підвищення масштабованості. 4. Економія ресурсів.	Низький

Було проаналізовано основні характеристики (таблиця 2) алгоритму Fortuna, який використовується при розробці генераторів.

Таблиця 2. Основні характеристики алгоритмів

Алгоритм	Основні характеристики
Fortuna	1. Криптостійкий. 2. Багаторівнева архітектура. 3. Використовуються генератори підвищення рівня випадковості. 4. Надійний та безпечний.

Висновки. Було запропоновано набір методів для покращення процесу генерування псевдовипадкових послідовностей, які включають в себе використання кращих алгоритмів, вибір оптимальних початкових значень, перевірку на відповідність стандартам, моніторинг та аудит системи генерації, оптимізацію швидкості та ефективності. Ці підходи дозволяють забезпечити високу якість та надійність псевдовипадкових послідовностей у різних сценаріях використання. Дослідження підкреслює важливість комплексного підходу до генерації псевдовипадкових чисел, що забезпечує криптографічну стійкість, ефективність і відповідність стандартам.

Список використаних джерел:

1. R. McEvoy, J. Curran, P. Cotter and C. Murphy, "Fortuna: Cryptographically Secure Pseudo-Random Number Generation In Software And Hardware," 2006 IET Irish Signals and Systems Conference, Dublin, Ireland, 2006, pp. 457-462. https://www.researchgate.net/publication/215858122_Fortuna_Cryptographically_Secure_Pseudo-Random_Number_Generation_In_Software_And_Hardware
2. Osara, J. A., & Bryant, M. D. (2024). Methods to Calculate Entropy Generation. Entropy, 26(3), 237. <https://doi.org/10.3390/e26030237>
3. Kim, Y., & Yeom, Y. (2021). Accelerated implementation for testing IID assumption of NIST SP 800-90B using GPU. PeerJ Computer Science, 7, e404. <https://doi.org/10.7717/peerj-cs.404>
4. Bansal, A., Kandikuppa, A., Hasan, M., Chen, C.-Y., Bates, A., & Mohan, S. (2023). System Auditing for Real-Time Systems. ACM Transactions on Privacy and Security, 26(4), 1–37. <https://doi.org/10.1145/3625229>
5. Pushkar, O., Hrabovskyi, Y., & Gordyeyev, A. (2020). Development of a method for optimizing the site loading speed. Eastern-European Journal of Enterprise Technologies, 6(2 (108)), 21–29. <https://doi.org/10.15587/1729-4061.2020.216993>

Ключові слова: кібербезпека, генератори псевдовипадкових послідовностей, криптографічна стійкість, стандартизація, моніторинг та аудит, оптимізація.

Keywords: cyber security, generators of pseudorandom sequences, cryptographic stability, standardization, monitoring and auditing, optimization.

QUANTUM PERIOD FINDING AS A THREAT FOR POST-QUANTUM CRYPTOGRAPHIC PRIMITIVES

Yevgen Kotukh

*Воєнна Академія ім. Євгена Березняка, доцент,
кандидат технічних наук.*

The advent of quantum computing presents unprecedented challenges to cryptographic security, particularly through the application of quantum period finding algorithms. While post-quantum cryptography (PQC) aims to resist quantum attacks, the subtle periodicities within certain implementations may create exploitable vulnerabilities through sophisticated QPF techniques. The quantum period finding threat model operates within the quantum mechanical framework, where the fundamental state evolution is described by

$$|\psi\rangle = 1/\sqrt{N} \sum_x |x\rangle |f(x)\rangle \rightarrow 1/\sqrt{N} \sum_k e^{i(2\pi kx/N)} |k\rangle |f(x)\rangle,$$

where $f(x)$ represents the cryptographic function under analysis, and N denotes the size of the input space. This transformation's ability to identify periodic structures within cryptographic implementations presents significant security implications.

Our analysis employs a systematic approach to vulnerability assessment across three primary categories of post-quantum cryptographic primitives: lattice-based systems, multivariate cryptography, and hash-based signatures. The methodology encompasses quantum algorithmic complexity analysis, implementation vulnerability assessment, and theoretical attack vector evaluation. Within lattice-based cryptography, the analysis reveals potential exploitable periodicities in Ring-LWE implementations with structured error distributions, NTRU variants utilizing cyclical polynomial rings, and specific LWE parameter sets exhibiting periodic patterns. Multivariate cryptographic systems demonstrate vulnerabilities through regular structures in oil-and-vinegar schemes, periodic patterns in Hidden Field Equation variants, and systematic weaknesses in Rainbow signature implementations. Hash-based signatures present critical concerns regarding regular tree structures in SPHINCS+ variants, deterministic index selection in XMSS implementations, and predictable state progression in stateful schemes.

The quantum attack protocol follows a sophisticated progression beginning with quantum state preparation, where quantum registers are initialized, and a superposition of the cryptographic function domain is implemented. This is followed

by period detection through the application of quantum Fourier transform and analysis of interference patterns. Classical post-processing extracts measurement results through continued fraction expansion and determines period candidates. The final phase involves cryptanalytic exploitation through period relevance analysis and parameter extraction.

Mitigation strategies encompass multiple levels of defense, including design-level countermeasures through the implementation of irregular mathematical structures and randomization techniques. Implementation safeguards focus on side-channel leakage prevention and noise injection mechanisms, while theoretical foundations require the development of QPF-resistant proof frameworks and worst-case quantum attack analysis. These strategies must balance security requirements with practical implementation considerations, including computational overhead, key size optimization, and parameter selection criteria.

The implications for cryptographic engineering are substantial, necessitating irregular mathematical structures, provable QPF resistance, and sophisticated countermeasures. Performance considerations must account for computational overhead, key size optimization, and parameter selection criteria. Implementation challenges include experimental validation protocols, efficient countermeasure development, and testing methodology standardization. The standardization process requires establishing quantum-resistant design criteria, developing testing protocols, and defining certification requirements.

Current research directions focus on enhanced quantum period finding variants, resource requirement analysis, and novel cryptanalytic applications. Implementation research emphasizes experimental validation protocols, efficient countermeasure development, and testing methodology standardization. Standardization efforts concentrate on establishing quantum-resistant design criteria, developing testing protocols, and creating certification requirements.

The quantum period finding algorithm represents one of the most significant developments in quantum computing, particularly for its revolutionary implications in cryptography and number theory. This fundamental quantum routine, which forms the cornerstone of Shor's algorithm, demonstrates the extraordinary potential of quantum computation for solving previously intractable mathematical problems.

The theoretical foundation of quantum period finding rests upon the quantum Fourier transform (QFT) and its ability to efficiently identify periodic structures in mathematical functions. Given a function $f(x)$ with period r , such that $f(x + r) = f(x)$ for all x , the quantum period finding algorithm can determine r exponentially faster than any known classical algorithm. This capability has profound implications, particularly in the context of cryptographic systems that rely on the computational difficulty of finding such periods.

The mathematical framework begins with the preparation of a quantum state in superposition. Given function $f(x)$, the algorithm initializes two registers: the first in a superposition of all possible inputs, and the second storing the function values. This can be expressed as:

$$|\psi_1\rangle = 1/\sqrt{N} \sum_x |x\rangle |f(x)\rangle$$

where N represents the size of the input space. The power of the algorithm lies in its ability to leverage quantum parallelism to evaluate the function for multiple inputs simultaneously.

The implementation process consists of several critical steps. First, the quantum Fourier transform is applied to the input register, creating interference patterns that encode information about the period. The resulting state can be represented as:

$$|\psi_2\rangle = 1/\sqrt{N} \sum_k e^{(2\pi i k x/N)} |k\rangle |f(x)\rangle$$

The measurement of this state yields values that, through continued fraction expansion, reveal the period r with high probability.

In cryptographic applications, particularly in the context of RSA cryptography, the period finding algorithm's ability to efficiently determine the order of elements in modular arithmetic becomes crucial. For a number a coprime to N , finding the period of the function $f(x) = a^x \bmod N$ enables the factorization of N , thereby compromising the security of RSA encryption.

The technical implementation faces several significant challenges. Quantum decoherence and error rates in current quantum hardware limit the practical application of period finding to small numbers. The requirement for quantum error correction and fault-tolerant quantum computation remains a critical area of ongoing research. Current implementations typically require $O(\log N)$ qubits and $O((\log N)^2)$ quantum gates, where N is the number being factored.

Recent advancements in quantum hardware and error correction have led to improved implementations. Superconducting quantum circuits and ion trap quantum computers have demonstrated successful period finding operations for small-scale problems. These experimental results validate the theoretical framework while highlighting the engineering challenges that must be overcome for practical applications.

The implications for cryptography extend beyond RSA factorization. The ability to efficiently find periods impacts various cryptographic protocols that rely on the computational difficulty of related mathematical problems. This has spurred the development of post-quantum cryptography, which seeks to create encryption methods resistant to quantum period finding attacks.

From a complexity theory perspective, quantum period finding demonstrates a clear quantum advantage over classical computation. The algorithm achieves exponential speedup for certain problems, providing one of the most compelling

examples of quantum computational supremacy. This has significant implications for our understanding of computational complexity classes and the relationship between classical and quantum computation.

Current research directions focus on several key areas. These include optimizing the algorithm for noise-resistant implementation, reducing the required quantum resources, and developing hybrid classical-quantum approaches that can operate within the constraints of near-term quantum devices. Additionally, research continues into the application of period finding techniques to other mathematical problems beyond factorization.

The practical significance of quantum period finding extends to various fields beyond cryptography. Applications in signal processing, pattern recognition, and data analysis benefit from efficient period detection. The algorithm's ability to identify hidden periodicities in complex systems has potential applications in physics, chemistry, and other scientific disciplines.

Looking toward future developments, several challenges and opportunities emerge. The scaling of quantum systems to handle larger problems remains a primary challenge. The development of error-corrected quantum computers capable of implementing period finding for cryptographically relevant numbers represents a critical milestone in quantum computing.

The societal implications of efficient period finding capabilities are profound, particularly in the context of information security. The potential to break widely-used cryptographic systems necessitates a transition to quantum-resistant encryption methods. This transition presents both technical and economic challenges for organizations and governments worldwide.

From a mathematical perspective, quantum period finding has stimulated new research in number theory and algebraic structures. The algorithm's efficiency in solving certain mathematical problems has led to new insights into the nature of periodicity and its relationship to computational complexity.

Experimental implementations continue to advance, with recent demonstrations showing improved coherence times and reduced error rates. These developments, while still far from practical cryptographic applications, provide valuable insights into the challenges and requirements for scaling quantum period finding to practically relevant problem sizes.

This analysis demonstrates that quantum period finding represents not merely a theoretical construct but a fundamental advancement in computational capabilities. Its continued development and implementation will significantly impact various fields, from cryptography to fundamental physics, while raising important questions about the future of secure communication in a quantum-enabled world.

References:

1. Kotukh Y., Khalimov G., Hard problems for non-abelian cryptography, 2021: Fifth International Scientific and Technical Conference Computer And Information Systems And Technologies, 2021, pp. 39-40, <https://doi.org/10.30837/csitic52021232176>
2. Kotukh, Y., Khalimov, G., Korobchynskyi, M., Rudenko, M., Liubchak, V., Matsyuk, S., & Chashchyn, M. (2024). Research horizons in group cryptography in the context of post-quantum cryptosystems development. *Radiotekhnika*, 1(216), 62–72. <https://doi.org/10.30837/rt.2024.1.216.05>
3. Kotukh E., Severinov O., Vlasov A., Tenytska A., & Zarudna E. (2021). Some results of development of cryptographic transformations schemes using non-abelian groups. *Radiotekhnika*, 1(204), 66–72. <https://doi.org/10.30837/rt.2021.1.204.07>

АУТЕНТИФІКАЦІЯ ЗА ДОПОМОГОЮ JSON WEB TOKEN

Кухаренко Сергій

*доцент кафедри кібербезпеки Національного університету
«Одеська юридична академія», кандидат технічних наук, доцент*

Овчинников Микола

*асистент кафедри кібербезпеки Національного університету
«Одеська юридична академія»*

JSON Web Token (JWT) – це відкритий стандарт (RFC 7519), який визначає спосіб створення токенів доступу на основі формату JSON. JWT використовується для передачі даних між учасниками системи, найчастіше з метою аутентифікації користувачів після входу в систему та дозволяє визначити, чи має користувач доступ до певних ресурсів або функцій, тобто авторизації у клієнт-серверних додатках [1]. Токени генеруються сервером, підписуються з допомогою секретного ключа чи ключа асиметричного шифрування і передаються клієнту. Надалі клієнт застосовує цей токен для підтвердження своєї справжності, надаючи доступ до ресурсів або функціоналу

JWT був уперше запропонований як спосіб стандартизації передачі даних у розподілених системах, де виникає необхідність безпечної та ефективної аутентифікації [2]. Основна ідея полягала у спрощенні процесу передачі інформації між клієнтом та сервером з мінімальними накладними витратами. Згодом JWT завоював популярність завдяки своїй простоті та широким можливостям інтеграції з різними мовами програмування та технологіями.

На ранніх етапах розвитку Інтернету для зберігання сесій використовувалися серверні підходи: дані про сесії зберігалися на сервері, а клієнту передавався ідентифікатор. Однак зі збільшенням навантаження на сервери та розвитком SPA (Single Page Applications) виникла потреба у більш легковажних, масштабованих рішеннях. JWT став одним із таких рішень, пропонуючи

перенесення частини відповідальності на клієнта та спрощуючи інтеграцію між різними компонентами системи.

Розглянемо структуру веб-токена Json. Веб-токени Json ніколи не шифруються, а кодуються за допомогою бази 64 (UTF-8). JWT складається з трьох частин: заголовка, корисного навантаження та підпису. Кожна частина відокремлена крапкою (.) і закодована окремо. це означає лише заголовок, якщо спробувати декодувати базу 64, буде отримано дійсний результат. немає необхідності розглядати весь маркер для декодування. Частина за частиною дійсна. Давайте детально розберемо кожен компонент веб-токена json.\cite{b1} [3].

Першим компонентом веб-токена json є заголовок. Він складається з інформації, а саме алгоритму, типу маркера тощо. Тип алгоритму варіюється від симетричного HS256 до асиметричного RS256 залежно від використання. цей пакет закодовано у форматі base 64 і розміщено як перший компонент маркера jwt.

```
JSON Header Format:  
{  
  "alg" : "RS256",  
  "type": "JWT"  
}
```

Рис 1. Заголовок

Другим компонентом веб-токена json є корисне навантаження. Він складається з інформації, зокрема ідентифікатора клієнта, ідентифікатора компанії, права доступу до маркера та дати закінчення терміну дії маркера. Цей комплект також закодовано у форматі base 64 і розміщено як другий компонент маркера jwt. Формат корисного навантаження Json:

```
{  
  "sub": "0987654321",  
  "name": "Joe",  
  "iat": 9875456678  
}
```

Рис 2. Корисне навантаження

Підпис JSON: третім компонентом веб-токена Json є підпис. І заголовок, і корисне навантаження пов'язані разом із секретним ключем до підпису. Цей підпис підтримує цілісність маркера. Формат підпису JSON:

Куки мають обмеження за обсягом даних зазвичай до 4 КБ. Це може стати проблемою, якщо ваш JWT містить велике корисне навантаження (наприклад, вкладені об'єкти або великий обсяг метаданих) або якщо необхідно зберігати кілька токенів. Перевищення цього ліміту призведе до збоїв у роботі програми.

Якщо куки містять великі дані, це може сповільнити передачу запитів, оскільки з кожним запитом весь обсяг куків надсилається на сервер. У високонавантажених системах це може призвести до збільшення часу відгуку та витрати трафіку.

Оновлення токенів, що зберігаються в куках, може бути складним процесом, особливо якщо необхідно дотримуватися суворих безпекових політик. Наприклад, при зміні ключів підпису токенів може знадобитися перевидання всіх куків, що вимагає продуманої реалізації на стороні сервера та клієнта.

Отже, зберігання JWT в куках – це зручне та безпечне рішення за умови правильного налаштування [4]. Токени компактні й добре підходять для передачі в URL або заголовках HTTP. Токен підписується (симетрично або асиметрично), що унеможливорює його підробку, а також серверу не потрібно зберігати стан сесії, що зменшує навантаження на базу даних.

Щоб мінімізувати ризики, рекомендується обмежувати час життя токена, щоб знизити ризик його компрометації, встановлювати прапори HttpOnly, Secure та SameSite, використовувати додаткові механізми захисту від CSRF-атак, оптимізувати розмір токенів, виключаючи їх надмірні дані.

Цей підхід особливо ефективний для додатків, де важливі зручність використання та захист від XSS-атак. Однак для проектів з особливими вимогами щодо безпеки або продуктивності варто розглянути альтернативні методи зберігання JWT.

Список використаних джерел:

1. Adam S. I., Moedjahedy J. H., Maramis J. RESTful web service implementation on Unklab information system using JSON web token (JWT) //2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS). – IEEE, 2020. – С. 1-6.
2. Bucko A. et al. Enhancing jwt authentication and authorization in web applications based on user behavior history //Computers. – 2023. – Т. 12. – №. 4. – С. 78.
3. Mahindraka P. Insights of JSON Web Token //International International Journal of Recent Technology and Engineering (IJRTE) ISSN. – 2020. – С. 2277-3878.
4. RFC 7519. JSON Web Token (JWT). Специфікація. <https://datatracker.ietf.org/doc/html/rfc7519>

Ключові слова: маркер, автентифікація, авторизація, JWT, безпека, захист даних, конфіденційність, сесії, шифрування, комп'ютерні науки

Keywords: token, authentication, authorization, JWT, security, data protection, privacy, sessions, encryption, computer science

ВИКОРИСТАННЯ РЕСУРСОМІСТКИХ ПАСТОК ДЛЯ УСКЛАДНЕННЯ АТАКИ НА ВЕБСЕРВЕР

Бойко Віктор

*доцент кафедри кібербезпеки Національного університету
«Одеська юридична академія», кандидат технічних наук*

Спесівцев Микола

*студент 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

В умовах постійного зростання кількості та складності кіберзагроз, захист веб-серверів від зловмисних атак перетворюється на один з найважливіших пріоритетів для будь-якої організації. Традиційні методи захисту, такі як фаєрволи, системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS), хоч і залишаються фундаментальними компонентами системи безпеки, часто виявляються недостатньо ефективними проти нових, ще невідомих векторів атак, а також проти цілеспрямованих атак, що використовують унікальні експлойти. Тому виникає гостра потреба в розробці та впровадженні більш проактивних, адаптивних та гнучких стратегій захисту. Одним з таких перспективних підходів є використання ресурсомістких пасток, зокрема технології, відомої як tarpit.

Tarpit – це захисний механізм, що функціонує на принципі уповільнення взаємодії зі зловмисними клієнтами. На відміну від фаєрволів, які повністю блокують з'єднання, Tarpit навмисно затримує обробку запитів, створюючи віртуальне "болото" (звідси й назва), в якому "грузне" атакуюча сторона [1]. Цей підхід дозволяє реалізувати низку важливих захисних функцій. По-перше, штучне уповільнення дає адміністраторам системи цінний час для реагування на атаку, детального аналізу її характеристик, ідентифікації вектора атаки та вжиття необхідних заходів для її нейтралізації. По-друге, Tarpit суттєво знижує ефективність автоматизованих атак, таких як сканування портів за допомогою інструментів типу Nmap, брутфорс-атаки на аутентифікацію за допомогою Hydra та інших подібних утиліт, а також розподілені атаки на відмову в обслуговуванні (DDoS), які покладаються на швидкість та масовість запитів [2]. Зловмисникам доводиться витратити значно більше часу і ресурсів на досягнення своєї мети, що робить атаку менш ефективною або навіть неможливою.

У контексті дослідження tarpit`ів важливо позиціонувати їх у рамках ширшої категорії інструментів кібербезпеки, відомих як honeypots. Honeypots являють собою спеціально розгорнуті ресурси, спроектовані для приваблення, виявлення та аналізу шкідливої активності в кіберпросторі [2]. Імітуючи

реальні системи, додатки та сервіси, honeypots створюють контрольоване середовище, де дослідники можуть спостерігати та аналізувати поведінку зломисників без ризику компрометації продуктивних систем. Це дозволяє збирати цінні дані про тактики, техніки та процедури (TTP), використовувані атакуючими, ідентифікувати нові вектори атак, а також отримати глибше розуміння мотивації та цілей зломисників.

Honeypots класифікуються за рівнем інтерактивності, що визначає ступінь свободи, наданий зломиснику в імітованому середовищі. Низькоінтерактивні honeypots емулюють обмежений набір сервісів та портів, мінімізуючи ризик компрометації та спрощуючи аналіз зібраних даних. Високоінтерактивні honeypots, навпаки, надають зломисникам доступ до повністю функціональних систем, що дозволяє детально вивчити їхню поведінку, але одночасно підвищує ризик використання honeypot для подальших атак.

Tarpit, з їхнім фокусом на уповільненні та аналізі зломисників, можуть розглядатися як спеціалізований підтип honeypots. Вони мінімізують інтерактивність зі зломисником, створюючи пастку, що затримує його дії та ускладнює подальше просування. Ця стратегія дозволяє не тільки виграти час для реагування на інцидент, але й детально проаналізувати поведінку зломисника в контрольованому середовищі. Таким чином, tarpit`и доповнюють функціональність інших видів honeypots, забезпечуючи додатковий рівень захисту та аналізу загроз. Розуміння місця tarpit`ів в екосистемі honeypots дає можливість ефективніше використовувати їх в комплексних стратегіях кібербезпеки [3].

Tarpit реалізує свою функціональність через введення затримок на різних рівнях мережевого стеку. Це може бути зроблено на рівні операційної системи, використовуючи інструменти управління мережевим трафіком, такі як iptables в Linux або netsh advfirewall в Windows. Наприклад, за допомогою iptables можна налаштувати правила, що затримують пакети, які відповідають певним критеріям, таким як IP-адреса джерела, порт призначення або тип протоколу. На рівні веб-сервера, такого як Nginx або Apache, можна використовувати спеціальні модулі або скрипти, які вводять затримки у відповідь на HTTP-запити. Наприклад, в Nginx можна використати модуль ngx_http_limit_req_module для обмеження швидкості запитів від одного IP. Крім того, існують спеціалізовані програмні рішення, призначені виключно для створення tarpit, які пропонують розширені можливості конфігурації, моніторингу та аналізу затриманих з'єднань [2]. Важливо також враховувати можливість використання tarpit в поєднанні з іншими технологіями захисту, такими як honeypots, для ще більш ефективного виявлення та аналізу зломисної активності. Правильне налаштування tarpit, включаючи вибір оптимальної величини затримки та критеріїв для її застосування, є критично

важливим для забезпечення балансу між ефективністю захисту та мінімізацією негативного впливу на легітимних користувачів.

Аналіз історичних випадків поширення комп'ютерних вірусів демонструє потенційну ефективність застосування тарптів як превентивного заходу. Хоча ретроспективний аналіз не може повністю відтворити динаміку минулих подій, він дозволяє оцінити можливий вплив тарптів на обмеження масштабів інцидентів минулого.

Епідемії черв'яка Code Red у 2001 році демонструє потенційну ефективність превентивного розгортання tarpit'ів для мінімізації негативних наслідків. Code Red, експлуатуючи buffer overflow вразливість в індексній службі (Indexing Service ISAPI extension) Microsoft Internet Information Services (IIS) версій 4.0 та 5.0, характеризувався експоненціальним поширенням за рахунок активного сканування мережі по TCP порту 80. Черв'як використовував спеціально сформований HTTP запит довжиною 197 байт, що дозволяв перезаписати ділянку пам'яті та отримати контроль над системою [4].

Стратегічне розгортання мережі tarpit'ів, налаштованих на прослуховування TCP порту 80, могло б суттєво вплинути на динаміку поширення Code Red. Імітуючи вразливі сервери IIS, tarpit'и відповідали б на скануючі запити черв'яка, створюючи ілюзію наявності вразливості. Отримавши відповідь, Code Red спробував би експлуатувати "підроблену" вразливість, відправляючи свій шкідливий HTTP запит. Tarpit, замість виконання коду черв'яка, штучно затримував би з'єднання, імітуючи процес експлуатації та аналізуючи отриманий запит. Це сповільнювало б розповсюдження Code Red, виснажуючи його ресурси та надаючи адміністраторам час для встановлення патчу, що виправляв вразливість.

Крім стримування поширення, tarpit'и дозволили б зібрати детальну технічну інформацію про активність Code Red. Логи tarpit'ів містили б IP-адреси заражених машин, повний вміст шкідливих HTTP запитів, часові мітки та інші метадані. Аналіз цієї інформації дав б можливість дослідникам визначити характерні сигнатури Code Red, розробити точніші правила для брендмауерів та систем виявлення вторгнень (IDS), а також глибше зрозуміти механізми його роботи. Таким чином, "липкі пастки" виступили б не тільки як засіб пасивного захисту, а й як інструмент активного збору розвідувальних даних для ефективної протидії загрозі.

Список використаних джерел:

1. Lark Editorial Team. Cybersecurity Glossary Tarpitting. *Lark*. URL: <https://shorturl.at/xlCBY>.
2. ONSEC.io Research Team. TCP Tarpit and Port Scanning. Barricades on Both Sides. *ONSEC*. URL: <https://shorturl.at/qHFNd>.

3. Walla S., Rossow C. M ALPITY : Automatic Identification and Exploitation of Tarpit Vulnerabilities in Malware. *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW 2019)*. 2019. P. 590–650. URL: <https://shorturl.at/UZta7>.
4. CAIDA research team. CAIDA Analysis of Code-Red. *CAIDA*. URL: <https://shorturl.at/Tr2o9>.

Ключові слова: веб-сервер, IDS, IPS, tarpit, honeypot, превентивний захист, ресурсомісткі пастки, штучне уповільнення.

Keywords: web server, IDS, IPS, tarpit, honeypot, preventative control, resource-intensive pastes, artificial slowing down.

АВТОМАТИЗАЦІЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ З ВИКОРИСТАННЯМ ФРЕЙМВОРКА METASPLOIT

Бойко Віктор

*доцент кафедри кібербезпеки Національного університету
«Одеська юридична академія», кандидат технічних наук*

Пілявський Владислав

*студент 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

Взаємозв'язок між тестуванням на вразливості та забезпеченням безпеки локальної мережі є одним із ключових факторів для підтримки захисту ІТ-інфраструктури. Metasploit[1] є важливим інструментом для виявлення уразливостей у локальній мережі, та може значно полегшити роботу системного адміністратора, якщо автоматизувати процес сканування операційних систем. Регулярне тестування на вразливості дозволяє своєчасно виявляти нові загрози, які можуть виникати унаслідок змін у мережевій архітектурі чи нових вразливостей у програмному забезпеченні. Використання Metasploit не лише спрощує цей процес, але й забезпечує точне сканування, яке заперечує виникнення помилки в результаті людського фактора.

Проблема полягає в недостатній перевірці вразливостей системним адміністратором окремих IP-адресів, а також в локальній мережі. В умовах сучасних загроз, пов'язаних з кібератаками, системні адміністратори стикаються з необхідністю регулярної перевірки вразливостей у мережах та оперативного усунення можливих проблем. З розвитком технологій та збільшенням складності мережесистем підхід до забезпечення їхньої безпеки також змінюється.

Вирішенням цієї проблеми є інструмент Metasploit Framework, ця утиліта є потужним інструментом для тестування інформаційних систем на проникнення та уразливості. Metasploit був створений HD Moore[2] в 2003 році як портативний мережесистемний інструмент який був написаний мовою програму-

вання Perl, однак у 2007 році проект був остаточно переписаний на Ruby. Msfconsole [3], ймовірно, є найпопулярнішим інтерфейсом для Metasploit Framework (MSF). Він надає централізовану консоль «все в одному» і дозволяє ефективно отримувати доступ практично до всіх опцій, доступних в MSF. Metasploit складається з 4 основних модулів [4], таких як сканери, які призначені для пошуків відомих уразливостей, даючи тестувальнику на проникнення швидко представлення про те, які атаки варто провести.

Експлойти - їх функція полягає в тому щоб виконувати послідовність команд, націлених на певну вразливість, виявлену в системі або програмі, щоб надати зловмиснику доступ до системи.

Payload - це скрипти, які хакери або тестувальники на проникнення використовують для взаємодії зі зламаною системою.

Постексплуатаційні модулі це модулі які призначені для отримання доступу до системи після успішної експлуатації вразливості.

Ручна перевірка вразливостей у локальній мережі потребує значних часових витрат, тому набагато ефективніше буде написати код мовою програмування Python, у якому можна буде вказати, як потрібні IP-адреси для вибіркової перевірки, так і використовувати сканування локальної мережі. При запуску програма звертається до RPC[4] сервера (дозволяє програмно керувати Metasploit Framework за допомогою служб віддаленого виклику процедур (RPC) на основі HTTP.), далі nmap сканує зазначений IP-адрес, або локально мережу і у разі якщо він уразливий Metasploit використовує вказаний нами експлоїт, якщо система вразлива цьому експлоїту, програма виводить повідомлення про успішну експлуатацію, і переходить до наступного відкритого порту, якщо програмі не вдається зламати систему по цьому порту, то виводиться відповідне повідомлення.

Можна виділити 3 основні переваги автоматизації сканування вразливостей.

1. Зниження навантаження на системного адміністратора, так як сканування виробляє скрипт, системному адміністратору залишається тільки спостерігати за системними повідомленнями програми.

2. Регулярна перевірка на вразливості, через менше споживання часу, це займає всього кілька хвилин.

3. Менша ймовірність помилки, людський фактор може відіграти негативну роль при ручній перевірці вразливостей, тоді як автоматизовані скрипти мінімізують ризик упущення важливих деталей.

Таким чином, автоматизація сканування вразливостей за допомогою скриптів не тільки знижує навантаження на системних адміністраторів, а й забезпечує регулярне та точне виявлення вразливостей. Це дозволяє мінімізувати помилки, пов'язані з людським фактором, та оперативно усувати по-

тенційні загрози, що у результаті підвищує загальну захищеність мережі та розвантажує персонал.

Список використаних джерел:

1. Metasploit I Penetration Testing Software, Pen Testing Security I Metasploit. Metasploit. URL: <https://www.metasploit.com/> (date of access: 15.09.2024).
2. Contributors to Wikimedia projects. H. D. Moore - Wikipedia. Wikipedia, the free encyclopedia. URL: [https://en.wikipedia.org/wiki/H. D. Moore](https://en.wikipedia.org/wiki/H._D._Moore) (date of access: 15.09.2024).
3. Msfconsole - Metasploit Unleashed. OffSec. URL: <https://www.offsec.com/metasploit-unleashed/msfconsole/> (date of access: 15.09.2024).
4. Metasploit modules. URL: <https://docs.metasploit.com/docs/modules.html#metasploit-modules> (date of access: 15.09.2024).
5. RPC API I Metasploit Documentation. Docs @ Rapid7. URL: <https://docs.rapid7.com/metasploit/rpc-api/> (date of access: 15.09.2024).

Ключові слова: Metasploit, Metasploit Framework, сканування операційних систем, тестування інформаційних систем, тестування на проникнення, Msfconsole, Експлойт, вразливість.

Keywords: Metasploit, Metasploit Framework, operating system scanning, information systems testing, penetration testing, Msfconsole, Exploit, vulnerability.

АВТОМАТИЗОВАНИЙ АНАЛІЗ ТРАФІКА ДЛЯ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Бойко Віктор

*доцент кафедри кібербезпеки Національного університету
«Одеська юридична академія», кандидат технічних наук*

Журавський Георгій

*студент 2-го курсу магістратури факультету кібербезпеки та інформаційних
технологій Національного університету «Одеська юридична академія»*

Ботнети досі являють собою одну з найзначніших загроз кібербезпеці. Всі пристрої IoT можуть стати частиною ботнету, якщо було скомпрометовано їх безпеку.

Будь-який ботнет має канал для команд та керування (C&C). Типи такого каналу можуть різнитися і називаються архітектурою ботнету. Архітектурні моделі ботнетів загалом поділяються на централізовані та децентралізовані [1].

Централізований канал C&C за своїм принципом роботи схожий на будь-який додаток з клієнт-серверною архітектурою. При використанні такої моделі боти встановлюють зв'язок з точками з'єднання, які частіш за все є спеціальними серверами. Сам канал може використовувати протокол HTTP [2] або IRC, хоча останній легко блокується фаєрволом, і тому рідко застосо-

вується в сучасних ботнетах. Децентралізовані ботнети складніше блокувати, адже вони не мають C&C серверу, а втрата кількох, та навіть багатьох ботів не означає втрату цілого ботнету [3]. Такі децентралізовані ботнети зазвичай базуються на різноманітних протоколах Peer-to-Peer (P2P) та працюють як оверлей-мережі, які можна розділити на неструктуровані та структуровані.

Неструктурований ботнет не має можливості маршрутизації або пошуку ключа, однак підтримує флуд, метод випадкового блукання та має підтримку протоколу пліток. Для структурованого ботнету створюється таблиця відповідності між вмістом та його розташуванням. Зазвичай, для такого типу мереж створюється розподілена хешована таблиця для маршрутизації. Сучасні P2P ботнети базуються на структурованих оверлеях, таких як Kademlia [4].

Для того, аби заражений хост став активним ботом та частиною ботнету, хост має пройти через декілька етапів перетворення. Зазвичай ці етапи називають: початкове ураження, вторинна ін'єкція, підключення, шкідливі команди, оновлення та підтримка [5].

Під час етапу початкового ураження, зловмисник сканує цільову підмережу на вразливість, та заражає пристрій. Після цього настає етап вторинної ін'єкції, на якому заражені хости виконують скрипт, який дістає образ двійкового кода бота із вказаного місця через FTP-, HTTP- або P2P-з'єднання. Двійковий код встановлює себе на цільовий пристрій. Щойно програму-бот встановлено, пристрій жертви стає "зомбі" та виконує шкідливий код. Таким чином, програма запускатиметься автоматично кожного разу, як зомбі включатиметься [6]. На етапі підключення програма-бот встановлює канал C&C та з'єднує зомбі із сервером. Таким чином зомбі стає частиною армії ботнету, і виконує команди ботмайстра. Останнім етапом є підтримка діяльності ботів та їх оновлення. Ботмайстри намагаються зберігати невидимість та портативність своїх ботів, застосовуючи Динамічний DNS (DDNS) [7]. На випадок блокування сервера C&C за IP-адресою, ботмайстр може використати інший екземпляр сервера під тією ж назвою, але за іншою адресою. Зміни IP-адреси в C&C серверах майже миттєво поширюються на ботів через короткий час життя (time-to-live — TTL) для набору доменних імен, заданих постачальниками DNS. Відповідно, боти будуть мігрувати на нове розташування C&C сервера та залишатимуться живими [7, 8].

Для того, аби захистити мережу та вебсервер від втручання ШПЗ, переважна більшість адміністраторів використовує системи виявлення та запобігання вторгненням (IDS/IPS) та фаєрвол.

IDS, або система виявлення, розпізнає загрози вторгнення, атаки та підозрілі дії в мережі та генерує тривоги, може виявити загрозу, неавторизований або підозрілий мережевий трафік. Обмеження IDS полягає в тому, що

вона не може покласти край атаці на мережу; вона знаходиться в мережі виключно для спостереження за трафіком. Кожна система IDS має свій заздалегідь визначений набір правил, через який вона може розглядати конфігурацію кінцевих точок для того, аби визначити чи можуть вони бути вразливими для атак, і може записувати дії в мережі та порівнювати їх із відомими атаками або зразками атак.

IPS є процесом виявлення дій або загроз вторгнення та управління діями у відповідь на виявлені вторгнення та загрози в мережі. IPS в реальному часі спостерігають за трафіком пакетів з підозрілими діями або за тими, які збігаються з конкретними профілями та викликатимуть тривоги. IPS не лише виявляє зламани пакети, ботнети, віруси та спрямовані атаки, але й може вжити заходів для того, аби такі активності не завдали шкоди мережі. IPS має надавати захист ресурсам, даним та мережам.

Фаєрвол є важливим інструментом для посилення безпеки мережі. Він застосовується для запобігання неавторизованого доступу ззовні чи всередині мережі. Фаєрвол також відноситься до будь-яких методів або технологій, які з метою забезпечення безпеки контролюють вхідний та вихідний мережевий трафік [9]. Мережеві фаєрволи та IDS були розроблені для захисту мережі від зовнішніх атак, але вони не можуть виявити та захистити від вразливостей, які вже знаходяться всередині мережі.

Слід зазначити, що IDS/IPS та фаєрвол незалежно від своєї якості не гарантуватимуть повну безпеку мережі, тому, зазвичай, мережевий трафік додатково аналізується вручну, автоматично, чи з використанням алгоритмів машинного навчання (далі — АМН) для виявлення підозрілої активності.

При ручному аналізі група фахівців переглядає логи та спостерігає за мережевим трафіком за допомогою командного рядка або текстових редакторів. Такий тип аналізу можна використати для невеликих об'ємів даних або для точкового аналізу. На жаль, прості інструменти, наприклад, `grep`, `awk`, тощо, дозволяють проводити лише базову фільтрацію та маніпуляцію даними, але не можуть забезпечити складну аналітику або візуалізацію. Сам собою ручний аналіз великої кількості даних є занадто витратним з боку часу, тому, незважаючи на його ефективність в окремих випадках, його не можна рекомендувати для виявлення шкідливого ПЗ.

Через недоліки ручного аналізу були розроблені автоматичні системи моніторингу та аналізу. Майже кожна хмарна платформа має свій власний інструмент для моніторингу трафіку та доступу, наприклад, комбінацію інструментів CloudTrail + CloudWatch для платформи AWS.

Зокрема, варто виділити Snort. Snort є системою для аналізу трафіку в реальному часі, яку часто використовують для виявлення атак та шкідливого ПЗ у мережі, зокрема ботів. Вона працює як мережевий інструмент виявлен-

ня та запобігання вторгненням. Систему Snort можна налаштувати для автоматичного реагування на виявлені загрози, наприклад, блокування IP-адрес або скидання пакетів. Система працює на рівні TCP/IP, що дозволяє бачити весь потік даних. Snort може використовувати сигнатурну та поведінкову техніки виявлення ШПЗ. Для порівняння трафіку з відомими шаблонами шкідливих дій, Snort використовує базу сигнатур. Якщо шаблон зловмисної активності (наприклад, спроба ботнет-комунікації) знайдений, система повідомляє про це. У випадку поведінкового аналізу, відхилення від “нормальної” активності може сигналізувати про ботів, які зазвичай діятимуть за циклічним шаблоном або генеруватимуть незвичну кількість запитів. Snort може записувати власні логи, де фіксуватиме всі потенційно небезпечні події. Для автоматизації аналізу логів, використовують додаткові інструменти, наприклад, Splunk.

Основним припущенням, на яких базуються методи виявлення ботнетів за допомогою МН, є те, що ботнети викликають помітні шаблони трафіку або поведінки на пристрої клієнта і що такі шаблони можна виявити, застосувавши деякі з АМН [10]. У випадку виявлення ботнету за аномальною поведінкою, МН являє собою середнє між класифікацією та кластеризацією трафіку, використовуючи деякі алгоритми навчання зі вчителем та без вчителя. Трафік аналізується як в потоку, так і на рівні пакетів, де використовуються різні властивості трафіку. Видобуті властивості описують той трафік, який характеризує конкретного хоста або сервер в мережі, або конкретний потік.

Якщо ШПЗ потрапляє в мережу, та інфікує пристрої, для його виявлення можуть використовуватися статичні та динамічні методи аналізу, а також їх поєднання, яке називають гібридним аналізом.

Статичним аналізом або аналізом коду називають процес огляду коду ПЗ без його запуску. Методи статичного аналізу включають зняття цифрових відбитків, огляд формату файлів, видобуток рядків, сканування антивірусом та розбір коду. Зазвичай, при написанні ШПЗ, послідовність бітів, відома як сигнатура, вбудовується в код. За нею можна зрозуміти, до якого сімейства належить дане ПЗ. Така техніка використовується, наприклад, програмами-антивірусами. Антивіруси розбирають код файлу та шукають шаблони, які належать до шкідливого ПЗ. Сигнатури ШПЗ зберігаються в базі даних та використовуються для порівняння під час виявлення. Даний метод не може виявити невідоме ШПЗ, а також потребує великої кількості людських ресурсів та часу. Також недоліком є неможливість протидії ШПЗ, в коді якого застосовується поліморфізм.

Динамічним аналізом називають процес огляду функціоналу ПЗ при його роботі, відстежуючи виклики та параметри функцій та контроль потоку. Код запускають у віртуальному середовищі для стеження за його поведінкою

та розробленням заходів проти нього. Динамічний аналіз ефективніший за статичний, оскільки інфіковане ПЗ запускається у віртуальній машині для спостереження, що надає змогу легко виявити велику кількість ШПЗ. Головною перевагою виявлення за поведінкою є можливість виявити нові типи ШПЗ, які не може виявити сигнатурна модель. З іншого боку, головними недоліками моделі виявлення за поведінкою є високий час сканування та велика кількість помилкових спрацювань[11].

Гібридним аналізом називають поєднання технік як статичного, так і динамічного аналізу для отримання переваг обох підходів. Спершу оглядається код ПЗ, перевіряючи його на підозрілі сигнатури, а потім ПЗ запускається у віртуальному середовищі для спостереження за його поведінкою.

В даній роботі пропонується система АМН, яка націлена на аналіз трафіку по периметру системи та за певними критеріями виявлятиме спроби порушення цього периметру ШПЗ. Використання такої системи дозволить доповнити ручний та автоматизований аналіз трафіку та суттєво підвищити рівень безпеки та захищеності об'єкта.

Список використаних джерел:

1. "BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection". URL: <http://surl.li/finwvk>.
2. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, "RFC 2616-hypertext transfer protocol – HTTP/1.1", 1999. URL: <https://datatracker.ietf.org/doc/html/rfc2616>.
3. Sérgio S.C. Silva a, Rodrigo M.P. Silva, Raquel C.G. Pinto, Ronaldo M. Salles: "Botnets: A survey", 2012. URL: <https://doi.org/10.1016/j.comnet.2012.07.021>.
4. S.A. Crosby, D.S. Wallach, "An analysis of bittorrent?s two kademliabased dhds", 2007. URL: <http://surl.li/woeney>.
5. M. Feily, A. Shahrestani, S. Ramadass, "A survey of botnet and botnet detection, in: Emerging Security Information, Systems and Technologies", 2009. SECURWARE '09. Third International Conference on, pp. 268–273. URL: <https://doi.org/10.1109/SECURWARE.2009.48>.
6. K. K. R. Choo, "Zombies and Botnets," Trends and issues in crime and criminal justice, no. 333, Australian Institute of Criminology, Canberra, March 2007. URL: <https://www.aic.gov.au/publications/tandi/tandi333>.
7. P. Vixie, S. Thomson, Y. Rekhter, and J. Bound, "Dynamic updates in the domain name system(dns update)", 1997. URL: <http://www.faqs.org/rfcs/rfc2136.html/>.
8. H. Choi, H. Lee, H. Lee, and H. Kim, "Botnet Detection by Monitoring Group Activities in DNS Traffic". URL: <https://doi.org/10.1109/CIT.2007.90>.
9. Scambray, J., McClure, S. and Kurtz G. (2001) Hacking Exposed: Network Security and Solutions, Osborne/McGraw-Hill. URL: <http://surl.li/bydjgj>.
10. A. Ahmed, E . Elhadi, M. A. Maarof and A. H. Osman, "Malware Detection Based on Hybrid Signature Behaviour Application Programming Interface Call Graph Information Assurance and Security Research Group." Journal, A., Sciences, A., & Publications, S.,

Faculty of Computer Science and Information Systems, 9(3), 283–288, 2012. URL: <https://tinyurl.com/ms5mv4hv>.

11. M. Masud, L. Khan, B. Thuraisingham, Data Mining Tools for Malware Detection, Taylor & Francis Group, 2011. URL: <https://doi.org/10.1201/b11298>.

Ключові слова: ботнети, машинне навчання, аналіз трафіку, шкідливе програмне забезпечення.

Keywords: botnets, machine learning, traffic analysis, malware.

ДОСЛІДЖЕННЯ БЕЗПЕКИ ЛОКАЛЬНИХ МЕРЕЖ

Бойко Віктор

*доцент кафедри кібербезпеки Національного університету
«Одеська юридична академія», кандидат технічних наук*

Верба Костянтин

*студент 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

Проблема безпеки у локальних мережах, полягає у тому, що усі підприємства, організації та звичайні домівки мають пристрої для виходу у інтернет, та для більш правильної організації використання публічних IP-адрес, люди вигадали використовувати локальні мережі. За допомогою цього велика кількість пристроїв можуть користуватися мережею від одної публічної IP-адреси. Також, це підтримує спільний доступ до ресурсів, які обмінюються інформацією та даними. Проте, з розвитком технологій зростає і кількість загроз, пов'язаних із безпекою локальних мереж [1]. Безпека LAN є критично важливою, бо вразливості мережі можуть призвести до крадіжки інформації, компрометації даних, або порушенню роботи компаній чи організацій. Із часом, з'явилась велика купа питань з проблем безпеки для даних та пристроїв, які підключенні до однієї локальної мережі. Якщо, при використанні дротового зв'язку відстежувати з'єднання було доволі не складно, то при поширенні бездротових девайсів, безпека користувачів була під великою загрозою. Це спонукало фахівців для до створення протоколів та стандартів захисту для бездротових мереж, які виконують свою роботу й сьогодні. Але навіть протоколи автентифікації не можуть гарантувати користувачам повної безпеки, з тої причини, що зловмисники навчились перехоплювати частини пакетів рукошукання, та отримувати подальший доступ у середину мережі [2]. З цього випливає, що парольний захист бездротових мереж також не є основним захисником інформації, та потрібно налагоджувати усі можливі методи захисту [3].

Ці проблеми підкріплюється тим, що створення локальних мереж сьогодні є дуже простим, але велика кількість людей не зважає на безпеку своєї

інформації. Отже й мережі не мають потрібних налаштувань та не отримують додаткових заходів безпеки. Деякі мережі, що використовують у громадських будівлях навіть не мають парольної аутентифікації. Більшість не приділяє достатньо уваги до аспектів безпеки, тож зловмисники мають велику купу незахищених цілей.

Приклади найпоширеніших загроз, що можуть виникнути у сучасних LAN та WLAN:

- Атака «Людина посередині» - суть атаки полягає у тому, що зловмисник перехоплює та змінює трафік між двома вузлами мережі без їх відому.
- Атака на маршрутизатор – полягає у отриманні доступу до панелі налаштування маршрутизатору, що дає зловмиснику можливість керувати усією мережею.
- Атака за допомогою шкідливого ПЗ – полягає у тому, що зловмисники використовують локальне підключення для поширення шкідливого ПЗ серед підключених пристроїв.
- Сніфінг – полягає у перехопленні незашифрованих пакетів зловмисником, та використанням отриманої інформації у своїх цілях [4].
- Атака на WPA/WPA2 – зловмисник перехоплює пакет «рукописання», та використовує ПЗ для атаки на отримання паролю від мережі.
- Атаки через вразливості мережевого обладнання – зловмисник визначає модель та тип вашого обладнання, та використовує вразливості їх ПЗ для отримання доступу.

Уникнення подібних загроз є складним, бо потребує комплексних заходів щодо встановлення безпеки. Дослідження показало, що саме бездротова мережа та її налаштування є найважливішим аспектом захисту інформації.

1. *Налаштування мережі.* Перш за все при розгортанні будь-якої локальної мережі, потрібно чітко сформулювати її потреби, та використати необхідні налаштування, а саме:

- a. Використання парольної аутентифікації
- b. Налаштування фільтрації MAC-адрес
- c. Приховування SSID

Подібні заходи у купі сильно підвищують рівень загальної безпеки, та лімітує доступ до вашої мережі. У більшості випадках це може бути не дуже зручним рішенням, але все одно доволі надійним.

2. *Встановлення пристроїв для виявлення вторгнень.* Пристрої, такі як (IDS/IPS) можуть запобігти несанкціонованим діям у мережі або системі. Вони відносяться до систем виявлення та запобігання, та використовуються для встановлення безпеки мереж. Такі пристрої контролюють вхідних та вихід-

ний трафік в мережі, що може запобігти деяким поширеним атакам. Таким як ARP Spoofing, або використання експлойтів.

3. *Налаштування кінцевих пристроїв.* Використання налаштувань безпеки на кінцевих пристроях є також важливим аспектом. У більшості випадків потрібно використовувати вже готові налаштування безпеки, наприклад – режим «Загальнодоступної мережі», у якому пристрій під керуванням Windows підвищує захист вашої інформації. Наприклад: пристрій не буде виявлятися у цій мережі, весь загальний доступ до ваших файлів чи принтерів буде заблоковано, більшість вхідних з'єднань буде заблоковано, окрім важливих. Підвищення захисту від атак перехоплення трафіку та «людини по середині».

4. *Використання захищених каналів (VPN).* У разі використання невідомої вам мережі, використовувати шифрування та приховування вашого трафіку, завдяки використанню VPN. Це сильно знижує потенційні загрози, та дозволяє користуватися мережею без завад [5].

Отже, як результат, було встановлено загальні норми та правила, що попереджають або й зовсім уникають втручання у роботу локальних мереж. Використання комплексних заходів безпеки дають високий рівень безпеки вашої інформації, при використанні локальних мереж. Отже, усі названі аспекти є важливими, та потребують окремої уваги.

Список використаних джерел

1. Ridwan, R. (2024). Using the Penetration Testing Execution Standard Method (PTES) for Wireless Network Security Analysis. Greenation. [Електронний ресурс]. – Режим доступу: <https://greenpub.org/GCIR/article/view/679>.
2. A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. MDPI. [Електронний ресурс]. – Режим доступу: <https://www.mdpi.com/2076-3417/13/12/6986>
3. D. N. Răceanu and C. V. Marian, "Cybersecurity Virtual Labs for Pentesting Education," 2023 13th International Symposium on Advanced Topics in Electrical Engineering (ATEE), Bucharest, Romania, 2023, pp. 1-4, doi: 10.1109/ATEE58038.2023.10108187.
4. Adam H. M. et al. A Review of Penetration Testing Frameworks, Tools, and Application Areas //2023 IEEE 7th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE). – IEEE, 2023. – С. 319-324.
5. Fugkeaw S. et al. LightPEN: Optimizing the Vulnerability Exposures for Lightweight Penetration Test //2023 15th International Conference on Knowledge and Smart Technology (KST). – IEEE, 2023. – С. 1-5.

Ключові слова: безпека мереж, бездротові мережі, налаштування локальних мереж, кібербезпека, кіберзахист.

Keywords: network security, wireless networks, setting up local networks, cyber security, cyber protection.

ВИКОРИСТАННЯ ТЕГІВ ID3V2 ДЛЯ ЗАХИСТУ АВТОРСЬКИХ ПРАВ НА ЗВУКОВІ ФАЙЛИ MP3

Овчинников Микола

*асистент кафедри кібербезпеки Національного університету
«Одеська юридична академія»*

У наш час технологій та стрімкого потоку контенту, що оточує нас усюди, забезпечення захисту аудіовізуальної продукції від незаконного розповсюдження та використання стає дедалі складнішим завданням. Питання захисту мультимедійних даних давно обговорюються в наукових колах і основна увага приділяється методам стеганографії, які на сьогодні найбільше підходять для вирішення цього завдання. Цей підхід дозволяє впроваджувати об'єкти з конфіденційною інформацією у контейнери даних так, щоб сам факт їх наявності залишався непомітним. Для аудіо контенту контейнером виступає звуковий файл, а прихована інформація містить дані про правовласника.

Розглянемо найпростіший метод впровадження цифрових водяних знаків (ЦВЗ) у мультимедійні файли, який полягає у додаванні мітки (ЦВЗ) безпосередньо до коду файлу, а саме до його метаданих на прикладі найпопулярнішого звукового формату MP3. Як відомо, 23 квітня 2017 року, минув термін дії патентів на формат MP3 і він став фактично відкритим. Це означає відсутність технічних обмежень модифікації вмісту файлу.

Вміст MP3-файлів - це різні аудіодані, наприклад музика, звукові ефекти або записи голосу. Від версії до версії структура цих файлів неодноразово змінювалася, але в сучасних MP3-файлах виділяють два основні компоненти: ID3-тег та послідовність кадрів. За своєю структурою цей формат нагадує кіноплівку. ID3-тег містить довідкову інформацію, наприклад назву треку, альбому, ім'я виконавця та інші метадані, що особливо корисно для музичних композицій. ID3-тег версії 2, який став найпопулярнішим на сьогодні, може розташовуватися на початку файлу (у версії ID3v2.3) або наприкінці (у версії ID3v2.4) [1].

ID3 (від англ. Identify MP3) – популярний формат тегів для аудіофайлів, який широко використовується для збереження метаданих. Теги ID3 підтримуються багатьма програмами, такими як iTunes, Windows Media Player, Winamp, YME, MusicMatch, а також на апаратних програвачах, включаючи iPod, Creative Zen, Toshiba Gigabeat та Sony Walkman.

ID3-тег виступає контейнером метаданих, що зазвичай застосовується разом із аудіофайлами у форматі MP3. Він дає змогу зберігати та передавати інформацію про аудіофайл, наприклад, назву треку, виконавця, альбом, номер треку, рік випуску, обкладинку та інші дані про файл. [2].

Таблиця 1. Структура вмісту файлу MP3 [1]

Область тега ID3v2	Фрейм тега ID3v2	Область заголовка тега ID3v2	Заголовок фрейму містить поля: Ідентифікатор, Розмір, Прапори
		Вміст фрейму тега	Метадані
	...	...	...
	Фрейм тега ID3v2	Область заголовка тега ID3v2	Заголовок фрейму містить поля: Ідентифікатор, Розмір, Прапори
		Вміст фрейму тега	Метадані
Область аудіо даних	Область фреймів (один або більше фреймів)	Фрейм MP3	Заголовок фрейма
			Аудіо дані
		...	...
		Фрейм MP3	Заголовок фрейма
			Аудіо дані

У таблиці 1 показана структура файлу формату MP3, в якій передбачені області ID3-тега і аудіоданих [2]. ID3-тег включає заголовок і один або кілька кадрів з різним змістом [3]. Формат ID3v2 відрізняється змінною довжиною і може бути або на початку файлу (версія v2.3), або в його кінці (версія v2.4).

Тег складається з набору "фреймів", кожен із яких містить певні метадані. Наприклад, кадр TIT2 використовується для збереження назви композиції. Максимальний розмір одного кадру становить 16 МБ, а загальний розмір тега вбирається у 256 МБ. Текстова інформація у кадрах може бути закодована у форматах UTF-16 або UTF-8, причому біт кодування вказує тип текстового кадру.

Найпростіший спосіб захистити авторські права - розмістити в метаданих файлу інформацію про автора, проте цього недостатньо, оскільки такі дані легко змінюються або видаляються за допомогою спеціалізованого програмного забезпечення.

У таких умовах дані про правовласника можна приховати, застосовуючи стеганографічні методи. Наприклад, у зображенні, що розміщується в метаданих як обкладинка музичного альбому або фотографія автора, можна використовувати метод LSB (Least Significant Bit, Найменший Значущий Біт)

для впровадження прихованої інформації про автора [4]. непомітними для користувача.

Так як в тегах ID3v2 відсутні обмеження на розмір файлів, що завантажуються, розміщення повної інформації про автора виглядає цілком здійсненним. Однак метод LSB не застосовується до популярного формату JPG, оскільки він використовує стиск із втратами, у процесі якого менш значні біти, містять приховану інформацію, губляться. Однак, якщо звукові файли доступні лише в режимі прослуховування і користувач не має доступу для їх зміни, цей спосіб цілком може підійти.

Список використаної літератури

1. ОВЧИННИКОВ М. Ю., СЛАТВІНСЬКА В. М. ТЕХНІЧНИЙ ТА НОРМАТИВНО-ПРАВОВИЙ АСПЕКТИ ЗАХИСТУ ОБ'ЄКТІВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ НА РИНКУ АУДІО-ВІЗУАЛЬНОЇ ПРОДУКЦІЇ //Вісник Херсонського національного технічного університету. – 2024. – №. 3 (90). – С. 259-270.
2. Yatigammana K., Wijayarathna G. Integrating Micro-lesson Metadata in ID3V2 of MP3. 2021 From Innovation To Impact (FITI). IEEE, 2021. Vol. 1. P. 1-6.
3. Nilsson M., "ID3 tag version 2.4.0 - Main Structure," 01 November 2000. [Online]. Available: <https://id3.org/id3v2.4.0-structure>. [Accessed 07 December 2020].
4. Samborskyi I., Tolstova A. Сучасний стан та перспективи розвитку стеганографії у телекомунікаційних системах. Collection" Information Technology and Security". 2022. Т. 10. №. 1. С. 27-38.

Ключові слова: стеганографія, аудіофайли, захист даних, авторське право, метод заміни найменших значущих бітів, комп'ютерні науки

Keywords: steganography, audio files, data protection, copyright law, method of replacing least significant bits, computer science

Науковий керівник: *к.т.н., доцент Ахмаметьєва Г.В.*

КОМПЛЕКСНИЙ СИСТЕМНИЙ АНАЛІЗ МЕТОДІВ ЗАХИСТУ ВІД ФІШИНГОВИХ АТАК: ПОЄДНАННЯ ТЕХНІЧНИХ І ОРГАНІЗАЦІЙНИХ ПІДХОДІВ ДЛЯ КОРПОРАТИВНИХ МЕРЕЖ

Баланюк Микита

студент факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Вступ. Фішингові атаки, які з кожним роком стають дедалі складнішими, є однією з найбільш серйозних загроз для корпоративних мереж. Вони спрямовані на отримання конфіденційної інформації або примушення співробітників до дій, що можуть негативно вплинути на безпеку організації. Зловмисники активно використовують соціальну інженерію та маніпулюють людською довірою, що робить такі атаки особливо небезпечними. У сучасних

умовах боротьби з фішингом недостатньо обмежуватися лише технічними засобами. Потрібен комплексний підхід, що охоплює як технічні, так і організаційні заходи, а також створення культури безпеки всередині організації.

Системний аналіз методів захисту допомагає оцінити ефективність наявних заходів і знайти оптимальні комбінації, що підвищують рівень захисту. Важливо не лише впроваджувати нові технології, а й підвищувати обізнаність співробітників про загрози та формувати стійку культуру кібербезпеки. Це дозволяє кожному співробітнику усвідомлювати свою роль у забезпеченні захисту компанії. Крім того, систематичний аналіз загроз і регулярне оновлення політик кібербезпеки під нові виклики сприяють зниженню ризиків, пов'язаних з фішингом, та підвищенню загальної кіберстійкості.

Фішингові атаки: сучасні загрози

Згідно з дослідженнями з Data Breach Investigations Report [2] та APWG (Phishing Activity Trends Report) [3], кількість фішингових атак на корпоративні мережі неухильно зростає. Окрім традиційних фішингових листів, зловмисники застосовують таргетовані атаки, такі як spear phishing та whaling, які спрямовані на конкретних співробітників високого рівня. Такі атаки використовують персоналізовану інформацію, що підвищує ймовірність успішного обману. Згідно з даних від Агентства з кібербезпеки Європейського Союзу, у 2030 році ми можемо очікувати ще більше ускладнення фішингових атак, включаючи зловмисне використання штучного інтелекту для автоматизації та персоналізації фішингових повідомлень. Зловмисники можуть використовувати дані з соціальних мереж для створення переконливих фішингових листів, що робить такі атаки ще більш небезпечними. Важливо також враховувати, що зростає кількість атак, які використовують комбінацію різних векторів впливу, наприклад, фішинг разом з атаками на послуги хмарного зберігання даних, що ускладнює їх виявлення.

Згідно з Cisco Threat Trends [1], фішингові атаки також часто використовуються як перший етап у більш складних атаках, таких як APT (Advanced Persistent Threats). Зловмисники можуть використовувати фішингові атаки для отримання початкового доступу, який пізніше використовується для просування по мережі та розгортання додаткових атак, наприклад, викрадення даних або встановлення програм-вимагачів.

Технічні методи захисту

Технічні методи захисту відіграють важливу роль у запобіганні фішинговим атакам. До основних заходів належать фільтрація електронної пошти, аналіз URL-адрес, використання технологій машинного навчання для виявлення підозрілих повідомлень та забезпечення багатофакторної автентифікації (MFA). Впровадження протоколів SPF, DKIM і DMARC допомагає перевірити автентичність електронних листів, що суттєво знижує ризик успішного фі-

шингу. За даними Cisco Threat Trends [1], технології штучного інтелекту можуть аналізувати поведінкові патерни користувачів для виявлення аномальної активності, що може свідчити про спробу фішингової атаки. Також необхідно враховувати роль систем управління подіями та інцидентами інформаційної безпеки (SIEM), які можуть інтегрувати та аналізувати дані з різних джерел, виявляючи можливі фішингові загрози ще на ранньому етапі.

Важливим компонентом технічного захисту є використання антивірусних та антифішингових рішень, які можуть ідентифікувати шкідливі посилання та вкладення у повідомленнях. Розширені системи виявлення та запобігання вторгненням (IDS/IPS) також можуть бути використані для виявлення спроб несанкціонованого доступу до мережі після успішного фішингу. У майбутньому компанії мають приділяти більше уваги автоматизації процесів кібербезпеки, що дозволить зменшити час реагування на атаки та швидше усувати їх наслідки.

Організаційні заходи захисту

Організаційні заходи відіграють не менш важливу роль у захисті від фішингових атак. Навчання співробітників є ключовим елементом у створенні стійкої до фішингу корпоративної культури. Згідно з даними зі звітом SOC 2 Type II від Kolide [4], регулярні тренінги та симуляційні фішингові атаки значно знижують ймовірність успішного обману. Працівники повинні бути навчені розпізнавати ознаки фішингових повідомлень, зокрема підозрілі посилання, помилки у тексті та прохання надати конфіденційну інформацію. Окрім навчання, важливо встановити чіткі політики реагування на інциденти та повідомлення про підозрілі дії. Важливою також є реалізація програм з мотивації співробітників для участі у тренінгах з безпеки, наприклад, використання гейміфікації або нагород за активну участь.

Організаційні заходи також повинні включати розробку чітких інструкцій для співробітників щодо повідомлення про підозрілі листи або дії. Це може бути реалізовано через впровадження спеціальних каналів для повідомлення про інциденти, таких як внутрішні служби підтримки або автоматизовані інструменти для швидкого реагування. Регулярне тестування на готовність співробітників до виявлення фішингових атак (наприклад, через проведення контрольних фішингових кампаній) дозволяє оцінити ефективність навчання та вчасно виявляти прогалини у знаннях.

Системний аналіз захисних заходів

Проведення системного аналізу методів захисту включає оцінку ефективності як технічних, так і організаційних заходів через різні інструменти аналізу, такі як SWOT-аналіз та оцінка ризиків. Наприклад, у процесі аналізу було виявлено, що використання багатофакторної автентифікації (MFA) є ефективним технічним заходом, але лише за умови проведення відповідного навчан-

ня співробітників. Під час тестових тренінгів ми помітили, що без належного розуміння важливості MFA користувачі часто нехтують його використанням або допускають помилки під час автентифікації. Тому важливо не лише впроваджувати технічні засоби, а й забезпечувати належний рівень підготовки персоналу.

Аналіз також показує, що комбінація технічних і організаційних заходів, таких як навчання та впровадження технологій штучного інтелекту, є найбільш ефективним підходом для захисту від фішингових атак. Зокрема, ми провели тестування з впровадження технології виявлення аномальної активності користувачів, що дозволило виявити кілька спроб фішингових атак на ранніх стадіях.

Використання стандарту ISO/IEC 27001:2022 допомогло структурувати процес управління інформаційною безпекою, що дозволило інтегрувати різні рівні захисту в рамках єдиної системи. Наприклад, в одному з кейсів, компанії вдалося знизити кількість успішних атак на 30% після поєднання технічних рішень із комплексною програмою навчання співробітників.

Системний аналіз також враховує специфіку корпоративної мережі, зокрема використання віддалених робочих місць і хмарних сервісів. У процесі аналізу ми виявили, що віддалені робочі місця мають підвищений ризик фішингових атак через ненадійні з'єднання. Для вирішення цієї проблеми було рекомендовано використовувати захищені VPN-з'єднання та додаткові засоби автентифікації, такі як апаратні токени, що значно підвищує рівень безпеки підключення.

Рекомендації для корпоративних мереж

На основі проведеного системного аналізу можна зробити кілька рекомендацій для покращення захисту корпоративних мереж від фішингових атак. По-перше, необхідно впроваджувати багаторівневий підхід до безпеки, поєднуючи технічні рішення з організаційними заходами, такими як навчання та тестування співробітників. Наприклад, під час впровадження багатофакторної автентифікації (MFA) ми виявили, що ефективність цього заходу значно підвищується, якщо співробітники проходять тренінги, що пояснюють важливість та принципи роботи MFA. У деяких випадках після навчання кількість інцидентів, пов'язаних з невикористанням MFA, зменшилась на 40%. По-друге, слід впроваджувати засоби для аналізу поведінкових патернів користувачів, що дозволяє виявляти підозрілу активність на ранніх етапах. Наприклад, впровадження системи поведінкового аналізу дозволило нам виявити аномальну активність одного з користувачів, що вказувала на можливу компрометацію облікового запису, і запобігти подальшому розвитку атаки. По-третє, важливо постійно оновлювати політики та процедури кібербезпеки, враховуючи нові типи загроз та актуальні рекомендації з документів.

Також важливо інтегрувати процеси кібербезпеки в загальну стратегію компанії, забезпечуючи їх підтримку на найвищому керівному рівні. Наприклад, залучення керівників до програм навчання з кібербезпеки значно підвищило увагу до цього питання серед співробітників і дозволило більш ефективно впроваджувати нові заходи безпеки. Окрім цього, регулярне тестування засобів захисту, включаючи сценарії «червоних команд» (Red Team), допоможе виявити слабкі місця до того, як вони будуть використані зловмисниками. Під час одного з тестів ми змогли виявити вразливість у процесі автентифікації, яку пізніше було виправлено, що значно зменшило ризик можливого проникнення. Використання гейміфікації у тренінгах також може значно підвищити мотивацію співробітників до участі у навчанні, перетворюючи їх на активних учасників процесу захисту. Під час одного з тренінгів з використанням гейміфікації рівень залучення співробітників підвищився на 25%, що позитивно вплинуло на їхню обізнаність щодо фішингових атак.

Висновок

Фішингові атаки залишаються однією з найбільш значущих кіберзагроз для корпоративних мереж. На мою думку, їх вплив на корпоративні мережі виходить за рамки простої втрати даних — вони впливають на довіру між співробітниками, клієнтами та партнерами. Для ефективного захисту необхідний комплексний підхід, який включає як технічні, так і організаційні заходи. Мій досвід показує, що поєднання сучасних технічних рішень із системним навчанням співробітників є ключовим фактором у забезпеченні кіберстійкості. Навчання повинно бути регулярним та інтерактивним, з використанням реальних прикладів атак, щоб підвищити обізнаність і готовність співробітників.

Системний аналіз захисних методів дозволяє оцінити їх ефективність і знайти оптимальні шляхи інтеграції різних заходів для забезпечення максимального рівня захисту. Важливо не тільки впроваджувати технічні засоби, але й створювати культуру безпеки, де кожен співробітник розуміє свою роль у забезпеченні захисту даних компанії. На практиці це означає, що кожен співробітник повинен відчувати відповідальність за захист компанії та знати, як діяти у разі виявлення загрози.

Я також рекомендую активно впроваджувати методи тестування безпеки за допомогою «червоних команд» (Red Team), які дозволяють виявити слабкі місця до того, як їх зможуть використати зловмисники. Впровадження таких підходів не тільки знижує ризики, але й сприяє більш швидкому відновленню після інцидентів та створенню більш безпечного корпоративного середовища. Лише завдяки поєднанню всіх цих заходів можна забезпечити стійкість до сучасних загроз і зменшити потенційні наслідки фішингових атак.

Список використаних джерел:

1. Cisco Threat Trends Report. Звіт про тенденції кіберзагроз Cisco. Cisco, 2024. URL: <https://www.cisco.com/c/en/us/products/security/cyber-threat-trends-report.html>
2. 2024 Data Breach Investigations Report. Звіт про розслідування витоків даних 2024 року. Verizon, 2024. URL: <https://www.verizon.com/business/resources/reports/dbir/>
3. APWG, Phishing Activity Trends Report for the 2nd Quarter of 2024. Звіт про тенденції фішингової активності за 2-й квартал 2024 року. APWG, 2024. URL: <https://apwg.org/trendsreports/>
4. SOC 2 Type II від Kolide. Звіт про відповідність вимогам безпеки, конфіденційності, доступності, обробки даних та конфіденційності для сервісних організацій в компанії Kolide. URL: <https://www.kolide.com/legal/soc2>

Ключові слова: Фішингові атаки, Системний аналіз, технічні методи захисту, Інциденти інформаційної безпеки (SIEM), поведінковий аналіз, культура безпеки, Cisco Threat Trends.

Keywords: Phishing attacks, System analysis, technical methods of protection, Information security incidents (SIEM), behavioral analysis, security culture, Cisco Threat Trends.

Науковий керівник: к.т.н., доцент Ахмаметьєва Г.В.

ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА ОСНОВІ КЛІТИННИХ АВТОМАТІВ

Бойко Віктор

*доцент кафедри кібербезпеки Національного університету
«Одеська юридична академія», кандидат технічних наук*

Балабан Володимир

*студент 2-го курсу магістратури факультету кібербезпеки та інформаційних
технологій Національного університету «Одеська юридична академія»*

Проблема генераторів псевдовипадкових чисел (ГПВЧ), полягає в тому, щоб створити генератор, який би не лише мав необхідний рівень випадковості, але й відповідав іншим важливим критеріям: довгому періоду, високій ентропії, мінімальній передбачуваності, рівномірному розподілу чисел, швидкості роботи та розумним вимогам до обчислювальних ресурсів.

Серед багатьох підходів до створення ГПВЧ клітинні автомати виділяються своєю універсальністю та простотою. Клітинні автомати – це моделі, в яких стан кожної клітини (одиниці, подібної до точки на двовимірній сітці) оновлюється за певними правилами залежно від стану сусідніх клітин. Така простота правил поєднується з можливістю створювати складні та непередбачувані системи. Це робить клітинні автомати цікавим кандидатом для створення генераторів псевдовипадкових чисел, оскільки вони здатні генерувати складні послідовності за мінімальних витрат ресурсів [1].

Клітинні автомати мають кілька переваг перед традиційними методами генерації випадкових чисел. Вони можуть ефективно використовуватися на

паралельних архітектурах, що робить їх більш швидкими на багатопотокових системах. Їх обчислювальна складність та використання пам'яті залежать від розміру мережі та правил оновлення клітин, що дозволяє гнучко налаштовувати параметри залежно від доступних ресурсів. До того ж вони дозволяють легко змінювати параметри, такі як початкові стани або правила переходу, що робить їх адаптивними до різних завдань [2].

Основне завдання в контексті використання клітинних автоматів для генерації псевдовипадкових чисел – підібрати оптимальний діалект автомата, який би відповідав переліченим критеріям якості. Діалектами в цьому випадку можна вважати різні варіації клітинних автоматів: одномірні або двовимірні автомати, які відрізняються за розміром сусідства (скільки сусідів враховується при переході клітини в наступний стан) і за правилами переходів. Кожне таке правило по-різному впливає на випадковість отримуваної послідовності, її період та передбачуваність [3].

Оптимальний діалект генератора повинен забезпечувати високу ентропію, що означає, що будь-яка можлива послідовність значень у межах заданого діапазону має приблизно однакову ймовірність появи. Ентропія – це показник, який відображає ступінь невизначеності системи; чим вища ентропія, тим менш передбачуваною стає поведінка системи [4]. Це особливо важливо в контексті криптографічних застосувань, де передбачуваність генератора чисел робить його вразливим для атак.

Інша важлива вимога – довжина періоду. Це означає, що генератор не повинен повторюватися через короткі проміжки часу. В ідеалі, період повинен бути настільки довгим, що для практично корисних послідовностей (наприклад, тих, що використовуються у шифруванні) не існує можливості виявити повторення у розумні строки. Деякі клітинні автомати, такі як однорідні автомати за правилом 30, демонструють хороші властивості щодо тривалості періоду, але це може змінюватися залежно від початкових умов [5].

Швидкість роботи клітинних автоматів також відіграє важливу роль. Оскільки генерація чисел вимагає багаторазових ітерацій автоматів, важливо, щоб ці ітерації виконувалися швидко. Тут критично важливим стає використання паралельних обчислень, що дозволяє клітинним автоматам оновлювати стани багатьох клітин одночасно. Це дає явну перевагу на багатопроцесорних системах, оскільки дозволяє прискорити процес генерації випадкових чисел без значного збільшення витрат на обладнання [6].

Також варто враховувати вимоги до ресурсів. Клітинні автомати можуть бути досить економними в плані використання оперативної пам'яті та процесорного часу, особливо у випадках із простими одномірними автоматами. Водночас складніші правила та двовимірні структури можуть вимагати більше пам'яті для зберігання станів і виконання операцій [7]. Тому для кон-

кретних застосувань (наприклад, для вбудованих систем або мобільних пристроїв) важливо підібрати таку конфігурацію, яка забезпечить баланс між якістю випадковості та споживанням ресурсів.

Для того щоб вибрати оптимальний діалект клітинного автомата для генерації псевдовипадкових чисел, необхідно провести детальний аналіз різних варіацій автоматів з урахуванням початкових станів і правил переходу. У ході такого аналізу перевіряються властивості генераторів на різних початкових конфігураціях, оцінюється їхня поведінка за ключовими критеріями та вибирається той варіант, який найкраще підходить для поставленого завдання [8]. Це дозволяє створити генератор, який стабільно генеруватиме якісні випадкові послідовності при зміні початкових умов, що важливо для універсальності та надійності використання у реальних системах.

Отже, використання клітинних автоматів для генерації псевдовипадкових чисел відкриває широкий простір для досліджень та оптимізації, дозволяючи адаптувати підхід до конкретних вимог і обмежити ресурси, забезпечуючи при цьому високий рівень випадковості та безпеки.

Список використаних джерел

1. Cellular Automaton. [Електронний ресурс]. – Режим доступу: <https://mathworld.wolfram.com/CellularAutomaton.html>
2. Pseudorandom Number Generation using Cellular Automata - Rule 30. [Електронний ресурс]. – Режим доступу: <https://arpitbhayani.me/blogs/rule-30-cellular-automata/>
3. Hybrid Cellular Automata-Based Pseudo Random Sequence Generator for BIST Implementation. [Електронний ресурс]. – Режим доступу: <https://ijrsset.org/pdfs/v2-i9/8.pdf>
4. Cellular Automaton-Based Pseudorandom Number Generator. [Електронний ресурс]. – Режим доступу: <https://content.wolfram.com/sites/13/2018/04/26-4-4.pdf>
5. A Survey on Cellular Automata with the Application in Pseudo Random Number Generation. [Електронний ресурс]. – Режим доступу: <http://www.publishingindia.com/GetBrochure.aspx?query=UERGQnJvY2h1cmVzfC80NTczLnBkZnwwNDU3My5wZGY=>
6. Generating high-quality random numbers in parallel by cellular automata. [Електронний ресурс]. – Режим доступу: https://www.moshesipper.com/pubs/quality_random.pdf
7. On the Generation of High-Quality Random Numbers by Two-Dimensional Cellular Automata. [Електронний ресурс]. – Режим доступу: https://www.moshesipper.com/pubs/twod_rand.pdf
8. Exploration of cellular automata: a comprehensive review of dynamic modeling across biology, computer and materials science. [Електронний ресурс]. – Режим доступу: https://www.cmms.agh.edu.pl/public_repo/2023_4_0820.pdf

Ключові слова: сучасні рішення, генератори псевдовипадкових чисел, псевдовипадкові числа, клітинні автомати, кіберзахист, кібербезпека, криптографія.

Key words: modern solutions, pseudorandom number generators, pseudorandom numbers, cellular automata, cyber defense, cybersecurity, cryptography.

USING POLICY AS CODE FOR AUTOMATED SECURITY CONTROL IN KUBERNETES

Вахула Олександр

асистент кафедри Захисту Інформації, Інститут комп'ютерних технологій та автоматики, НУ "Львівська Політехніка"

Introduction.

The rapid adoption of cloud-native technologies has led to increased complexity in managing and securing Kubernetes clusters. Traditional security practices often struggle to keep pace with the dynamic nature of these environments, resulting in delayed implementation of security controls and costly late-stage vulnerability fixes. Policy as Code (PaC) emerges as a solution to these challenges by enabling the definition, enforcement, and management of security policies through code, ensuring consistency and scalability across the development lifecycle. This paper focuses on the application of PaC in Kubernetes environments, particularly using Open Policy Agent (OPA) and OPA Gatekeeper, to address common security and compliance challenges.

Methodology

PaC leverages tools like the Open Policy Agent (OPA) and its Kubernetes-integrated implementation, OPA Gatekeeper. OPA is an open-source, general-purpose policy engine that unifies policy enforcement across the stack [1]. Gatekeeper extends OPA's capabilities by integrating with Kubernetes admission controllers, allowing for real-time validation of resource configurations and providing a framework for auditing existing resources in the cluster [2]. Policies are written in Rego, a declarative policy language designed for expressing complex rules over hierarchical data structures [3]. Integration with GitOps practices further enhances automation, enabling policy enforcement directly from version-controlled repositories, thereby promoting consistency and traceability [4].

Additionally, Gatekeeper supports custom constraints through Constraint Templates, which allow users to define their own validation logic. This flexibility is critical in environments where regulatory compliance or organizational policies require specific security measures. Gatekeeper's audit functionality provides an additional layer of governance by evaluating existing resources against current policies, identifying non-compliant resources without immediate enforcement.

Scientific Contribution

1. An optimized model for implementing PaC in Kubernetes environments, emphasizing integration with Continuous Integration/Continuous Deployment (CI/CD) pipelines and GitOps workflows. This model facilitates automated policy enforcement throughout the development lifecycle, reducing manual intervention and minimizing the risk of misconfigurations.
2. Evaluation of policy audit functionality to detect non-compliant resources without

disrupting existing services. Gatekeeper's audit capabilities allow for a proactive approach to compliance and security management, providing insights into the state of the cluster [5].

3. A comparative study of OPA Gatekeeper and native Kubernetes Admission Controllers, focusing on performance, flexibility, and scalability. This study highlights the trade-offs between the simplicity of native controllers and the advanced capabilities offered by Gatekeeper [6].

Results

Our findings demonstrate that implementing PaC significantly enhances the security posture of Kubernetes clusters by preventing misconfigurations early in the development process. The auditing capabilities of Gatekeeper effectively identify non-compliant resources, enabling proactive remediation without service disruption. In one case study, auditing revealed 15% of resources were non-compliant due to outdated configurations, which were addressed within hours of discovery.

The comparative study between OPA Gatekeeper and native Kubernetes Admission Controllers revealed that while Gatekeeper adds a minor performance overhead, its flexibility and extensibility make it a superior choice for complex environments. Gatekeeper's ability to define custom policies and integrate with CI/CD pipelines provides a scalable solution that aligns with modern DevOps practices.

Conclusions

Policy as Code enhances security automation and minimizes risks in cloud-native environments. Its implementation in Kubernetes environments ensures consistent enforcement of security policies, reducing human error and operational overhead.

OPA Gatekeeper is a robust solution for Kubernetes security, particularly in complex and scalable clusters, offering advanced policy enforcement and auditing capabilities.

Future research should explore dynamic policy adjustments and broader integrations with other cloud-native security tools to further enhance the effectiveness of PaC in diverse environments

References

- [1] Open Policy Agent. "OPA Documentation." Available: <https://www.openpolicyagent.org/docs/latest/>
- [2] OPA Gatekeeper. "Gatekeeper Documentation." Available: <https://open-policy-agent.github.io/gatekeeper/website/docs/>
- [3] Rego Language. "Rego Documentation." Available: <https://www.openpolicyagent.org/docs/latest/policy-language/>
- [4] Weaveworks. "What is GitOps?" Available: <https://www.weave.works/technologies/gitops/>

- [5] Kubernetes. "OPA Gatekeeper: Policy and Governance for Kubernetes." Available: <https://kubernetes.io/blog/2019/08/06/opa-gatekeeper-policy-and-governance-for-kubernetes/>
- [6] ElasticSys. "Enforcing Policy as Code using OPA and Gatekeeper in Kubernetes." Available: <https://elasticSys.com/enforcing-policy-as-code-using-opa-and-gatekeeper-in-kubernetes/>
- [7] Permify. "OPA Gatekeeper: How To Write Policies For Kubernetes Clusters." Available: <https://permify.co/post/opa-gatekeeper-kubernetes/>

Keywords: Policy as Code, Kubernetes security, OPA Gatekeeper, automation, access control

Ключові слова: Політика як код, Безпека Kubernetes, OPA Gatekeeper, автоматизація, контроль доступу

АНАЛІЗ КІБЕРЗАГРОЗ У ХМАРНИХ ОБЧИСЛЕННЯХ: МЕТОДИ ЗАХИСТУ ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ

Грезіна Олена

*асистент кафедри інформаційних технологій Національного університету
«Одеська юридична академія», PhD*

Хмарні обчислення є однією з перспективних технологій у сфері інформаційних технологій. Вони дозволяють компаніям і індивідуальним користувачам ефективно зберігати, обробляти та аналізувати великі обсяги даних без потреби в утриманні власної інфраструктури. Однак із впровадженням цієї технології виникає низка викликів у галузі кібербезпеки, оскільки зростаюча залежність від зовнішніх платформ і обчислювальних мереж у поєднанні з підвищеними вимогами до конфіденційності та цілісності даних створює нові ризики. Отже, захист даних у хмарних обчисленнях є надзвичайно важливим для забезпечення безпеки та довіри користувачів до цієї технології.

Однією з основних проблем, яка виникає в хмарних середовищах, є кіберзагрози, які можуть призвести до несанкціонованого доступу до даних, їх втрати або пошкодження. Атаки, спрямовані на порушення конфіденційності, доступності та цілісності інформації, становлять серйозну небезпеку, що потребує ефективних методів захисту. Зважаючи на це, доцільно розглянути основні типи загроз у хмарних обчисленнях та методи їх нейтралізації.

З огляду на те, що кібератаки стають дедалі складнішими, а загрози кібербезпеці постійно зростають, необхідність у розробці комплексної стратегії безпеки для хмарних сервісів стає надзвичайно важливою. Для забезпечення ефективного захисту від кібератак в хмарних середовищах слід впроваджувати різноманітні заходи і методи захисту, які здатні гарантувати підвищений рівень безпеки для користувачів [1].

Серед основних кіберзагроз, з якими стикаються хмарні обчислення, можна виокремити кілька ключових напрямів. По-перше, хмарні сервіси є частинами цілями атак на доступність, зокрема для реалізації атак типу DDoS (Distributed Denial of Service), метою яких є створення перепон для доступу користувачів до необхідних сервісів і даних. Зазначені атаки можуть призвести до серйозних економічних і репутаційних втрат для організацій, що покладаються на хмарні технології.

По-друге, хмарні обчислення часто пов'язані з обробкою персональних та чутливих даних, що робить їх вразливими до витоків інформації. Порушення конфіденційності даних у хмарі може виникнути як результат уразливостей в апаратному або програмному забезпеченні, а також через помилки у налаштуваннях безпеки чи недостатній рівень захисту облікових записів користувачів. У цих умовах витік інформації може призвести до серйозних наслідків для кінцевих користувачів та організацій, що використовують ці платформи.

Також необхідно враховувати проблеми, пов'язані з уразливостями програмного забезпечення, яке використовують хмарні сервіси. Багато хмарних платформ інтегрують стороннє програмне забезпечення, яке може містити невиявлені помилки безпеки і сприяти потенційним можливостям для зловмисників, які використовуватимуть ці вразливості для здійснення атак і проникнення в систему.

Для того, щоб захистити дані в хмарних середовищах від зазначених загроз, необхідно застосовувати різноманітні методи безпеки. Один із основних підходів до захисту даних у хмарі — це їх шифрування. Шифрування забезпечує конфіденційність і цілісність даних, навіть у разі їх витoku чи несанкціонованого доступу. Використання як симетричних, так і асиметричних методів шифрування дозволяє захистити дані на всіх етапах їх обробки і зберігання.

Метод шифрування є ефективним у разі таких загроз, як перехоплення інформації під час передачі, а також частково при хакерських атаках і зломі інтерфейсів управління [2].

Іншим важливим інструментом захисту є багатоетапна аутентифікація (MFA), яка використовує кілька факторів для перевірки користувача. Це значно ускладнює зловмисникам отримання несанкціонованого доступу до ресурсів хмарної платформи, навіть у разі крадіжки пароля. MFA дозволяє гарантувати, що тільки авторизовані особи мають доступ до чутливої інформації.

Інструменти моніторингу і виявлення вторгнень (IDS) є ще одним критичним елементом в системі безпеки хмарних обчислень. Вони дозволяють виявляти підозрілу активність у реальному часі та оперативно реагувати на

можливі кіберінциденти. Зазначені системи можуть виявляти аномалії в поведінці користувачів і в мережевих потоках, що є першим кроком до запобігання чи мінімізації шкоди від кіберзагроз.

Забезпечення конфіденційності даних у хмарних середовищах є основною вимогою для багатьох користувачів і організацій. Крім шифрування даних, важливою складовою є ефективне управління доступом до цих даних. Користувачам повинні надаватися лише необхідні привілеї для виконання їхніх обов'язків, що дозволяє мінімізувати ризик витоку інформації через людський фактор.

Крім того, важливо забезпечити безпечне видалення даних після того, як вони більше не потрібні. Процес видалення має бути настільки ж безпечним, як і процес їхнього зберігання, щоб уникнути випадкового або умисного витоку інформації через старі резервні копії або архіви. Важливо, щоб ці процеси були автоматизовані і відповідали всім сучасним стандартам безпеки.

Захист даних у хмарних обчисленнях є важливим аспектом сучасних інформаційних технологій. Зважаючи на зростаючі загрози в кіберпросторі, необхідно вжити всіх заходів для забезпечення безпеки даних, що зберігаються та обробляються в хмарі. Впровадження комплексних заходів, включаючи шифрування, багатоетапну аутентифікацію, моніторинг активності, а також належне управління доступом і конфіденційністю, дозволяє знижувати ризики та забезпечувати ефективний захист від сучасних кіберзагроз.

Список використаних джерел

1. Король М.Я., Опірський І.Р. Дослідження та аналіз проблем та викликів, що виникають у забезпеченні кібербезпеки в хмарних обчисленнях. *Захист інформації*. Том 26. № 1 (2024). С. 64-71. URL: <https://jrn1.nau.edu.ua/index.php/ZI/article/view/18829>
2. Вараніцький, Д. В., Розколодько, О. О., Люта, М. В., Захарова, М. В., & Хотунов, В. І. Аналіз механізмів захисту даних в хмарних середовищах. *Технології та інжиніринг*. № 1 (18). 2024. С. 9–16. URL: <https://doi.org/10.30857/2786-5371.2024>

РОЛЬ СУБ'ЄКТИВНИХ ФАКТОРІВ АВТЕНТИФІКАЦІЇ ДЛЯ КІБЕРБЕЗПЕКИ

Голосова Ірина

*студент 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

Проблема ролі суб'єктивних факторів автентифікації для кібербезпеки полягає у визначенні природи, сприйняття і функції суб'єктивності в поєднан-

ні і стосовно факторів автентифікації в кібербезпеці. Організаційні заходи використовуються для підтримки технологічних, але технологічні заходи можуть бути скомпрометовані поведінкою користувачів, їхніми уявленнями про політику безпеки і ставленням до практик безпеки. Наприклад, навіть впровадження складних технічних рішень, таких як захист логів розподілених систем від кібератак за допомогою Verkle дерев [1], може бути неефективним, якщо користувачі не дотримуються протоколів безпеки. Тому існує необхідність дослідити, як суб'єктивні фактори впливають на безпеку, і розробити стратегії, які враховують людський фактор для підвищення рівня кібербезпеки.

Суб'єктивні фактори автентифікації також називають факторами автентифікації, які ґрунтуються на людському сприйнятті та судженнях щодо автентифікації. Ці фактори використовуються разом із загальними формами двофакторної автентифікації, такими як використання паролів і відбитків пальців. Паролі, PIN-коди, біометричні дані (відбитки пальців, обличчя, райдужна оболонка ока, голос), токени, SMS-підтвердження коду допомагають підвищити увагу користувачів до теми кібербезпеки, оскільки користувачі залучені до процесу ідентифікації. Суб'єктивні параметри використовуються для того, щоб гарантувати, що особа буде остаточно визнана у веб-системах, наприклад, інтернет-банкінгу, соціальних мережах, корпоративних мережах та електронній пошті; таким чином, це захищає обліковий запис від хакерських атак, фішингових шахрайств та інших кіберзлочинів.

Суб'єктивні фактори автентифікації, такі як поведінкові шаблони, знання користувача та особисті біометричні дані, відіграють важливу роль у підвищенні рівня безпеки систем, оскільки вони додають додатковий рівень захисту. Ці фактори дозволяють своєчасно ідентифікувати аномальну або підозрілу активність, що ускладнює шахрайську активацію або несанкціонований доступ до ресурсу. Наприклад, поведінкова автентифікація, заснована на вивченні рухів миші, ритму натискання клавіш або часу входу в систему, допомагає виявити інші несанкціоновані спроби отримати доступ. Коли до традиційних методів, таких як пароль і PIN-код, додаються додаткові суб'єктивні компоненти, підвищується надійність системи і можливість зниження ризиків.

Заходи суб'єктивної автентифікації посилюють захист персональних даних, продовжуючи звужувати доступ до них. Наприклад, інтеграція відбитків пальців, обличчя, голосу та інших інструментів ідентифікації посилює захист персональних даних від кіберзагроз. Це особливо помітно в місцях, де зберігаються дані, переважно банківська інформація або індивідуальні рахунки. Інші атрибути також відіграють певну роль у мінімізації фішингових атак, оскільки навіть якщо злоумисник зможе отримати пароль, він зіткнеться

ся з великими труднощами при проходженні поведінкових або біометричних перевірок.

Сучасні системи онлайн-банкінгу та соціальні мережі, наприклад, практикують введення елементів суб'єктивного фактору для посилення безпеки. Наразі маємо випадки, коли ідентифікація здійснюється на основі паролів, які дублюються загальним підтвердженням, отриманим за допомогою SMS або відбитків пальців. Це забезпечує гарантований ступінь захисту користувачів і захищає їх від таких несанкціонованих грошових операцій. Соціальні мережі також застосовують багато факторів автентифікації, таких як оцінка ризику залежно від місця перебування користувача або іншої підозрілої активності. Вони допомагають запобігти певній активності та негайно заблокувати її, щоб запобігти крадіжці або неправомірному використанню особистих даних користувача.

Автентифікація на основі знань актуальна для заборони несанкціонованого доступу до конфіденційної інформації шляхом запиту у користувачів певної інформації, яку вони не можуть знати, якщо вони не мають відповідного дозволу.

Третій тип автентифікації може бути корисним для виявлення та запобігання шахрайським діям, таким як фішинг та шкідливе програмне забезпечення, оскільки в його основі лежить аналіз поведінки.

Автентифікація на основі ризиків може забезпечити кращий захист конфіденційної інформації шляхом розпізнавання загроз безпеці та реагування на них у режимі реального часу.

Перевага автентифікації на основі довіри полягає у зменшенні кількості факторів автентифікації для суб'єктів, яким довіряють, при одночасному забезпеченні високого рівня безпеки.

Контекстна автентифікація дозволяє системі розпізнавати потенційні загрози безпеці в режимі реального часу, що дозволяє уникнути несанкціонованого доступу до інформації з обмеженим доступом.

Отже, суб'єктивні фактори автентифікації виступають важливими компонентами, необхідними для безпеки комп'ютерних систем та захисту даних від усіх спроб несанкціонованого доступу. Посилення ІТ-безпеки може бути досягнуто шляхом включення цих факторів разом з традиційними формами автентифікації.

Список використаних джерел:

1. Boyko V., Vasilenko M., Slatvinska V. Distributed systems log protection from cyberattacks by Verkle trees. Conference proceedings of the VII International Scientific-Practical Conference "Information Technology for Education, Science and Technics" (ITEST-2024), (Cherkasy, May 23-24, 2024). Cherkasy: ChSTU, 2024. 349 p.

C. 165-166. https://itest.chdtu.edu.ua/Conference%20Proceedings%20ITEST-2024_13_06.pdf (дата звернення: 06.11.2024).

Ключові слова: кібербезпека, автентифікація, персональні дані.

Keywords: cybersecurity, authentication, personal data.

Науковий керівник: доктор філософії, ас. каф. кібербезпеки Слатвінська В.М.

ІНСТРУМЕНТИ ПРОТИДІЇ КІБЕРЗАГРОЗАМ В ІНДУСТРІЇ КОМП'ЮТЕРНИХ ІГОР

Скідан Владислав

*асистент кафедри кібербезпеки Національного університету
«Одеська юридична академія»*

Індустрія комп'ютерних ігор сьогодні є однією з найприбутковіших та найдинамічніших галузей цифрової економіки, що приваблює мільярди користувачів з усього світу. Разом із стрімким розвитком технологій і розширенням функціональності ігрових продуктів зростають і ризики, пов'язані з кіберзагрозами. Кібератаки на ігрові сервіси загрожують не лише фінансовими збитками для компаній та витоками конфіденційної інформації користувачів, але й негативно впливають на репутацію брендів та загальну довіру до галузі. Отже, розробники ігор змушені шукати й запроваджувати різноманітні інструменти захисту – від технологій шифрування та багатофакторної автентифікації до інноваційних антипіратських систем на кшталт Denuvo, що дозволяє запобігати нелегальному використанню ігор [1].

Одним із ключових напрямків захисту користувацьких даних є застосування інструментів шифрування та багатофакторної автентифікації (MFA). Шифрування даних у процесі передачі між сервером і клієнтом допомагає захистити конфіденційну інформацію користувачів від перехоплення та використання її третіми сторонами. Багатофакторна автентифікація дозволяє підвищити рівень безпеки облікових записів, забезпечуючи додатковий рівень захисту від несанкціонованого доступу, оскільки користувачі мають підтвердити свою особу, використовуючи декілька елементів, таких як пароль та одноразовий код. Разом із заходами для захисту даних інструменти кібербезпеки забезпечують моніторинг активності користувачів, що допомагає виявити підозрілу активність та оперативно реагувати на потенційні загрози.

Зокрема, серед ефективних інструментів захисту інтелектуальної власності особливе місце займає антипіратська система Denuvo, розроблена компанією Irdeto. Denuvo є програмним рішенням, яке спрямоване на запобігання нелегальній копії та використанню відеоігор. Ця технологія забезпечує

захист ігрових продуктів на рівні коду шляхом упровадження різних механізмів шифрування, що ускладнює процес зламу гри. Denuvo застосовує унікальну систему захисту від дебагінгу та реверс-інжинірингу, що унеможливорює доступ до вихідного коду гри. Така система працює на рівні обфускації, де код гри ускладнюється, перешкоджаючи зловмисникам створювати піратські версії гри. Це дозволяє розробникам ефективніше протидіяти втратам від піратства та забезпечити стабільні фінансові надходження протягом перших місяців після релізу.

Denuvo, однак, є темою постійних дискусій серед розробників, гравців і хакерів, оскільки багато геймерів вважають, що наявність цієї системи захисту негативно впливає на продуктивність гри. Деякі користувачі заявляють про зниження частоти кадрів, проблеми з підвищеним навантаженням на процесор і обмеження доступу до модифікацій гри. З іншого боку, виробники ігор зазначають, що Denuvo відіграє важливу роль у захисті від нелегального копіювання в перші дні після релізу гри, коли максимальний попит забезпечує основну частину прибутків. Більшість розробників все ж схильні використовувати Denuvo хоча б на ранніх етапах випуску гри, після чого захист може бути знятий для уникнення претензій користувачів і покращення ігрового досвіду [2].

Додатково до захисту інтелектуальної власності системи кібербезпеки охоплюють такі аспекти, як управління вразливістю, захист від DDoS-атак і боротьба з шахрайством у багатокористувацьких іграх. Управління вразливістю передбачає ідентифікацію, аналіз і усунення слабких місць у коді ще на етапі розробки гри. Завдяки використанню спеціалізованих систем управління вразливістю компанії можуть швидко випускати патчі для усунення виявлених недоліків, зменшуючи ймовірність їх використання зловмисниками.

DDoS-атаки є ще однією серйозною загрозою для багатокористувацьких ігор, оскільки вони здатні паралізувати роботу серверів і зупинити доступ до гри для мільйонів користувачів. Для протидії таким атакам компанії використовують IDS/IPS-системи (системи виявлення та запобігання атак), а також хмарні сервіси, які автоматично адаптують ресурсні потужності серверів під час навантаження. Окрім цього, кібербезпека в багатокористувацьких іграх передбачає боротьбу з шахрайством та захист від сторонніх втручань у геймплей. Системи античитінгу, що використовують алгоритми машинного навчання, допомагають розпізнавати підозрілу поведінку гравців, що може вказувати на використання заборонених програм [3].

Крім технічних заходів, індустрія комп'ютерних ігор активно запроваджує кібергігієнічні практики як серед своїх співробітників, так і серед користувачів. Це охоплює навчання персоналу правилам безпечного поведіння з даними та проведення інформаційних кампаній для підвищення обізнаності

гравців про кіберзагрози. Такі кампанії допомагають користувачам усвідомити важливість багатофакторної аутентифікації та унікальних паролів, що знижує ризик несанкціонованого доступу до облікових записів.

Таким чином інструменти протидії кіберзагрозам в індустрії комп'ютерних ігор є різноманітними та комплексними, що охоплює широкий спектр методів і технологій. Від захисту інтелектуальної власності, зокрема через використання антипіратських систем, таких як Denuvo, до управління вразливістю, активної боротьби з DDoS-атаками, шахрайством та іншими формами зловживань у багатокористувацьких іграх – усі ці заходи спрямовані на створення надійного й безпечного ігрового середовища для користувачів, а також забезпечення стабільності та безперебійності роботи для розробників.

Список використаних джерел:

1. Кучірка М., Власенко Л. Роль кібербезпеки в розробці комп'ютерних ігор в умовах воєнних викликів. Інформаційні технології та кібербезпека в умовах воєнного часу [Електронний ресурс] : матеріали студ. наук.-практ. конф. Київ, 18 квіт. 2024 р. / відп. ред. К. В. Хорольська. Київ : Держ. торг.-екон. ун-т, 2024. С. 229-232.
2. Denuvo. Irdeto. URL: <https://irdeto.com/denuvo> (дата звернення: 20.10.2024)
3. Античит Valve (VAC). Служба підтримки Steam. URL: <https://help.steampowered.com/uk/faqs/view/571A-97DA-70E9-FF74> (дата звернення: 22.10.2024).

Ключові слова: кібербезпека, DDoS-захист, античит, шифрування, кібергігієна.

Keywords: cybersecurity, DDoS protection, anti-cheat, encryption, cyber hygiene.

ТЕОРЕТИЧНІ СПОСОБИ ПОКРАЩЕННЯ КРИПТОСТІЙКОСТІ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Олег Цебак

асистент кафедри

Національного університету «Львівська політехніка»

Генератори псевдовипадкових чисел (ГПВЧ) є основою багатьох криптографічних систем, від шифрування до протоколів аутентифікації. Проте сучасні криптоалгоритми стикаються з викликами, пов'язаними зі зростанням обчислювальної потужності, новими математичними атаками та розвитком квантових обчислень [2]. Огляд теоретичних способів покращення криптостійкості ГПВЧ, спрямованих на забезпечення безпеки в умовах сучасних та майбутніх загроз є важливим аспектом кібербезпеки.

До можливих способів покращення криптостійкості генераторів псевдовипадкових чисел слід віднести в першу чергу ускладнення математичних задач, що лежать в основі криптостійкості ГПВЧ, які мають забезпечувати

високу обчислювальну складність навіть за умови часткової компрометації внутрішнього стану:

- ускладнення базових задач - використання задач із більш складними параметрами, наприклад, Ring-LWE, що дозволяє створювати ефективніші генератори [5]. Розширення класу математичних задач до задач із використанням гіперкомплексних чисел чи ізогеній може значно підвищити стійкість;

- розширення простору ключів - генерація випадкових чисел із використанням великих чисел і нестандартних груп, наприклад, простих чисел із особливими властивостями (Sophie Germain primes). Це ускладнює будь-який аналіз вихідної послідовності;

- математичне змішування - включення кількох незалежних алгоритмів у структуру ГПВЧ із регулярним об'єднанням їх результатів для зниження ймовірності відновлення закономірностей.

Ці підходи забезпечують більш високий рівень захисту від атак як класичних, так і квантових, дозволяючи адаптувати алгоритми до майбутніх викликів.

Ще один із можливих способів це висористання адаптивних алгоритмів. Адаптивність дозволяє ГПВЧ реагувати на потенційні загрози та змінювати свої внутрішні механізми в реальному часі:

- ротація вхідних параметрів - періодичне оновлення внутрішнього стану генератора та його ключових параметрів на основі раніше згенерованих випадкових даних. Це ускладнює спроби відновлення початкових умов;

- динамічне змішування - включення додаткових джерел ентропії в процес генерації, наприклад, даних із фізичних датчиків, для унеможливлення прогнозування вихідних значень.

- аналіз атак у реальному часі - вбудовані механізми моніторингу, які виявляють можливі відхилення в послідовностях (наприклад, за результатами статистичних тестів) та ініціюють перехід до альтернативних режимів генерації.

Ці методи забезпечують гнучкість алгоритмів та їхню стійкість навіть у разі спроб атаки чи компрометації частини системи.

Розвиток квантових обчислень ставить під загрозу традиційні криптографічні алгоритми, тож постквантові підходи стають ключовими для підвищення стійкості ГПВЧ. Таким чином генератори, що базуються на складності обчислення ізогеній, забезпечують ефективне створення випадкових послідовностей із низькими обчислювальними витратами. Або ж використання багатовимірних задач, таких як Multivariate Quadratic Problems, що поєднують математичну складність з високою ентропією, підвищує стійкість до аналізу

послідовностей [5]. Ці підходи формують фундамент майбутніх стандартів криптографії, зберігаючи ефективність навіть у епоху квантових обчислень.

Хоч і не відносяться до псевдовипадкових, але все ж можна виділити такий підхід як використання фізичних джерел випадковості для покращення криптостійкості ГПВЧ, забезпечуючи високий рівень непередбачуваності. Використання теплових, електронних або фотонних шумів як джерел початкової ентропії значно ускладнює математичне моделювання та прогнозування послідовностей. Та як наслідок поєднання фізичних джерел випадковості з математичними алгоритмами підвищує захист від можливих атак на апаратний рівень, зберігаючи високу швидкість генерації.

Покращення криптостійкості генераторів псевдовипадкових чисел є важливою задачею для забезпечення надійності сучасних та майбутніх криптографічних систем [1]. Застосування новітніх теоретичних підходів дозволяє суттєво підвищити стійкість генераторів до атак, як класичних, так і квантових. Запропоновані стратегії, такі як використання складних математичних задач, адаптивних алгоритмів, постквантових методів та інтеграція фізичних джерел ентропії, мають значний потенціал у підвищенні рівня безпеки. Подальший розвиток у цій галузі потребує комплексного підходу, що поєднує теоретичні дослідження з інженерними рішеннями для створення ефективних і стійких криптографічних систем, здатних витримати виклики майбутнього.

Список використаних джерел

1. Дорофєєв С. І., Миколєнко І. В. Методи оцінки стійкості генераторів випадкових чисел // Вісник Київського політехнічного інституту. – 2018. – № 6. – С. 88–95.
2. Bernstein D. J., Buchmann J., Dahmen E. *Post-Quantum Cryptography*. – Berlin: Springer, 2009. – 170 p.
3. Goldreich O. *Foundations of Cryptography. Volume 1: Basic Tools*. – Cambridge: Cambridge University Press, 2001. – 372 p.
4. National Institute of Standards and Technology (NIST). Recommendation for Random Number Generation Using Deterministic Random Bit Generators. – NIST SP 800-90A, 2012.
5. Shor P. Algorithms for quantum computation: discrete logarithms and factoring // *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. – IEEE, 1994. – P. 124–134.

Ключові слова: криптографічна стійкість, генератори псевдовипадкових чисел, постквантова криптографія, задачі на решітках, ізогенії еліптичних кривих, адаптивні алгоритми, фізична ентропія, квантова випадковість, математична складність, гібридні генератори.

Keywords: cryptographic strength, pseudorandom number generators, post-quantum cryptography, lattice problems, elliptic curve isogenies, adaptive algorithms, physical entropy, quantum randomness, mathematical complexity, hybrid generators.

ВИКОРИСТАННЯ АЛГОРИТМІЧНИХ ТА ТЕХНІЧНИХ АСПЕКТІВ КІБЕРБЕЗПЕКИ В МЕРЕЖІ ІoT

Підлісний Юрій

*аспірант Національного університету
«Чернігівська політехніка»*

Вперше поняття "інтернет речей" (IoT, Internet-of-Things) було застосовано у 1999 році, коли компанія Procter&Gamble створила мережу пристроїв, що були здатні обмінюватися інформацією без втручання людини. Близько 10 років термін не набував широкого розповсюдження і лише наприкінці нульових років до нього прийшла популярність завдяки розвитку нових сенсорів та засобів зв'язку [1].

З середини 2010-х років (трохи більше ніж п'ять років від старту масового застосування) почалося вибухове експоненціальне зростання кількості IoT, яке не припиняється й нині (мова вже йде про 15 мільярдів пристроїв). З тих пір IoT-пристрої впроваджуються практично в усі аспекти життя людини: промисловість, охорону здоров'я, транспорт та звичайні "домашні господарства" (розумні кондиціонери, телевізори, електромобілі тощо).

Однак багато IoT-пристроїв виготовляються з відносно слабкими обчислювальними ресурсами та мають обмежену операційну систему. Багато виробників не приділяли достатньої уваги кібербезпеці своїх продуктів (це питання ніколи не було на "чільному місці" - рахувалося, що такі пристрої працюють у середовищі, де це "нібито не так важливо"). А це призвело до того, що IoT-пристрої часто мають вразливості у програмному забезпеченні, які можуть бути використані для атак.

Природно, що масштабність та розповсюдженість Інтернет речей створює великий потенціал для кіберзлочинців, впливати на широкий спектр систем. Як правило, IoT-пристрої інтегруються в загальну мережу (чи то домашня WI FI мережа, чи то велика корпоративна), і якщо один із пристроїв у результаті злому буде скомпрометовано, можна отримати доступ до всієї мережі з усіма пристроями. Тому злочинні елементи можуть використовувати IoT-пристрої для створення ботнетів, здійснення DDoS-атак, зламу даних або навіть фізичного шкоди[2].

Кібербезпека IoT вимагає розробки алгоритмічних і технічних рішень для виявлення загроз і протидії атакам. Нижче наведено ключові методи, що застосовуються для виявлення вразливостей та захисту IoT в контексті алгоритмічних або технічних аспектів [3].

Етапи виявлення вразливостей в мережі IoT:

Перший етап: Пошук вразливостей .

Початковий етап розпочинається з сканування сигнатур, використовуючи бази даних відомих атак, наприклад, CVE (*Common Vulnerabilities and Exposures*).

Алгоритмічними аспектами для сканування - буде порівняння трафіку або коду з шаблонами вразливостей, а також використання ефективних хеш-функцій для швидкого пошуку збігів.

Обмеженням для використання є необхідність регулярного оновлення бази даних, а головний мінус - неможливість виявлення невідомих атак (zero-day).

Другий етап: Виявлення аномалій.

Для автоматизації аналізу даних та поведінки IoT пристроїв слід використовувати методи машинного навчання. Алгоритмічні аспекти є навчання моделей на основі нормального трафіку (наприклад, класифікатори SVM -Support Vector Machine, нейронні мережі), виявлення відхилень за допомогою статистичних методів.

Обмеженнями для використання машинного навчання будуть значні обчислювальні ресурси, а статистичні методи можуть надати хибнопозитивні спрацювання.

Третій етап: Аналіз поведінки

Обов'язковий перегляд логів та моделей поведінки пристроїв. Алгоритмічні аспекти етапу є використання алгоритмів кластеризації (наприклад, K-means) для групування нормальної поведінки, а також побудова графових моделей зв'язків між пристроями.[4]

Етапи протидії кібератакам в мережі IoT:

Перший етап: Використання реактивних методів

Один з них це механізм блокування трафіку підозрілих IP-адрес. Технічними аспектами метода є налаштування брандмауерів і забезпечення автоматичного оновлення чорних списків.

Другий етап: Використання превентивних методів

Таких як - забезпечення безпечної автентифікації та шифрування даних. Алгоритмічні аспекти вказаного метода це використання асиметричних криптографічних алгоритмів (RSA, ECC) для захисту обміну ключами, а також застосування AES для шифрування трафіку.

Третій етап: Впровадження ізоляції компонентів IoT

Використовується для мінімізації впливу атаки. Технічними аспектами метода буде використання легковагових контейнерів (наприклад, Docker) і побудова архітектури мікросервісів.

Перелік алгоритмів виявлення та захисту:

1) *Побудова Байєсівських мереж довіри* (як приклад, визначення залежностей між змінними тип пристрою та ризик атак) і побудова ймовірнісної моделі для оцінки ризику.[5]

2) *Використання мультиагентних систем*, головними технічними аспектами яких є гнучкість децентралізованих структур і взаємодія агентів для обміну інформацією про загрози.

3) *Гібридні моделі* – поєднання сигнатур і аномалій для забезпечення більшої точності. Алгоритмічними аспектами слугуватиме ансамблі моделей з машинного навчання поєднанні з автоматичним оновленням баз сигнатур на основі аналізу поведінки.[5]

Важливим завершальним аспектом є візуалізація результатів, яка дозволяє аналітикам приймати швидкі рішення

Візуалізація даних:

1) *Діаграми потоків даних*: Відображення передачі даних між вузлами IoT.

2) *Графові моделі*: Аналіз зав'язків між пристроями для ідентифікації аномалій.

Висновок:

Для забезпечення кібербезпеки в IoT необхідно використовувати комплексний підхід, що включає виявлення вразливостей, алгоритми захисту та ефективну візуалізацію результатів. Комбінація методів аномалій, сигнатур та поведінкового аналізу у поєднанні з криптографічними протоколами може значно підвищити стійкість IoT-мереж до атак

Список використаних джерел

1. IEEE Internet of Things Journal // available at: <https://iee-iotj.org/>.
2. Кетрін Малліган, Девід Бойл, Ян Холлер, Стаматіс Карноускос, Стефан Авесанд, Власіос Ціаціс Інтернет речей: Принципи та парадигми // Journal of Sensor and Actuator Networks (JSAN). - available at: <https://www.mdpi.com/journal/jsan>.
3. Mosenia, A., & Jha, N. K. . A Comprehensive Study of Security in Internet of Things. IEEE Transactions on Emerging Topics in Computing, 5(4), 586-602, Available at: https://www.researchgate.net/publication/309055995_A_Comprehensive_Study_of_Security_of_Internet-of-Things
4. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. . *Internet of Things Security: A Survey*. Journal of Network and Computer Applications, 88, 10-28- Available at: <https://www.scirp.org/reference/referencespapers?referenceid=3327490>
5. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley. Available at: <https://www.taylorfrancis.com/chapters/edit/10.1201/9781003220978-3/analysis-systems-security-engineering-design-principles-development-secure-resilient-systems-paul-beach-logan-mailloux-brent-langhals-robert-mills>

Ключові слова: IoT Security, Vulnerability Detection in IoT, Cyberattacks in IoT, IoT Network Protocols and Security, Anomaly Detection in IoT. Виявлення вразливостей у мережах IoT, Кібератаки в мережах Інтернету речей Безпека IoT, Машинне навчання для безпеки IoT, Виявлення аномалій у IoT

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ МЕДИЧНОЇ ДІАГНОСТИКИ ІЗ ЗАСТОСУВАННЯМ НЕЙРОМЕРЕЖ

Юзва Анна

*Студентка кафедри комп'ютерних наук та кібербезпеки Волинського
національного університету імені Лесі Українки*

Собчук Валентин

*Професор кафедри інтегральних та диференціальних рівнянь Київського
національного університету імені Тараса Шевченка*

Біляєв Дмитро

Аспірант Державного університету інформаційно-комунікаційних технологій

Постановка проблеми

У сучасному світі медична діагностика стикається з низкою проблем, які аж ніяк не покращують якість медичних послуг, серед них: дефіцит фахівців-радіологів, високий обсяг медичних зображень для аналізу та необхідність зменшення ймовірності людських помилок. У таких умовах автоматизація процесу аналізу медичних знімків стає надзвичайно важливою.

Однак ефективність нейромережевих моделей залежить від багатьох факторів. Крім того, конфіденційність та етичність використання медичних даних є дуже важливими у сфері медицини. Ці виклики вимагають пошуку рішень, які зможуть забезпечити високу якість та надійність моделей штучного інтелекту, що будуть інтегровані у систему охорони здоров'я.

Ціль дослідження

Розробка ефективних нейромережевих підходів для автоматизації діагностики медичних зображень, оптимізація процесів підготовки даних та забезпечення точності, надійності й етичності діагностичних рішень.

Розробка нейромережевої моделі

Для покращення медичних послуг дуже важливо розвивати їх у всіх напрямках і автоматизація є одним з них. Шлях використання нейромереж може значно покращити швидкість та точність аналізу масивів зображень, чим зменшить навантаження на лікарів. Це дуже важливо в таких ситуаціях як зараз у нас в країні, дефіцит лікарів.

Те наскільки ефективними будуть нейромережі для діагностики дуже залежить від того наскільки ретельно будуть підготовлені дані. Нормалізація є одним з основних етапів, вона приводить піксельні значення зображень до

стандартного діапазону, що забезпечує стабільність і передбачуваність навчання моделі. Також важливою є аугментація даних, повороти, масштабування, зміна яскравості. Проблема нерівного розподілу, яка може спричинити упередженість моделі, вирішується балансуванням класів.

Основними метриками для визначення ефективності моделей є точність, чутливість, специфічність і F1-міра. Точність визначає загальну частку правильно класифікованих зображень і показує, наскільки добре модель справляється із завданням у середньому. Чутливість (або відношення справжніх позитивних результатів) відображає здатність моделі правильно виявляти патології, тобто захворювання, якщо вони присутні. Специфічність, у свою чергу, вимірює здатність моделі правильно ідентифікувати здорові знімки, знижуючи кількість хибних спрацьовувань. F1-міра є гармонійним середнім між точністю та чутливістю, що дозволяє врахувати як правильно виявлені патології, так і помилки класифікації.

Під час класифікації патологій можна стикнутись з низкою викликів, які можуть вплинути на ефективність та точність моделі. Однією з головних проблем є невідповідність між різними наборами даних. Неоднорідність якості зображень також є серйозною перешкодою. Рентгенівські знімки можуть відрізнятися за роздільною здатністю, контрастністю, наявністю шумів чи артефактів, що залежить від обладнання, умов зйомки та індивідуальних особливостей пацієнтів. Це може негативно впливати на точність класифікації, особливо якщо модель не адаптована до таких змін. Ще одним викликом є низький обсяг даних для рідкісних патологій. Такі захворювання, як рідкісні форми легеневих чи серцевих уражень, часто погано представлені у загальнодоступних наборах даних, що обмежує можливості тренування моделей. Це може призводити до поганої точності в класифікації цих станів, оскільки модель недостатньо знайома з їхніми характеристиками.

Використання нейромережових технологій у медичній діагностиці потребує вирішення низки етичних та практичних питань. Одним із ключових аспектів є забезпечення конфіденційності медичних даних пацієнтів. Медичні зображення часто містять чутливу інформацію, яка потребує захисту згідно з міжнародними стандартами, такими як GDPR у Європі чи HIPAA у США. Забезпечення конфіденційності вимагає анонімізації даних, зокрема видалення або шифрування ідентифікуючої інформації, такої як імена, дати народження чи номери ідентифікації пацієнтів.

Для навчання нейромереж на основі медичних зображень, таких як рентгенівські знімки та КТ, визначаються два основні шляхи навчання: на рентгенівських знімках та на КТ. Кожен з них може мати власні підходи та способи навчання.

Перший шлях спрямований на навчання моделі на рентгенівських знімках.

Підхід класифікації патологій дозволяє моделі аналізувати медичні знімки та класифікувати їх за наявністю певних патологій, таких як пневмонія, COVID-19 чи фіброз. Для навчання використовуються великі анотовані набори даних, що містять мітки, відповідні конкретним захворюванням. Наприклад, PadChest[4] є одним із найбільш всеосяжних наборів даних, що включає рентгенівські знімки з 174 діагнозами. Його різноманітність забезпечує навчання моделей розпізнаванню широкого спектра патологій.

Ще одним важливим ресурсом є COVID-19 Radiography Database[1], яка надає чітке розмежування між знімками пацієнтів із COVID-19, вірусною пневмонією та здоровими легень. Це створює надійну основу для навчання моделей на завданні розпізнавання COVID-19, що є актуальним у сучасній медичній діагностиці.

Використання таких наборів дозволяє створювати моделі, здатні автоматизувати аналіз медичних зображень, зменшувати час діагностики та підвищувати точність виявлення захворювань, особливо на ранніх стадіях.

Інший підхід передбачає використання не лише медичних зображень, а й текстових звітів, що супроводжують ці зображення. Наприклад, набір даних **MIMIC-CXR[3]** містить як рентгенівські знімки, так і текстові описи, написані лікарями. Це дозволяє створювати неймережі, які поєднують візуальну та текстову інформацію. Текстові звіти надають додатковий контекст для кожного зображення, що може покращити інтерпретованість моделі і допомогти в точнішій діагностиці. Використання багатомодальних даних дозволяє неймережам краще розуміти взаємозв'язок між зображеннями та їх описами, що значно покращує точність виявлення патологій і забезпечує більшу надійність результатів. Цей підхід є перспективним для медичних застосувань, де комбінація візуальної та текстової інформації може надати більш повну картину стану пацієнта.

Другий шлях навчає модель більш орієнтовано на КТ знімки.

Перший підхід фокусується на точному виявленні та сегментації легневих вузлів, що є ключовим для ранньої діагностики раку легень. Сегментація легневих вузлів на КТ-знімках є важливим етапом, оскільки допомагає виявити навіть невеликі зміни в тканинах, що можуть свідчити про наявність пухлин. Наприклад, набір даних **LIDC-IDRI[2]** містить КТ-знімки, а також анотації, створені кількома радіологами, які позначають вузли в легнях. Ці анотації є важливими для тренування моделей, що автоматично виявляють і сегментують ці вузли, покращуючи точність і швидкість діагностики раку легень. У поєднанні з наборами даних, такими як **MIMIC-CXR[3]**, можна додатково підвищити точність моделей завдяки використанню текстових звітів.

Текстові звіти, що супроводжують знімки, надають додатковий контекст для виявлення вузлів, допомагаючи нейромережам краще розуміти, які патології можуть бути присутні на зображенні. Це поєднання візуальних і текстових даних дозволяє досягти значного покращення у точності розпізнавання патологій, таких як рак легенів.

Інший підхід до навчання полягає в мультикласовій класифікації, де нейромережі вчать класифікувати різні стани, зокрема доброякісні та злоякісні вузли, нормальні та патологічні тканини. Такий підхід допомагає знизити кількість хибнопозитивних і хибнонегативних результатів, що є важливим для медичних діагнозів, де точність критична. Наприклад, у випадку з раком легень, мультикласова класифікація дозволяє моделі відрізнити між доброякісними утвореннями, які не потребують хірургічного втручання, і злоякісними, що потребують негайного лікування. Важливою частиною цього підходу є те, що модель має бути навчена на великих і різноманітних наборах даних, щоб уникнути переоснащення і забезпечити стійкість до варіацій у зображеннях, таких як різний кут знімка чи якість зображення.

Список використаних джерел

1. Papers with Code - Covid-19 radiography database Dataset. *The latest in Machine Learning I Papers With Code*. URL: <https://paperswithcode.com/dataset/covid-19-radiography-database> (date of access: 02.11.2024).
2. Papers with Code - LIDC-IDRI Dataset. *The latest in Machine Learning I Papers With Code*. URL: <https://paperswithcode.com/dataset/lidc-idri> (date of access: 02.11.2024).
3. Papers with Code - MIMIC-CXR Dataset. *The latest in Machine Learning I Papers With Code*. URL: <https://paperswithcode.com/dataset/mimic-cxr> (date of access: 02.11.2024).
4. Papers with Code - PadChest Dataset. *The latest in Machine Learning I Papers With Code*. URL: <https://paperswithcode.com/dataset/padchest> (date of access: 02.11.2024).

Ключові слова. Автоматизація діагностики, нейромережеві технології, рентгенівські знімки, нормалізація даних, класифікація патологій, мультикласова класифікація, медична діагностика.

Keywords. Diagnostic automation, neural network technologies, X-ray images, data normalization, pathology classification, multi-class classification, medical diagnostics.

ПРОБЛЕМА ЗАХИСТУ МЕРЕЖЕВИХ МАРШРУТИЗАТОРІВ

Овсянко Дмитро

аспірант кафедри Безпеки інформаційних технологій
Національного університету «Львівська Політехника»

Домашні маршрутизатори є критично важливим компонентом мережі Інтернет, що виконує підключення клієнтських пристроїв у локальній мережі до мережі Інтернет-провайдера (ISP).

З початку пандемії вірусу COVID-19 безпеці маршрутизаторів почали приділяти більше уваги. Багато компаній запровадили дистанційну роботу для співробітників, деякі з яких так і не повернулися до офісу. У результаті кіберзлочинці тепер розглядають домашні маршрутизатори як шлюзи до корпоративних мереж, а компанії – як потенційні вектори атак. У 2020 році Фраунгоферівській інститут комунікації, обробки інформації та ергономіки провів перше дослідження рівня безпеки домашніх маршрутизаторів та виявив значну кількість вразливостей [1]. Кількість вразливостей високого рівня, виявлених у маршрутизаторах різних виробників сягає сотень (рис.1).

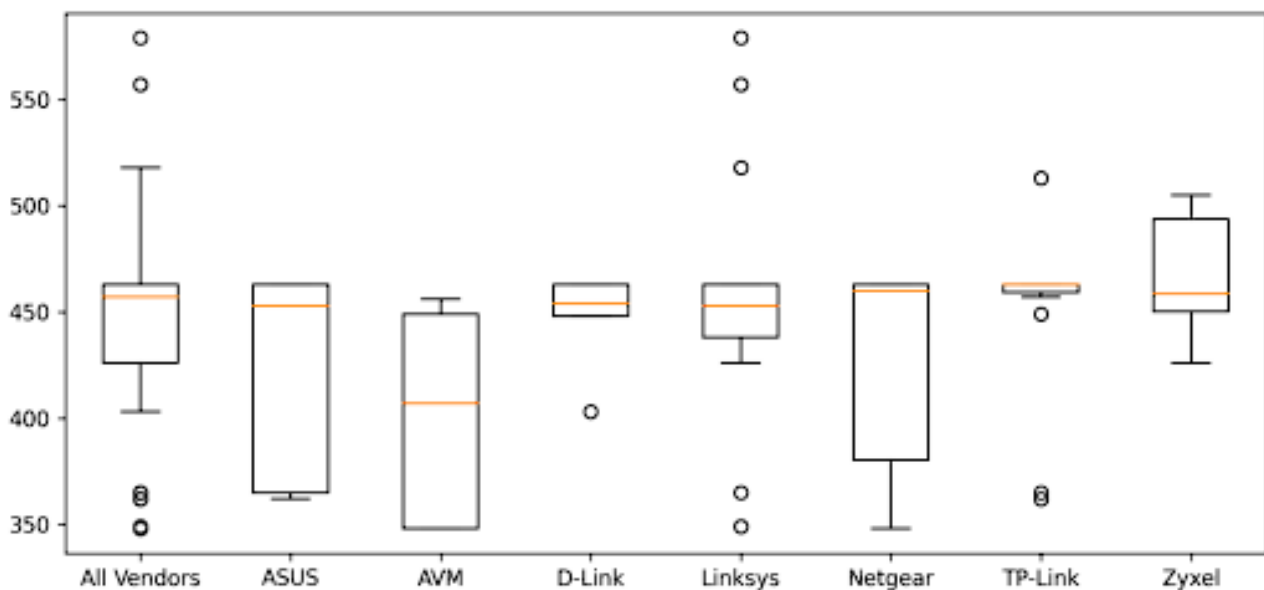


Рис. 1 Кількість вразливостей високого рівня в маршрутизаторах різних виробників

Критичність проблеми зростає через велике різноманіття моделей мережевих маршрутизаторів. Існує велика кількість виробників пристроїв, що використовують різне програмне та апаратне забезпечення, не зважаючи на сучасні спроби уніфікувати підходи до виробництва мережевих пристроїв. При розгляді безпеки мережевих пристроїв треба враховувати наступні особливості цього класу обладнання:

- Обмеженість в ресурсах. Обмеженість апаратних ресурсів, таких як пам'ять та процесорний час, унеможливають використання складних систем захисту, наприклад з використанням машинного навчання.
- Складна конфігурація. Залежно від необхідного функціоналу та апаратного забезпечення пристрої можуть мати різний набір модулів. Це може призвести до проблем з налаштуванням, що може відкрити шлях для атак. Також ускладнює уніфікацію методів захисту.
- Доступ до чутливої інформації. Це включає в себе особисті дані користувачів, дані про мережу та інші конфіденційні дані.

Звідси випливає, що методи захисту залежать конкретно від пристрою та видів загроз. Тому складніші методи захисту не знайшли широкого використання у мережевих пристроях. При розгляді безпеки мережевих пристроїв спеціалісти потрапляють у замкнутий «трикутник» (рис. 2) в межах якого пристрій вимушений працювати.

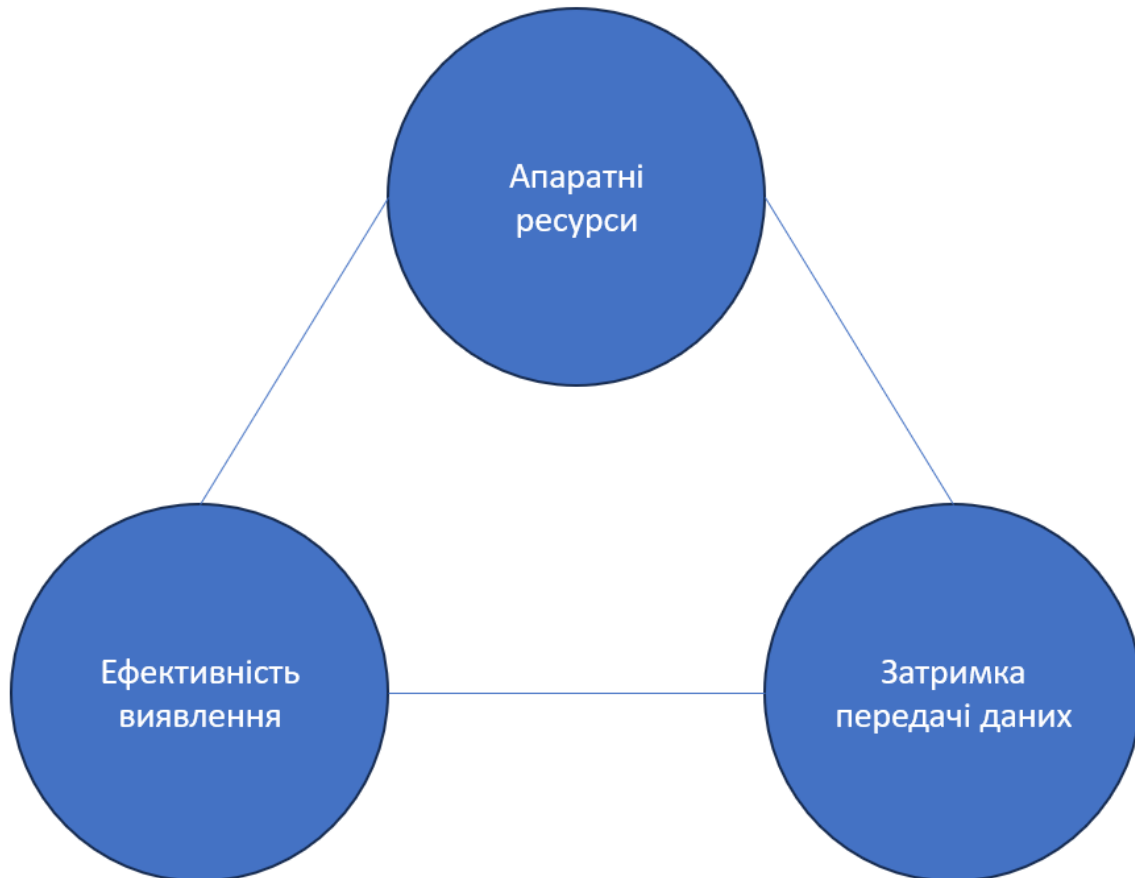


Рис 2. Трикутник обмежень систем, що працюють в мережевих маршрутизаторах

Він включає в себе три наступних проблеми:

1) Обмежена кількість ресурсів. Сучасні маршрутизатори значно потужніші за своїх попередників, проте ресурси досі обмежені. Кількість оперативної пам'яті може сягати кількох гігабайт, а процесорний час обмежений, проте паралельно з цим пристрій має виконувати комунікаційні функції. Також, може виникати обмеження на споживання електричної енергії, наприклад, для відповідності екологічним стандартам.

2) Ефективність виявлення. Попри роботу в обмежених ресурсах, система захисту має ефективно виявляти загрози. Якщо система не буде виконувати покладені на неї задачі, то єдине, що вона буде робити – це споживати і без того обмежені ресурси.

3) Вплив на затримку комунікацій. Хоча сучасні маршрутизатори і виконують багато різноманітних функцій, першочерговою функцією є комунікації.

При використанні модулів захисту, виникає затримка передачі даних, що може бути критичним за певних обставин. Для спеціалізованих фінансових структур мілісекунди можуть бути важливими, оскільки затримка може бути причиною значних збитків. Для побутових користувачів це може впливати на поточкову передачу даних, таку як зв'язок, трансляції відео, онлайн ігри.

Проблема полягає в тому, що неможливо забезпечити одночасно всі три пункти захисту. Якщо пристрій буде надто повільний, це призведе до зниження продажів. При цьому, якщо пристрій буде мати багато вразливостей, то це теж призведе до великої кількості відмов користувачів від використання.

Маршрутизатори зазвичай включають в себе пасивні методи захисту, які допомагають контролювати та обмежувати небажаний доступ, проте не виконують активної протидії загрозам або активного виявлення. Зазвичай реалізована фільтрація пакетів та обмеження доступу на основі списків контролю доступу, що забезпечує базовий рівень безпеки [2]. Для підвищення безпеки мережевих маршрутизаторів необхідно розглядати впровадження систем виявлення вторгнень (CBV), які аналізують мережевий трафік на предмет аномалій та можливих атак. CBV допомагає своєчасно виявляти та попереджати про наявність потенційних загроз, підвищуючи загальний рівень захисту мережі. Як статичні, так і динамічні системи виявлення вторгнень використовуються для виявлення несанкціонованого доступу до комп'ютерних систем або мереж. Однак між ними є ключова відмінність: статичні CBV аналізують інформацію, яка зібрана заздалегідь, а динамічні CBV здійснюють моніторинг системи в режимі реального часу. Статичні CBV створюють «відбиток» підконтрольної мережі та її середовища. Якщо статична CBV виявляє відхилення від відбитка, це може бути ознакою атаки. Динамічні CBV аналізують системні процеси, трафік в мережі та інші дані. Динамічні CBV зазвичай більш ефективні, ніж статичні, оскільки вони можуть виявляти атаки, які не були відомі на момент створення відбитка.

Через обмеженість ресурсів, довгий час мережеві маршрутизатори не були здатні застосовувати системи виявлення вторгнення, оскільки більшість з них потребувала більшої кількості ресурсів для аналізу трафіку. Крім цього, сучасні маршрутизатори намагаються прийти до стандартизації ПЗ для покращення комунікації між пристроями різних виробників. Це призвело до того, що все більше виробників стали відмовлятися від написання власних прошивок з нуля і почали використовувати Linux системи, такі як OpenWRT, RDK-B тощо. Окрім стандартизації цей підхід дозволяє використовувати Linux додатки для маршрутизаторів [3]. Здебільшого, вони потребують модифікацій, проте це значно спрощує та здешевлює розробку систем виявлення вторгнення для мережевих пристроїв або дозволяє застосовувати наявні CBV.

Хоча безпека мережевих пристроїв все ще не є популярною темою в сфері кібербезпеки у порівнянні із загрозами в системах загального призначення, вразливості в мережевих вбудованих системах набувають все більш загрозливого рівня. З огляду на зростання рівня критичності вразливостей мережевих пристроїв доцільно розглянути можливість адаптації систем виявлення вторгнень для мережевого обладнання. Це допоможе оперативно реагувати на потенційні атаки, знижуючи ризик витоку конфіденційної інформації та забезпечуючи стабільну роботу мережевих ресурсів. Інтеграція таких систем сприятиме підвищенню рівня безпеки мережі, роблячи її більш стійкою до новітніх кіберзагроз.

Список використаних джерел:

1. Weidenbach P., Dorp vom J. Home Router Security Report 2020. *Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE*. URL: https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouter-Security_2020_Bericht.pdf (date of access: 08.11.2024).
2. XDRI Attacks- and- How to Enhance Resilience of Residential Routers / P. Jeitner et al. *31th USENIX Security Symposium (USENIX Security 22)*, 2022 : Матеріал міжнародної конференції, 10–12 August 2020. P. 118. URL: <https://doi.org/10.48550/arXiv.2208.12003>.
3. Wang M., Yang N., Weng N. Securing a Smart Home with a Transformer-Based IoT Intrusion Detection System. *Electronics*. 2023. Vol. 12, no. 9. P. 2100. URL: <https://doi.org/10.3390/electronics12092100> (date of access: 08.11.2024).

Ключові слова: Безпека мережевих пристроїв, системи виявлення вторгнень, вразливості вбудованих систем.

Keywords: Network device security intrusion detection systems, embedded system vulnerabilities.

ЗАХИСТ ВІД ЗОВНІШНІХ ТА ВНУТРІШНІХ КІБЕРЗАГРОЗ

Олександр Колесніков

*студент 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

Аналіз несанкціонованого доступу в комп'ютерні мережі свідчить про необхідність комплексного підходу до забезпечення безпеки, що враховує різноманітні кіберзагрози, спрямовані як ззовні, так і зсередини організації [1].

У боротьбі з зовнішніми та внутрішніми кіберзагрозами є люди, процеси та речі, які слід інтегрувати, об'єднати та задіяти. Ось кілька практичних кроків, які допоможуть зміцнити свій захист:

Порівняльна Таблиця

Зовнішні кіберзагрози	Внутрішні кіберзагрози
Сегментація мережі	Контроль доступу
Брандмауери та IDS/IPS	Управління привілейованим доступом
Шифрування	Запобігання втраті даних (DLP)
Управління вразливостями	Реагування на інциденти
Брандмауери веб-додатків (WAF)	Навчання співробітників
Безпека електронної пошти	Моніторинг та ведення журналів
Захист кінцевих точок	Відповідність та управління

Зовнішні кіберзагрози:

Організаційно розділіть вашу мережу на різні зони та застосуйте кратну кількість рівнів безпеки для кожної зони, щоб уникнути поширення вірусів та зловмисного доступу.

Немає нічого важливішого, ніж правильне використання брандмауерів та використання IDS/IPS для контролю трафіку, який вважається небезпечним.

Шифруйте дані, які потрібно переміщувати з місця на місце або які зберігаються у вашій мережі чи в хмарі.

Постійно шукайте та виправляйте вразливості у ваших системах, додатках та програмному забезпеченні.

Використовуйте брандмауери веб-додатків для захисту від атак на веб-додатки, які включають SQL-ін'єкції та міжсайтовий скриптинг (XSS).

Впроваджуйте рішення для захисту електронної пошти від спаму, фішингу та шкідливого програмного забезпечення.

Впроваджуйте рішення для захисту кінцевих точок, такі як антивірусні програми, антивірусні програми та HIDS, щоб запобігти зараженню шкідливим кодом та несанкціонованому доступу.

Внутрішні кіберзагрози:

Завжди застосовуйте надійну автентифікацію користувачів, за допомогою якої користувачі повинні надати більше одного способу підтвердження своєї особи, щоб отримати доступ до даних і системи.

Використовуйте рішення з управління привілейованим доступом (PAM) для нагляду за доступом, а також для контролю доступу до певних систем та інформації.

Використовуйте інструменти DLP для виявлення та уникнення витоків і втрати даних під час надсилання або передачі інформації за межі організації.

З будь-якою встановленою внутрішньою зловмисною діяльністю слід боротися шляхом розробки та постійного застосування процедури реагування на інциденти.

Проводьте навчання працівників та надавайте їм інструкції з питань кібербезпеки, включаючи управління паролями, протидію фішингу та поведіння з даними.

Використовуйте плани моніторингу та фіксованої реєстрації для виявлення та боротьби з внутрішніми кіберзагрозами.

Дотримуйтесь норм і стандартів, включаючи, але не обмежуючись, GDPR, HIPAA та PCI-DSS, а також впроваджуйте надійну програму управління для постійного управління ризиками кібербезпеки.

Додаткові найкращі практики:

Регулярно оновлюйте програмне забезпечення та патчі. Встановлюйте найновіші патчі безпеки для програмного забезпечення, операційної системи та додатків, які ви використовуєте на своєму комп'ютері.

Використовуйте надійні паролі. Це включає використання дуже складних і спеціальних паролів для всіх облікових записів і, можливо, використання програмного забезпечення для підбору паролів.

Відстежуйте підозрілу активність. Щоразу, коли щось не так, включаючи дивні спроби входу або отримання даних у вашій фірмі, негайно реагуйте на загрози.

Проводьте регулярний аудит безпеки. Щорічно слід проводити дослідження з оцінки безпеки, щоб виявити загрози та вразливі місця, і таким чином розробити дорожню карту, як з ними боротися.

Створіть команду з кібербезпеки. Організуйте команду з кібербезпеки, яка забезпечуватиме безпеку та координуватиме роботу з різними програмами, а також працюватиме над вирішенням проблем у міру їх виникнення.

Дотримуючись цих найкращих практик, зможете значно мінімізувати ймовірність виникнення зовнішніх і внутрішніх кіберзагроз, які можуть завдати шкоди даним і системам вашої організації.

Список використаних джерел:

1. Василенко М., Рачук В., Слатвінська В. Аналіз несанкціонованого доступу в комп'ютерні мережі в контексті заходів щодо їх безпеки. Інформаційні технології та суспільство. 2024. № 2 (13). С. 12-16. DOI: <https://doi.org/10.32689/maup.it.2024.2.2> URL: <https://journals.maup.com.ua/index.php/it/article/view/3927> (дата звернення: 09.11.2024).

Ключові слова: кіберзагроза, кібербезпека, вразливості.

Keywords: cyber threat, cybersecurity, vulnerabilities.

Науковий керівник : к. ф.-м. н., доцент Черевко Є.В.

АНАЛІЗ СУЧАСНИХ ТРЕНДІВ АТАК АРТ-ГРУП

Опанович Максим

*аспірант кафедри захисту інформації Національного університету
«Львівська політехніка»*

У сучасному цифровому середовищі кіберзагрози еволюціонують з безпрецедентною швидкістю, вимагаючи від організацій постійного оновлення стратегій безпеки. Аналізуючи звіти про останні тренди в кібератаках[1-3], можна прослідкувати тенденції розвитку методів атак та визначення їх патернів, що дозволить ефективніше виявляти загрози та сфокусувати увагу команд захисту на вразливих компонентах інформаційних систем. Основна увага приділяється методам, які використовують зловмисники, та тенденціям, що формують сучасний ландшафт кібербезпеки.

1. Ідентичність як основний вектор атаки

1.1. Компрометація облікових записів

Однією з головних тенденцій є використання зловмисниками компрометації ідентичностей як основного засобу доступу до корпоративних систем. З поширенням хмарних технологій та SaaS-рішень, облікові записи стають ключем до великої кількості ресурсів. Зловмисники активно використовують фішинг, соціальну інженерію та крадіжку облікових даних для отримання несанкціонованого доступу.

1.2. Обхід багатофакторної автентифікації (MFA)

Незважаючи на впровадження MFA як стандартного заходу безпеки, зловмисники знаходять способи його обходу. У 2023 році особливо поширеним став метод соціальної інженерії, спрямований на технічну підтримку. Зловмисники, видаючи себе за внутрішніх співробітників, переконують служби підтримки змінювати налаштування MFA або надавати доступ до облікових записів. Це підкреслює вразливість людського фактору в системах безпеки.

2. Еволюція методів початкового доступу

2.1. Фішинг та соціальна інженерія

Фішинг залишається одним із найефективніших методів початкового доступу. У 2023 році зловмисники активно використовували різноманітні формати файлів для доставки шкідливого ПЗ, обходячи механізми безпеки, такі як Mark-of-the-Web (MOTW). Після оновлення Microsoft у листопаді 2022 року, яке обмежило використання ISO та ZIP-файлів, зловмисники перейшли на інші формати, такі як OneNote-файли та MSIX-пакети.

2.2. Малвертайзинг та SEO-поєднання

Малвертайзинг, або зловмисна реклама, став ключовим інструментом для розповсюдження шкідливого ПЗ. Кампанії, такі як Charcoal Stork та

ChromeLoader, використовували платформи реклами для поширення підrobних програмних оновлень або популярних додатків. SEO-поєднання дозволяє зловмисникам маніпулювати результатами пошуку, спрямовуючи користувачів на шкідливі сайти.

3. Використання вразливостей у програмному забезпеченні

3.1. Експлуатація нових та старих уразливостей

У 2023 році було зафіксовано активну експлуатацію як нових, так і старих вразливостей. Зловмисники використовували уразливості в таких продуктах, як TeamCity, Progress Software WS_FTP та PaperCut, для отримання початкового доступу. Водночас, старі уразливості в Telerik та Fortinet також залишалися ціллю, що підкреслює важливість регулярного оновлення програмного забезпечення.

3.2. Пост-експлуатаційні дії

Після успішної експлуатації вразливості, зловмисники зазвичай завантажували веб-шелл або віддалені адміністративні інструменти. Це дозволяло їм отримати привілеї, збирати облікові дані та рухатися мережею. Методи залишалися доволі консервативними, використовуючи такі інструменти, як Mimikatz для збору паролів та Impacket для переміщення мережею.

4. Програмне забезпечення-крадії як інструмент зловмисників

4.1. Поширення та цілі

Програми-крадії, такі як RedLine, LummaC2 та Ducktail, стали широко використовуваними для збору конфіденційної інформації. Вони націлені на паролі, куки, файли та навіть криптовалютні гаманці. Особливий інтерес викликає зростання кількості атак на macOS-системи, де з'явилися нові загрози, такі як Atomic Stealer та MacStealer.

4.2. Методи доставки

Зловмисники використовують різноманітні методи доставки крадіїв:

- **Малвертайзинг:** Поширення через підrobні оголошення або сайти, що імітують легітимні.
- **Фішингові електронні листи:** Вкладені файли або посилання, що ведуть до завантаження шкідливого ПЗ.
- **Соціальні мережі:** Контакткування потенційних жертв через платформи, такі як LinkedIn, з пропозиціями роботи або іншими привабливими пропозиціями.

5. Зловживання інструментами віддаленого управління

5.1. Легітимність як маскування

Інструменти віддаленого управління, такі як NetSupport Manager, Remcos та Atera, є легітимними програмами, які широко використовуються адміністраторами. Зловмисники використовують цю легітимність для маску-

вання своїх дій, що ускладнює їхнє виявлення. Вони часто встановлюють ці інструменти в нестандартні директорії або під іншими іменами файлів.

Особливу увагу привернула група SCATTERED SPIDER, яка активно використовувала різноманітні RMM-інструменти для швидкого переміщення мережею. Вони використовували десятки різних інструментів, що свідчить про їхню адаптивність та гнучкість. Їхні методи включали використання SMS-фішингу та соціальної інженерії для отримання доступу.

6. Тенденції у використанні штучного інтелекту

6.1. Автоматизація атак

Зловмисники почали активно впроваджувати штучний інтелект для автоматизації та покращення ефективності своїх атак. ШІ дозволяє створювати більш переконливі фішингові повідомлення, автоматично аналізувати великі обсяги даних для виявлення вразливих цілей та навіть генерувати шкідливий код, який важче виявити.

6.2. ШІ для уникнення виявлення

З використанням ШІ зловмисники можуть адаптувати свої методи в реальному часі, уникаючи виявлення традиційними антивірусними та IDS/IPS системами. Вони можуть змінювати сигнатури шкідливого ПЗ, використовувати поліморфізм та інші техніки для обходу систем захисту.

Аналіз демонструє, що зловмисники стають все більш інноваційними та адаптивними, використовуючи як нові технології, так і вдосконалюючи традиційні методи атак. Компрометація ідентичностей, використання програм-крадіїв та зловживання легітимними інструментами віддаленого управління є ключовими трендами, які формуватимуть ландшафт кіберзагроз у майбутньому.

Список використаних джерел:

1. 2024 Threat Detection Report: techniques, Trends & Takeaways., RedCanary, 2024.
2. Top Cybersecurity Threats in 2024. URL: <https://onlinedegrees.sandiego.edu/top-cyber-security-threats/>
3. CrowdStrike 2024 Global Threat Report. URL: <https://crowdstrike.com/global-threat-report>

Ключові слова: APT, кібер-атака, еволюція загроз

Keywords: APT, cyber-attack, threat evolution

ЕМУЛЯЦІЯ DOS/DDOS АТАК В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Кузьменко Денис

*аспірант кафедри кібербезпеки та математичного моделювання,
Національного університету «Чернігівська політехніка»*

Атаки відмови в обслуговуванні (DoS) та розподілені атаки відмови в обслуговуванні (DDoS) є одними з найпоширеніших і найнебезпечніших загроз для інформаційних систем. Вони націлені на виснаження ресурсів системи, роблячи її недоступною для користувачів. Емуляція таких атак є ключовим інструментом для оцінки стійкості та безпеки системи, а також для розробки ефективних механізмів захисту. DoS/DDoS атаки ґрунтуються на ідеї перевантаження ресурсів цільової системи, що може включати процесорний час, пам'ять, пропускну здатність мережі або інші критично важливі ресурси. У розподілених DDoS атаках використовується велика кількість скомпрометованих пристроїв (так званих "ботів") для одночасного надсилання запитів до цілі, що значно ускладнює їх виявлення та блокування. Емуляція DoS/DDoS атак передбачає моделювання умов, які відповідають реальним атакам, з метою оцінки реакції системи та її здатності протистояти таким загрозам. Це дозволяє виявити вразливості в архітектурі системи, конфігурації мережі та налаштуваннях безпеки. Розглянемо основні методи емуляції DoS/DDoS атак:

1. Генерація трафіку високої інтенсивності: Створення великої кількості запитів до системи для перевірки її здатності обробляти навантаження. Це може бути досягнуто за допомогою спеціалізованих інструментів, що генерують трафік певного типу.

2. Симуляція різних типів атак: Емуляція специфічних протоколів або вразливостей, наприклад, атаки на рівні мережевих протоколів (SYN flood, UDP flood) або на рівні додатків (HTTP flood).

3. Використання розподілених інструментів: Моделювання DDoS-атак шляхом одночасного запуску трафіку з декількох джерел або за допомогою віртуалізації для імітації великої кількості атакуючих вузлів.

Далі опишемо основні моделі для емуляції трафіку DoS/DDoS атак. Модель Пуассона широко використовується для моделювання випадкових подій у часі, включаючи мережевий трафік. У контексті DoS/DDoS атак, процес Пуассона може моделювати кількість пакетів або запитів, що надходять до сервера за певний інтервал часу. Нехай $N(t)$ — число подій (прибуття пакетів) до моменту часу t . Процес Пуассона з параметром λ має такі властивості:

$$P(N(t) = k) = \frac{(\lambda t)^k e^{-\lambda t}}{k!} \quad (1)$$

Інтервали між подіями є незалежними та експоненційно розподіленими з параметром λ :

$$f_T(t) = \lambda e^{-\lambda t} \quad (2)$$

У простих моделях DoS атак припускається, що атакуючі генерують пакети з постійною середньою інтенсивністю λ . Це дозволяє оцінити навантаження на систему та аналізувати її стійкість до атак з відомою інтенсивністю. Реальний трафік DoS/DDoS атак може бути більш непередбачуваним та самоподібним, що не повністю описується процесом Пуассона.[1]

Фрактальні та самоподібні моделі трафіку

Фрактальні моделі враховують довгострокову залежність та самоподібність мережевого трафіку. Інтернет-трафік часто має властивість самоподібності, що характеризується важкими хвостами в розподілах та довгостроковою залежністю. Фрактальні моделі можна представити за допомогою автокореляційної функції з повільним спаданням:

$$R(k) \sim k^{-\beta}, 0 < \beta < 1 \quad (3)$$

Херстовий показник (Hurst parameter) H :

$$H = 1 - \frac{\beta}{2} \quad (4)$$

Де $H \in (0.5, 1)$ для самоподібних процесів.

Самоподібні моделі дозволяють більш точно описати характер трафіку під час DDoS атак, враховуючи його нерівномірність.[2]

Моделі ботнетів на основі епідеміологічних моделей

Епідеміологічні моделі, такі як SIR (Susceptible-Infectious-Recovered), використовуються для моделювання поширення ботнетів у мережі. Модель дозволяє оцінити розмір ботнету $I(t)$ у часі, що визначає потенційну потужність DDoS атаки.

$$\frac{dS(t)}{dt} = -\beta S(t)I(t) \quad (5)$$

$$\frac{dI(t)}{dt} = \beta S(t)I(t) - \gamma I(t) \quad (6)$$

$$\frac{dR(t)}{dt} = \gamma I(t) \quad (7)$$

Де $S(t)$ — кількість вразливих вузлів у момент часу t , $I(t)$ — кількість інфікованих вузлів (ботів), $R(t)$ — кількість відновлених або захищених вузлів, β — швидкість інфікування, γ — швидкість відновлення.[3]

Теорія черг

Системи масового обслуговування (СМО), використовуються для моделювання та аналізу процесів обслуговування запитів у серверах. У контексті DoS/DDoS атак, СМО допомагає зрозуміти, як збільшення інтенсивно-

сті прибуття запитів впливає на продуктивність сервера та час очікування користувачів.[4] Коефіцієнт завантаження сервера:

$$\rho = \frac{\lambda}{\mu} \quad (8)$$

λ — середня інтенсивність прибуття запитів, μ — середня інтенсивність обслуговування запитів, ρ відображає, наскільки завантажений сервер. Якщо $\rho=0.5$, сервер зайнятий 50% часу. При $\rho \rightarrow 1$, сервер майже постійно зайнятий. Середня кількість запитів у системі :

$$L = \frac{\rho}{1-\rho} \quad (9)$$

Формула показує залежність між завантаженням сервера та середньою кількістю запитів у системі. При ρ близькому до 1, $(1-\rho) \rightarrow 0$, що призводить до різкого збільшення L . Це відображає ситуацію, коли сервер не встигає обробляти всі запити, і черга зростає. Середній час перебування в системі (W):

$$W = \frac{1}{\mu - \lambda} \quad (10)$$

Формула показує, скільки часу в середньому займає обслуговування одного запиту, включаючи час очікування. При $\lambda \rightarrow \mu$, різниця $(\mu - \lambda)$ стає дуже малою, і W зростає значно. Це означає, що користувачі будуть довго чекати на обслуговування.

Загалом, глибоке розуміння методів емуляції DoS/DDoS атак та їх математичного моделювання є необхідним для підвищення безпеки інформаційних систем. Це дозволяє не лише виявляти та усувати вразливості, але й розробляти проактивні заходи захисту, забезпечуючи стабільну та безперебійну роботу систем навіть в умовах підвищеного ризику кібератак.

Список використаних джерел

1. What do packet dispersion techniques measure? [Електронний ресурс] / C. Dovrolis, P. Ramanathan, D. Moore – Режим доступу: <https://www.researchgate.net/publication/3893862>
2. On the self-similar nature of Ethernet traffic [Електронний ресурс] / W. Leland, M. Taqqu, W. Willinger, D. Wilson – Режим доступу: <https://dl.acm.org/doi/10.1109/90.282603>
3. Worm propagation modeling and analysis under dynamic quarantine defense [Електронний ресурс] / C. C. Zou, W. Gong, D. Towsley – Режим доступу: <https://dl.acm.org/doi/10.1145/948187.948197>
4. Trivedi, K. S., & Naidu, K. V. M. (1995). Composite performance and availability analysis of fault-tolerant systems. IEEE Transactions on Reliability, 44(2), 221–232.

Ключові слова: Атаки відмови в обслуговуванні, Denial of Service (DoS), Розподілені атаки відмови в обслуговуванні, Distributed Denial of Service (DDoS), Інформаційні системи, Емуляція атак

Keywords: Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS), Information systems, Attack emulation

ПРОЕКТУВАННЯ ЗАСОБУ ПЕРЕДАЧІ ПРИХОВАНИХ ПОВІДОМЛЕНЬ ЗА ДОПОМОГОЮ DNS-ТУНЕЛЮВАННЯ

Павлюк Олександр - Юрій

*аспірант кафедри безпеки інформаційних технологій
Національного університету «Львівська політехніка»*

Нечипор Степан

*бакалавр кафедри безпеки інформаційних технологій
Національного університету «Львівська політехніка»*

Система Доменних Імен (DNS) традиційно використовується для перекладу доменних імен у чисельні IP-адреси, забезпечуючи зручний доступ до ресурсів Інтернету. Однак, за рахунок глобального поширення, DNS містить більше застосувань, ніж просто резолвінг доменних імен. Одним з таких нестандартних підходів є DNS-тунелювання – технологія, яка дозволяє передавати довільні дані через протокол DNS [1].

Ідея використання DNS для передачі даних може здатися неочевидною, оскільки цей протокол первинно розроблений для зовсім інших цілей. Проте, завдяки своєму широкому розповсюдженню та принципу публічності, DNS-система потенційно може бути використана для створення каналів передачі даних, які дозволяють обходити мережеві фільтри та забезпечувати приховану комунікацію. DNS має ряд властивостей, які роблять протокол підходящим для таких цілей [2]:

- Глобальна доступність: DNS-сервери є невід'ємною частиною Інтернету, що забезпечує широкі можливості для встановлення з'єднання.
- Проходження через фільтри: Трафік DNS часто не піддається детальному аналізу, що дозволяє обходити фільтри та брандмауери.
- Низький рівень підозрілості: Через свою поширеність та прямолінійність, DNS-трафік рідко викликає підозри.

За умов правильної конфігурації, протокол DNS можна використати як технічну основу для простого текстового месенджера, який може бути корисним в умовах обмеженого доступу до мережі або для обходу цензури. Для цього можна скористатись процесом, відомим як DNS-тунелювання: це концепт, що дозволяє створити прихований і відносно безпечний канал для передачі текстових повідомлень.

Технічні аспекти реалізації, переваги та недоліки такого месенджера, а також можливі застосування та ризики можна розглянути змодельювавши принцип роботи системи прихованої передачі даних.

Учасники процесу:

- Клієнт: Відправляє дані через DNS-тунель.
- Сервер: Приймає дані, що передаються через DNS-тунель.

- DNS-сервери: Обробляють DNS-запити, не підозрюючи про прихований трафік.

Для забезпечення конфіденційності даних використовується симетричний алгоритм шифрування, наприклад, AES. Обидві сторони попередньо обмінюються секретним ключем. Дані, що передаються, потрібно перетворити на послідовність символів, які можна вставити в поля DNS-запитів. Для цього можна використати Base64 кодування; хоча Base64 збільшує розмір даних приблизно на 33%, він все ще є досить компактним для використання в DNS-запитах.

Процес передачі даних у спрощеному вигляді виглядає таким чином:

1. TLS-handshake:

- Клієнт ініціює з'єднання з сервером;
- Відбувається обмін криптографічними повідомленнями, в результаті якого обидві сторони генерують спільний секретний ключ.

2. Формування DNS-запитів:

- Клієнт бере фрагмент даних (наприклад, текстове повідомлення), шифрує його за допомогою спільного ключа, кодує в формат Base64 та розбиває на фрагменти;

- Отримані фрагменти вставляються у відповідні поля DNS-запиту (наприклад, у ім'я домену або значення TXT-запису);

- Формується DNS-запит і відправляється на DNS-сервер.

3. Обробка DNS-відповіді:

- Сервер отримує DNS-запит, витягує зашифровані дані з відповідних полів.

- Розшифровує дані за допомогою спільного ключа.

- Декодує дані з формату Base64 і отримує вихідні дані.

Таким чином, між клієнтом та сервером відбувається обмін даних за використанням лише протоколу DNS, окрім початкового TLS-рукошлякування. Цей опис роботи месенджера є спрощеним і не охоплює всіх нюансів DNS-тунелювання. Процес також передбачає ряд проблем та обмежень:

- Оскільки розмір DNS-запитів обмежений, кількість даних, які можна передати за один раз, також обмежена. Це призводить до необхідності розбивати великі файли на менші частини і передавати їх послідовно, що збільшує час передачі.

- Велика кількість запитів або проблеми з мережею можуть призвести до значних затримок у доставці даних, хоч DNS-запити зазвичай і мають високий пріоритет та обробляються швидко.

- Як наслідок розбивання повідомлень на велику кількість запитів можуть виникати аномалії в DNS-трафіку, що вказуватимуть на наявність ту-

нелю. Це може бути досягнуто шляхом аналізу розміру пакетів, частоти запитів, змісту відповідей та інших параметрів.

Переваги та недоліки DNS-тунелювання наведено у таблиці.

<i>Переваги</i>	<i>Недоліки</i>
<u>Стійкість до блокування</u> : DNS-тунелювання використовує стандартний протокол DNS, який зазвичай дозволений в більшості мереж.	<u>Низька пропускна здатність</u> : Через обмеження розміру DNS-пакетів і необхідність шифрування даних, пропускна здатність DNS-тунелів
<u>Пройходження через проксі-сервери та брандмауери</u> : Багато проксі-серверів і брандмауерів дозволяють DNS-трафік, що дозволяє використати	<u>Висока затримка</u> : Розбиття даних на маленькі фрагменти і послідовна їх передача призводять до значної затримки при передачі великих об'
<u>Відносна анонімність</u> : За рахунок використання стандартного протоколу DNS і шифрування даних, DNS-тунелювання може забезпечити певний рівень анонімності. Од-	<u>Складність реалізації</u> : Реалізація надійного і ефективного DNS-тунелю вимагає глибоких знань в області мережевих протоколів, криптографії і програмування.

DNS-тунелі дозволяють обходити мережеві фільтри та брандмауери, які блокують доступ до певних веб-сайтів або сервісів. Це особливо актуально в країнах з жорсткою цензурою Інтернету. Також DNS-тунелювання може бути використане для створення приватних мереж між різними пристроями. Це дозволяє обмінюватися даними конфіденційно, уникаючи перехоплення інформації сторонніми особами.

Втім, при проектуванні такого каналу комунікації, варто зважати і на ризики для кібербезпеки: хакери можуть використовувати DNS-тунелі для створення каналів управління зараженими пристроями, обходячи традиційні засоби виявлення, або для ексфільтрації та виведення цінних даних з мереж непомітним чином. Також, велика кількість DNS-запитів, що генеруються тунелем, може призвести до перевантаження DNS-серверів і спричинити відмову в обслуговуванні.

Підсумовуючи, месенджер з використанням DNS-тунелювання пропонує інноваційний підхід до передачі даних, використовуючи протокол DNS для створення прихованих каналів комунікації. Завдяки шифруванню і спеціальним методам кодування, дані можуть бути надійно захищені від несанкціонованого доступу. Однак, ця технологія не позбавлена недоліків. Обмежена пропускна здатність, затримки в передачі даних та ризик виявлення роблять DNS-тунелювання не ідеальним рішенням для всіх завдань. Майбутні дослідження варто фокусувати на підвищенні швидкості передачі даних за допомо-

гою використання компресії та зниженню ризику виявлення через застосування ефективних методів обфускації.

Список використаних джерел:

1. Salat L., Khan N. DNS Tunnelling, Exfiltration and Detection over Cloud Environments. *Sensors* 2023, 23(5), 2760; <https://doi.org/10.3390/s23052760>.
2. Alzighaibi A. R. Detection of DoH Traffic Tunnels Using Deep Learning for Encrypted Traffic Classification. *Computers* 2023, 12(3), 47; <https://doi.org/10.3390/computers12030047>.

Ключові слова: DNS-тунелювання, приховані повідомлення, мережеві фільтри, шифрування AES, обхід цензури

Keywords: DNS tunneling, hidden messages, network filters, AES encryption, censorship bypass

ПЕРЕВАГИ І НЕДОЛІКИ ХМАРНИХ СХОВИЩ ДЛЯ КЕРУВАННЯ ПАРОЛЯМИ ICLOUD ТА CHROME

В'ячеслав Бевза

*студент 4 курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

Як зазначають В.І. Бевза та В.М. Слатвінська, збої у захисті систем, як-от CrowdStrike, можуть призводити до масових витоків паролів, що ставить під сумнів надійність хмарних сервісів для зберігання конфіденційної інформації [1].

iCloud - це хмарне сховище та сервіс хмарних обчислень від Apple, що дозволяє користувачам зберігати та отримувати доступ до своїх файлів, фотографій, музики та інших даних на всіх пристроях Apple. Chrome Cloud Environment, з іншого боку, є хмарною платформою, розробленою компанією Google, що надає набір інструментів для підвищення продуктивності, включаючи Google Диск, Документи, Таблиці та Слайди.

iCloud - це хмарне сховище та сервіс хмарних обчислень від Apple Inc. Він дозволяє користувачам зберігати та отримувати доступ до своїх даних, включаючи файли, фотографії, контакти, календарі та багато іншого, з будь-якого пристрою, підключеного до Інтернету.

Основні функції:

1. Хмарне сховище: Зберігайте файли, документи та фотографії в iCloud Drive, доступні з будь-якого пристрою.

2. Хмарне резервне копіювання: Автоматичне резервне копіювання даних з iPhone, iPad або iPod touch до iCloud.

3. Хмарна синхронізація: Синхронізуйте дані на всіх своїх пристроях, включаючи контакти, календарі, нагадування тощо.

4. Знайти мій iPhone/iPad: Знайдіть і віддалено заблокуйте або видаліть свій пристрій, якщо його загублено або викрадено.

5. iCloud Photo Library: Зберігайте свої фотографії та відео та отримуйте доступ до них з будь-якого пристрою.

Хмарне середовище Chrome - це хмарна інфраструктура та послуги, що надаються популярним веб-браузером Google Chrome. Хмарне середовище Chrome призначене для забезпечення безперебійного та безпечного перегляду веб-сторінок на різних пристроях.

Основні функції:

1. Хмарне сховище: Зберігайте закладки, історію та інші дані з будь-якого пристрою та отримуйте до них доступ.

2. Хмарна синхронізація: Синхронізуйте дані веб-перегляду, включаючи паролі, розширення та налаштування, на всіх своїх пристроях.

3. Безпека в хмарі: Вбудовані функції безпеки Chrome, такі як "пісочниця" та захист від шкідливого програмного забезпечення, допомагають захистити ваш досвід роботи в Інтернеті.

4. Продуктивність у хмарі: Хмарна інфраструктура Chrome допомагає зменшити час завантаження сторінок і підвищити загальну продуктивність браузера.

5. Хмарна співпраця: Хмарні функції Chrome, такі як Google Диск і Google Документи, забезпечують безперешкодну співпрацю та обмін файлами.

iCloud, і хмарне середовище Chrome надають можливості хмарного зберігання та синхронізації. Однак є кілька ключових відмінностей:

1. Платформа: iCloud доступний виключно для пристроїв Apple, тоді як Chrome Cloud Environment доступний на багатьох платформах, включаючи Windows, macOS та Linux.

2. Сховище: iCloud пропонує 5 ГБ безкоштовного сховища, тоді як Chrome Cloud Environment пропонує 15 ГБ безкоштовного сховища.

3. Синхронізація: iCloud синхронізує ширший спектр даних, включаючи контакти, календарі та нагадування, тоді як Chrome Cloud Environment більше зосереджується на специфічних для браузера даних, таких як закладки та історія.

4. Безпека: Обидва сервіси мають надійні функції безпеки, але в Chrome Cloud Environment більше уваги приділяється захисту від шкідливого програмного забезпечення та пісочниці (Таблиця 1):

Параметри	Icloud	Chrome
Зберігання файлів	До 5 Гб безкоштовного сховища з можливістю розширення до 50 Гб, 200 Гб або 1	15 Гб безкоштовного сховища з можливістю розширення до 100 Гб,
Синхронізація	Автоматична синхронізація файлів, контактів, календарів та інших даних між	Функції спільної роботи в реальному часі в Google Документах,
Резервне копіювання	Автоматичне резервне копіювання пристроїв iOS, включаючи фотографії, контакти та інше	Доступ до набору інструментів для підвищення продуктивності, включаючи Google Диск, Документи, Таб-
Безпека	Наскрізне шифрування, двофакторна автентифікація та захищені сервери	Наскрізне шифрування, двофакторна автентифікація та захищені
Інтеграція	Безшовна інтеграція з іншими сервісами Apple, такими як iMessage, FaceTime та Apple Music	Безперешкодна інтеграція з іншими сервісами Google, такими як Gmail, Google Calendar

Таблиця 1. Порівняльна таблиця параметрів

Отже, iCloud та Chrome Cloud Environment - це сервіси хмарного зберігання та хмарних обчислень, кожен з яких має свої сильні та слабкі сторони. iCloud ідеально підходить для користувачів Apple, які цінують безперешкодну інтеграцію з іншими сервісами Apple та функції автоматичного резервного копіювання. Хмарне середовище Chrome ідеально підходить для команд і груп, яким потрібні функції співпраці в режимі реального часу та комплексний набір інструментів для підвищення продуктивності. Зрештою, вибір між iCloud та Chrome Cloud Environment залежить від ваших конкретних потреб та вподобань.

Список використаних джерел:

- Бевза В.І., Слатвінська В.М. Вплив збою Crowdstrike на мега-витік паролів: чи є зв'язок? Ч. 1. Вісник Хмельницького національного університету. Серія: Технічні науки. 2024. № 4. С. 332-338 DOI: <https://doi.org/10.31891/2307-5732-2024-339-4-52> URL: (дата звернення: 08.11.2024).

Ключові слова: хмарне сховище, керування паролями, Icloud, Chrome.

Keywords: cloud storage, password management, Icloud, Chrome.

Науковий керівник: доктор філософії, асистент кафедри кібербезпеки Слатвінська В.М.

ПЕРСПЕКТИВИ ТА ВІДКРИТІ ПРОБЛЕМИ ЗАСТОСУВАННЯ ПЕРЕТВОРЕННЯ УОЛША-АДАМАРА ДЛЯ ПОБУДОВИ АЛГОРИТМІВ СТИСКУ ГРАФІЧНОЇ ІНФОРМАЦІЇ

Соколов Артем

професор кафедри кібербезпеки Національного університету «Одеська юридична академія», д.т.н.

Хусід Натан

студент 1 курсу магістратури за спеціальністю «Комп'ютерні науки» Національного університету «Одеська юридична академія»

Методи стиску зображень є ключовим елементом у сучасних системах зберігання та обміну графічною інформацією, який дозволяє забезпечити ефективне застосування каналів передавання інформації, а також простору на накопичувачах.

Сучасні методи стиску інформації можна розділити на два види: з втратами та без втрат (англ. *lossy* та *lossless*, відповідно).

До методів без втрат відносяться такі алгоритми ефективного кодування, як: RLE, код Хаффмана, методи статистичного та арифметичного кодування тощо. На даних ефективних кодах засновані розповсюджені та часто застосовувані на практиці формати зберігання зображень без втрат: PNG, TIFF, BMP, TGA, PCX.

До форматів з втратами відносяться такі алгоритми, як: JPEG, JPEG XL, WebP, JPEG 2000 тощо.

На сьогодні можна констатувати, що методи з втратами є більш часто застосовуваними через їх більшу ефективність в плані забезпечення найбільшого рівня стиску при допустимому рівні надійності сприйняття зображення.

Основною ідеєю, на якій засновано практичні всі алгоритми стиску графічної інформації із втратами, є застосування простору перетворення, який дозволяє розкласти блоки зображення на частотні компоненти та квантування тих частотних компонент, що найменше сприймаються людським зором. Це дозволяє максимізувати рівень стиску зображення при мінімізації видимих спотворень та артефактів на стиснутому зображенні.

Зважаючи на розповсюдженість алгоритму JPEG та не обмежуючи загальності, коротко охарактеризуємо сім основних етапів даного алгоритму [1].

На першому етапі зображення переводиться з простору RGB у простір YCbCr, де Y $\frac{3}{4}$ яскравість зображення, Cb $\frac{3}{4}$ синя кольорорізностна компонента, Cr $\frac{3}{4}$ червона кольорорізностна компонента. Перехід у даний простір

дозволяє забезпечити більший рівень стиску компонент C_b і C_r , які є такими, що сприймаються людським оком менше, ніж компонента Y .

На другому етапі зображення розбивається на матриці 8×8 , що дозволяє забезпечити блокову обробку зображень.

На третьому етапі блоки зображення обробляються дискретним косинусним перетворенням. Цей етап потрібен для розкладання блоків на частотні складові.

На четвертому етапі блоки проходять квантування та округлення отриманого результату, яке дозволяє високочастотним складовим зберігатися з меншою кількістю використовуваної пам'яті.

На п'ятому етапі відбувається зигзагоподібне сканування, яке дозволяє низькочастотним блокам опинитися спочатку послідовності, а високочастотним $\frac{3}{4}$ в кінці.

На шостому етапі блоки зображення проходять стиск алгоритмом RLE, який дозволяє згорнути послідовність однакових чисел (в першу чергу, нулів) у кортежі, де вказано кількість символів в такій послідовності однакових чисел.

На сьомому та останньому етапі використовується кодування інформації за допомогою ефективного коду Хаффмана, який дозволяє стиснути отримані трансформанти дискретного косинусного перетворення.

Суттєвим є питання дослідження якості зображень, що стиснені алгоритмами із втратами. На сьогоднішній день це питання лишається відкритим, через складність математичного опису сприйняття людиною графічної інформації. Одним із класичних підходів до вимірювання якості зображень після їх стиску алгоритмами із втратами є застосування показника PSNR, що характеризує пікове відношення сигналу до шуму, який вноситься алгоритмом стиску. Тим не менш, варто зазначити, що показник PSNR не є вичерпним показником, та не здатен достеменно ідентифікувати видимі спотворення у зображенні.

На сьогоднішній день, через значну актуальність питання підвищення ефективності алгоритмів стиску графічної інформації, чимало вчених роблять спроби підвищення ефективності наявних алгоритмів із застосуванням різноманітних математичних конструкцій із метою забезпечення найнижчих показників PSNR при найбільшій ефективності стиску зображення. При цьому важливим є також забезпечення найвищої обчислювальної ефективності, адже алгоритми стиску застосовуються на різноманітних, у тому числі, на ресурсообмежених пристроях.

Однією з таких ідей стала публікація роботи «Застосування нееквівалентних класів матриць Адамара для стиску зображень за допомогою алгоритма JPEG» [2]. Стаття пропонує на третьому етапі замість дискретного ко-

синусного перетворення використовувати перетворення Уолша-Адамара, що, як показують попередні дослідження, дозволяє підвищити ефективність алгоритму стиску з втратами, а також забезпечити зниження обчислювальної складності через природу перетворення Уолша-Адамара, яке містить лише цілочисельні коефіцієнти та є більш відповідним принципам, на яких заснована сучасна обчислювальна техніка.

Перетворення Уолша-Адамара задається як добуток вектора на матрицю Адамара

$$W = TH_N, \quad (1)$$

де T – вектор-рядок, який складається з N координат, в той час як матриця Уолша-Адамара H_N порядку N може бути сформована у відповідності до конструкції Сильвестра

$$H_N = \begin{bmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{bmatrix}, H_1 = 1. \quad (2)$$

В роботі [2] вивчено ефективність різних видів перетворень Уолша-Адамара порядків $N=4,8,16$ при їх застосуванні в алгоритмі JPEG, що дозволило зробити висновок, що дискретне косинусне перетворення володіє більшою ефективністю, ніж класичне перетворення Уолша-Адамара порядку $N=2^k$ для $k=2,3,4$ і, найімовірніше, інших значень k .

Тим не менш відомо, що крім матриць Уолша-Адамара порядку $N=2^k$ існують матриці Уолша-Адамара порядку $N=20,24,28$, й так далі. В статті [2] вивчено можливість застосування матриці Уолша-Адамара порядку $N=24$ з конструкцією Пелі в алгоритмі JPEG. Така комбінація показала кращі результати у порівнянні з дискретним косинусним перетворенням. Проведені дослідження дозволяють показати, що при стиску зображення в п'ятнадцять разів, ми спостерігаємо достатній рівень деталізації та якості.

На основі цих даних можна зробити висновок про великий потенціал у застосуванні матриць Уолша-Адамара для стиску зображень з втратами. Однак, для більшого застосування на практиці повинні бути досліджені наступні аспекти.

1. Результати досліджень повинні бути верифіковані на більшій кількості зображень.

2. Інші раніше згадані етапи алгоритму стиску із втратами JPEG можуть бути удосконаленими з урахуванням застосування перетворення Уолша-Адамара.

3. Дослідження ще шестидесяти [3] конструкцій матриць Уолша-Адамара порядку $N=24$ можуть значно покращити ефективність алгоритму JPEG.

4. Дослідження ряду інших порядків $N=20,28,\dots$ матриць Уолша-Адамара можуть значно покращити ефективність алгоритму JPEG.

5. Оцінка швидкодії алгоритму JPEG на основі дискретного косинусного перетворення та на основі перетворення Уолша-Адамара.

Таким чином у даній роботі розглянуто сучасні напрямки розробки алгоритмів стиску графічної інформації з втратами на основі застосування перетворення Уолша-Адамара, виокремлено основні відкриті проблеми та подальші напрямки проведення досліджень.

Список використаних джерел:

1. Verma N., Mann P. Survey on JPEG Image Compression. Int. J. Adv. Res. Comput. Sci. Softw. Eng. 2014. No. 4. P.1072–1075.
2. Соколов А. В., Авекин В.В. Застосування нееквівалентних класів матриці Адамара для стиску зображень за допомогою алгоритма JPEG. Інформаційні технології в освіті, науці та підприємстві . 2017. С. 1-8.
3. A Library of Hadamard Matrices. Огляд: <http://neilsloane.com/hadamard/>

Ключові слова: алгоритм стиску з втратами, JPEG, перетворення Уолша-Адамара.

Keywords: lossy compression algorithm, JPEG, Walsh-Hadamard transform.

АНАЛІЗ ВРАЗЛИВОСТЕЙ КОРПОРАТИВНОЇ МЕРЕЖІ В УМОВАХ НЕСАНКЦІОНОВАНОГО ФІЗИЧНОГО ДОСТУПУ

Іващук Даніель

студент 1 курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасні корпоративні мережі є складними системами, що потребують багаторівневого захисту для забезпечення безпеки даних. Однією з головних загроз для закритих корпоративних мереж є несанкціонований доступ за допомогою вбудованих пристроїв та використання інструментів для прихованого проникнення. У цій роботі розглядається сценарій, в якому був використаний одноплатний комп'ютер із доступом до GSM-мережі та локальної мережі підприємства для подолання периметрової безпеки та організації несанкціонованого доступу до закритої мережі підприємства. В подальшому, за допомогою шкідливого програмного забезпечення, було захоплено кілька комп'ютерів і вивантажено значний обсяг конфіденційної інформації.

1. Опис корпоративної мережі

Корпоративна мережа сучасного підприємства часто містить кілька рівнів захисту, які охоплюють як фізичні, так і програмні засоби. Закриті мережі підприємств, що не мають прямого доступу до Інтернету, зазвичай використовуються для зберігання та обробки критично важливих даних, таких як оборонна промисловість, документи громадян країни та інші види конфіденційної інформації.

2. Використання одноплатного комп'ютера

В даному випадку, основним вектором атаки став одноплатний комп'ютер, обладнаний GSM-модемом та мережею Ethernet, підключений до корпоративного комутатора.

GSM-модуль: забезпечив доступ до зовнішнього Інтернету через мобільний зв'язок, що дозволило уникнути контролю та моніторингу мережевими інструментами підприємства. Ethernet-підключення: дозволило інтегруватися в локальну мережу підприємства, забезпечивши доступ до внутрішньої інфраструктури.

3. Використання тунелювання

Завдяки тунелюванню зломисник отримав доступ до локальної мережі, залишаючись непоміченим мережевими інструментами безпеки. Це обійшло політики безпеки підприємства, оскільки мережевий трафік йшов через локальну мережу, що виглядало як легітимний трафік для мережових моніторингових систем [1].

4. Захоплення комп'ютерів та витік інформації

Після встановлення зв'язку з внутрішньою мережею підприємства через тунель, наступним кроком стало проникнення в комп'ютерні системи співробітників. Було використано самописне шкідливе програмне забезпечення для проведення наступних операцій:

- Сканування мережі: для виявлення активних пристроїв і визначення потенційних цілей атаки;
- Використання експлойтів: для отримання привілейованого доступу до кількох комп'ютерів у мережі;
- Ескалація привілеїв: після початкового компрометування систем, було отримано права адміністратора для подальшого розширення доступу.

У підсумку, зломисники змогли отримати контроль над кількома робочими станціями, з яких було вивантажено значний обсяг конфіденційної інформації. Зокрема, гігабайт закритих даних, що стосувалися діяльності підприємства, які потім були передані через тунель.

5. Аналіз уразливостей та заходи захисту

Основною причиною успішної атаки стало використання фізичного доступу до мережевої інфраструктури підприємства. Хоча в мережі були налаштовані базові заходи захисту, таких як VLAN та брандмауери, понижений контроль локальної мережі та відсутність оновлення програмного забезпечення призвело до експлуатування вразливостей на комп'ютерах [2].

Для запобігання подібним атакам можуть бути впроваджені наступні заходи:

- Контроль фізичного доступу: обмеження фізичного доступу до мережевого обладнання для сторонніх осіб;

- Моніторинг підключень: використання систем моніторингу для виявлення підозрілих підключень до мережевої інфраструктури;
- Автоматичний аналіз трафіку: налаштування систем IDS, IPS, SIEM для виявлення аномалій мережевої активності;
- Сегментація мережі: подальша сегментація мережі для мінімізації можливих векторів атак [3].

Висновок

Інцидент показав важливість комплексного підходу до забезпечення безпеки корпоративних мереж. Для запобігання подібним інцидентам необхідно вдосконалювати як фізичний, так і програмний захист. Також потрібно регулярно проводити аудит безпеки та оцінку ризиків для підвищення загального рівня кібербезпеки.

Список використаних джерел:

1. Hill, J. (2000, March). Bypassing firewalls: tools and techniques. In *12th Annual FIRST conference*. URL https://www.academia.edu/download/32169447/Bypassing_Firewalls_Tools_and_Techniques.pdf (дата звернення: 23.10.2024).
2. KUMAR, Anand. DATA SECURITY IN LOCAL NETWORK USING DISTRIBUTED FIREWALL. 2008. URL - <https://www.academia.edu/download/109041769/38139563-Data-Security-in-Local-Network-Using-Distributed-Firewall.pdf> (дата звернення: 23.10.2024).
3. Mhaskar, N., Alabbad, M., & Khedri, R. (2021). A formal approach to network segmentation. *Computers & Security*, 103, 102162. URL https://www.researchgate.net/profile/Neeraj-Mhaskar/publication/348333249_A_Formal_Approach_to_Network_Segmentation/links/6047898a299bf1e07867b8b3/A-Formal-Approach-to-Network-Segmentation.pdf (дата звернення: 23.10.2024).

Ключові слова: ids, cyib, брандмауер, витік інформації, порушення кібербезпеки

Keywords: ids, siem, firewall, information leak, cybersecurity breach

Науковий керівник: к.т.н., доцент **Задерейко Олександр**

ТЕОРЕТИЧНІ ЗАСАДИ ЗНАХОДЖЕННЯ ПРИХОВАНОГО КАНАЛУ ЗВ'ЯЗКУ В ОБЛАСТІ ПЕРЕТВОРЕНЬ УОЛША-АДАМАРА

Соколов Артем

професор кафедри кібербезпеки Національного університету

«Одеська юридична академія», д.т.н.

Лановська Олександра

студентка магістратури Національного університету «Одеська політехніка»

На сьогодні відбувається сталий розвиток інформаційних технологій, що призвів до збільшення кількості мультимедійного контенту у світовому трафіку і, відповідно, до актуалізації питань застосування стеганографічних

методів захисту інформації, які дозволяють приховати сам факт наявності інформації, що захищається. З'являються нові та вдосконалюються існуючі стеганографічні методи, що здатні працювати як у просторовій області, так і в області перетворень контейнера. Одним з перспективних стеганографічних методів, що працює в просторовій області, забезпечуючи високу обчислювальну ефективність при стійкості до атак проти вбудованого повідомлення, високій надійності сприйняття стеганоповідомлення, достатній пропускній спроможності, є стеганографічний метод з кодовим управлінням вбудовуванням додаткової інформації [1].

Втім, бурхливий розвиток стеганографії актуалізує питання розробки методів стеганоаналізу, які були б здатні на виявлення прихованих каналів передавання інформації. Такі методи для виявлення прихованих каналів зв'язку, створених на основі стеганографічного методу з кодовим управлінням на сьогодні відсутні у відкритих джерелах.

У даній роботі представлено теоретичні засади, які є основою для стеганоаналізу стеганографічного методу з кодовим управлінням.

Метою цієї роботи є формування теоретичного базису виявлення прихованого каналу зв'язку з кодовим управлінням, що є основою для подальшої розробки методу стеганоаналізу на основі перетворень Уолша-Адамара.

Кодові слова, що використовуються у даному методі для попереднього кодування додаткової інформації, представляють собою матричне уявлення рядків матриці Уолша-Адамара порядку N^2 і впливають на конкретну трансформанту перетворення.

Визначимо необхідне нам для подальших досліджень двовимірне дискретне перетворення Уолша-Адамара матриці X розміру $N \times N$

$$W = H'_N X H_N^T, \quad (1)$$

де $H'_N = \frac{1}{\sqrt{N}} H_N$ — нормована матриця Уолша-Адамара, що побудована у відповідності до конструкції Сильвестра [2].

Для проведення досліджень було створено вибірку з 530 зображень у форматі TIFF з бази NRCS, а також додаткові вибірки, основні з яких — зображення із вбудованою інформацією, з використанням бінарних кодових слів [3], що впливають на трансформанти перетворення Уолша-Адамара (5,1), (5,5), (1,5). Вбудовування відбувалося у червоний канал, при задіянні 100% блоків.

Для визначення критеріїв, придатних для виявлення втручання, було проведено аналіз значень трансформант перетворення Уолша-Адамара для стеганоповідомлень та оригінальних контейнерів, що визначаються (1). Амплітуда числових значень збурених трансформант залишалася в межах амплітуди відповідних значень для оригінальних зображень. Проте, було знай-

дено певну залежність у межах блоків розміру 8×8 . Дану залежність визначимо як

$$U_{orig}(k, l, c) < U_{seg}(k, l, c), \quad (2)$$

де c — кольоровий канал, а $U_{orig}(k, l, c)$ та $U_{seg}(k, l, c)$, у свою чергу, визначаються як

$$\begin{aligned} U_{orig}(k, l, c) &= p\{|W_{orig}(k, l, c)| = \max_{i,j} \{|W_{orig}(i, j, c)|\}\}; \\ U_{seg}(k, l, c) &= p\{|W_{seg}(k, l, c)| = \max_{i,j} \{|W_{seg}(i, j, c)|\}\}; \\ i, j &= 1, 2, \dots, N; (i, j, c) \neq (1, 1, c). \end{aligned} \quad (3)$$

де W_{orig} та W_{seg} — матриці модулів трансформант перетворення Уолша-Адамара для оригінального та стеганозображення, відповідно, $p\{|W(k, l, c)| = \max_{i,j} \{|W(i, j, c)|\}\}$ — ймовірність події, що полягає у тому, що відповідне значення $W(k, l, c)$ є максимальним у межах блоку для заданого кольорового каналу c .

Складова (1,1) не враховується, оскільки відомо, що вона є постійною і завжди приймає значення відчутно більше за інші трансформанти.

Для визначення частоти виникнення максимумів за індексом використовується наступна формула

$$\begin{aligned} M(i, j, c) &= \frac{1}{N} \sum_{k=1}^N \delta\left((i, j, c), \max_{i_{max}, j_{max}, c} W_k(i_{max}, j_{max}, c)\right), \\ (i, j) &\neq (1, 1, c), (i_{max}, j_{max}, c) \neq (1, 1, c), \end{aligned} \quad (4)$$

де N — кількість блоків у зображенні,

c — кольоровий канал,

k — номер блоку, що аналізується,

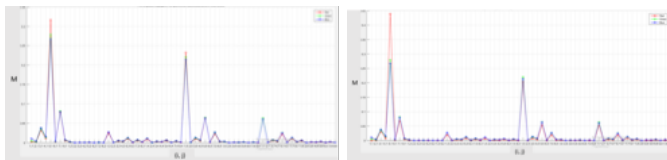
W_k — матриця трансформант Уолша-Адамара зображення для k -го блока,

δ — дельта Кронекера, що приймає наступні значення:

$$\delta((i, j, c), (i_{max}, j_{max}, c)) = \begin{cases} 1 & (i, j, c) = (i_{max}, j_{max}, c) \\ 0 & (i, j, c) \neq (i_{max}, j_{max}, c) \end{cases} \quad (5)$$

Далі обраховується середній результат для усіх зображень у множині.

На рис. 1 зображено графіки середніх значень частоти виникнення максимумів у блоці для множини ориганільних зображень (а), та підмножин, що зазнали впливу стеганографічного методу із кодовим управлінням із використанням наступних кодових слів: (5,1) (б), (5,5) (в), (1,5) (г).



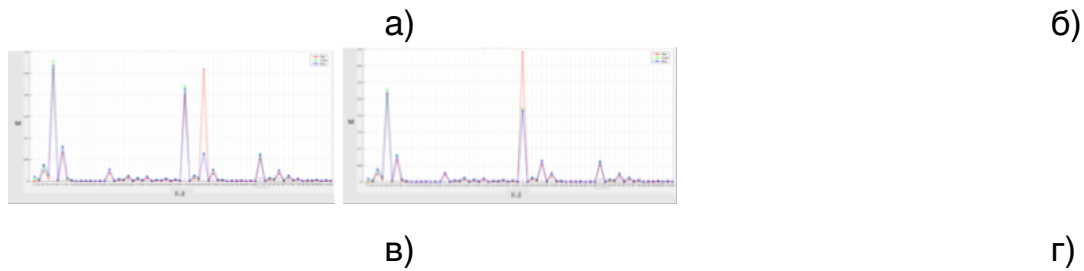


Рисунок 1 — Графік частоти місцеположення максимального значення за індексом для зображень

Із наведених вище графіків частот розташування максимальних значень за індексами для оригінальних зображень та зображень із вбудованою додатковою інформацією можна визначити наступні особливості:

¾ характерний стрибок значення $U_{neg}(k, l, c)$ у збурених множинах саме в тій позиції k, l , на яку впливає кодове слово. Стрибок значно перевищує значення, що були зафіксовані під час аналізу оригінальних зображень;

¾ даний стрибок $U_{neg}(k, l, c)$ значною мірою перевищує значення $U_{orig}(k, l, c)$ в інших кольорових каналах c ;

¾ частота появи максимумів $M(i, j, c)$ за іншими індексами блоку i, j , крім тих, які зазнали впливу кодового слова, у збурених множинах переважно зменшується.

Таким чином можна виділити 3 основні засади, на які можна орієнтуватися в області Уолша-Адамара для виявлення прихованого каналу зв'язку із кодовим управлінням: порогові значення для кожного індексу, збільшення значення одного кольорового каналу у порівнянні з іншими за одним індексом, зменшення значення одного кольорового каналу у порівнянні з іншими за кількома індексами.

В результаті було сформовано три критерії для стеганоаналізу. Матрицю порогових значень було визначено за формулою (4), аналізуючи множину оригінальних зображень, після чого відкориговано експериментально для індексів трансформант, що відповідають кодам (5,1), (5,5), (1,5):

1. Для індексів (5,1), (5,5) та (1,5) встановлено порогові значення $M(i, j, c)$ як: 0,3; 0,06 та 0,25, відповідно. Ця умова застосовується для уникнення хибнонегативних результатів.

2. Значення $M(i, j, c)$ досліджуваного кольорового каналу c повинно відрізнятися від значень інших каналів щонайменше на 0,02 (експерименти з більшими та меншими значеннями дали менш задовільні результати). Ця умова введена для зниження ймовірності хибнонегативних результатів.

3. Усі значення $M(i,j,c)$ кольорового каналу, окрім аналізованого, повинні бути меншими за відповідні значення в інших каналах не менше ніж у 40% випадків (експерименти з вищими та нижчими відсотками показали менш задовільні результати). Ця умова введена для зменшення ймовірності хибно-позитивних результатів.

Таким чином, виконання усіх трьох критеріїв необхідно для визначення зображення таким, яке зазнало впливу стеганографічного методу із кодовим управлінням. Це дозволяє визначити конкретний канал, куди була вбудована інформація, та трансформанту, на яку було здійснено вплив (а значить, що і використане кодове слово).

Літературні джерела:

1. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. Problemele energeticii regionale. 2021. No. 4 (52). P. 115-130.
2. Horadam K. J. Hadamard matrices and their applications. Princeton university press, 2012. 280 p.
3. Kobozeva A.A., Sokolov A.V. Theoretical foundations for constructing effective codewords for the code-controlled information embedding steganographic method. Radiotekhnika. 2021. 4(207). P. 27–39.

Ключові слова: стеганоаналіз, кодове управління, перетворення Уолша-Адамара.

Keywords: steganoanalysis, code control, Walsh-Hadamard transform.

АВТОМАТИЗАЦІЯ ТЕСТУВАННЯ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Максимович Максим

*аспірант кафедри безпеки інформаційних технологій
Національного університету «Львівська політехніка»*

Вступ. У сучасному цифровому середовищі програмне забезпечення стало невід'ємною частиною життя, проникаючи в усі сфери — від комунікацій і розваг до бізнесу й освіти. Стрімкий розвиток програмного забезпечення та інтеграція його практично в усі сфери життя зумовлює потребу не тільки в його надійності та доступності, але й в безпечності [1]. Із розвитком технологій швидко змінюються й методи кібератак, змушуючи розробників інвестувати ресурси не лише в основний функціонал, але й у безпеку програмного забезпечення, що є нелегким завданням, оскільки потребує від розробників експертизи не тільки в області розробки, але й в області безпеки. Відсутність належного рівня захисту може призвести до значних фінансових втрат, втрати довіри користувачів та компрометації конфіденційної інформації, що

підкреслює важливість інтеграції заходів кібербезпеки на всіх етапах життєвого циклу розробки.

Аналіз сучасних методів вирішення задачі. Одним із ефективних підходів для цього є впровадження автоматизованого тестування безпеки в життєвий цикл розробки програмного забезпечення, яке допомагає виявляти вразливості на етапі розробки. На сьогоднішній день існують 4 основні методи тестування безпеки (рис. 1), а саме: інтерактивне тестування, динамічне тестування, статичний та композитний аналізи. Кожен із цих методів має свої переваги та недоліки, а їхнє комбіноване використання дозволяє забезпечити більш комплексний підхід до виявлення та усунення потенційних загроз у програмному забезпеченні.



Рис. 1 Методи тестування безпеки програмного забезпечення

Динамічне тестування безпеки (dynamic application security testing, DAST) - це метод перевірки безпеки, який аналізує веб-додатки або API під час їхнього виконання, виявляючи потенційні вразливості [2]. Він дозволяє імітувати дії злоумисника в реальному середовищі, щоб знайти потенційні загрози на рівні інтерфейсу користувача

Статичне тестування безпеки (static application security testing, SAST) - це метод тестування безпеки, який аналізує вихідний код додатка на наявність вразливостей без запуску програми [3]. Воно дозволяє виявляти потенційні загрози на ранніх етапах розробки, що сприяє економії ресурсів і зменшенню ризиків безпеки в кінцевому продукті.

Інтерактивне тестування безпеки (interactive application security testing, IAST) - це метод тестування безпеки, який аналізує додаток під час його виконання, поєднуючи підходи статичного й динамічного тестування [4]. IAST дозволяє виявляти вразливості в реальному часі та з високою точністю, забезпечуючи глибоке розуміння безпеки програми безпосередньо під час роботи в тестовому середовищі.

Композитний аналіз (software composition analysis, SCA) - використовується для виявлення вразливостей у відкритих бібліотеках і компонентах, що використовуються в програмному забезпеченні. Цей процес дозволяє ідентифікувати потенційні загрози та безпекові недоліки у сторонніх бібліотеках, які можуть бути вразливими до атак, забезпечуючи тим самим захист основних додатків від використання небезпечного коду.

Впровадження даних методів тестування в життєвий цикл розробки програмного забезпечення зможе суттєво підвищити рівень стійкості програмного продукту до найбільш популярних кібератак за версією OWASP TOP-10 [5], що свою чергу забезпечить можливість безпечного використання даного продукту кінцевим користувачем та збереженням 3 основних принципів безпеки, таких як: цілісність, доступність та конфіденційність.

Висновки. В сучасному світі, де програмне забезпечення активно використовується практично в кожній сфері діяльності, підтримка належного рівня його безпеки стає критичною. Впровадження автоматизованих методів забезпечення стійкості програмного забезпечення до кібератак має бути невід'ємним елементом життєвого циклу розробки, що в свою чергу підвищить імовірність збереження основних принципів безпеки при використанні програмного продукту.

Список літератури:

1. Aljabri, M., Aldossary, M., Al-Homeed, N., Alhetelah, B., Althubiany, M., Alotaibi, O., & Alsaqer, S. (2022). Testing and Exploiting Tools to Improve OWASP Top Ten Security Vulnerabilities Detection. 797–803. Scopus. <https://doi.org/10.1109/CICN56167.2022.10008360>
2. Singh, R., Kumar Gupta, M., Patil, D. R., & Maruti Patil, S. (2024). Analysis of Web Application Vulnerabilities using Dynamic Application Security Testing. 2024 IEEE 9th International Conference for Convergence in Technology, I2CT 2024. Scopus. <https://doi.org/10.1109/I2CT61223.2024.10543484>
3. Yang, J., Tan, L., Peyton, J., & A Duer, K. (2019). Towards Better Utilizing Static Application Security Testing. 51–60. Scopus. <https://doi.org/10.1109/ICSE-SEIP.2019.00014>
4. Pan, Y. (2019). Interactive Application Security Testing. 2019 International Conference on Smart Grid and Electrical Automation (ICSGEA). <https://doi.org/10.1109/ICSGEA.2019.00131>
5. Fredj, O. B., Cheikhrouhou, O., Krichen, M., Hamam, H., & Derhab, A. (2021). An OWASP Top Ten Driven Survey on Web Application Protection Methods. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 12528 LNCS, 235–252. Scopus. https://doi.org/10.1007/978-3-030-68887-5_14

Ключові слова: програмне забезпечення, кібербезпека, автоматизація, тестування, захист інформації, забезпечення безпеки.

Keywords: software, cyber security, automation, testing, information security, security assurance.

BYOD (BRING YOUR OWN DEVICE) RISK: A GROWING CONCERN IN CONFLICT ZONES – UKRAINE'S CASE

Олена Зоз

студентка 1 курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

The rise of Bring Your Own Device (BYOD) practices, where employees use personal devices to access work-related systems and data, has revolutionized workplace flexibility. However, it introduces significant cybersecurity risks. This challenge becomes particularly acute in high-stress environments, such as conflict zones. Ukraine, amid its ongoing war with Russia, heavily relies on remote work in various sectors, including government and military, making BYOD-related vulnerabilities a critical issue.

The BYOD Landscape: Risks and Benefits

BYOD offers several advantages, such as increased flexibility, employee satisfaction, and reduced hardware costs for organizations. However, it comes with a range of cybersecurity risks:

- **Data Breaches:** Personal devices are often less secure than corporate devices. A 2023 survey revealed that more than half of organizations encountered data breaches due to unsecured personal devices.

Personal devices may lack sufficient encryption, antivirus software, and firewalls, making them easy targets for attackers.

- **Uncontrolled Access to Sensitive Data:** When personal devices are used for work, employees might access sensitive data without the same level of scrutiny as corporate-issued devices. In conflict zones like Ukraine, this could lead to leakage of classified government or military information, potentially undermining national security.

- **Insecure Networks:** Remote work during the conflict has led to employees accessing sensitive systems from personal networks, which may not be secure. Using unprotected Wi-Fi networks heightens the risk of interception, especially by state-sponsored actors.

BYOD Risks in High-Stress Environments

In high-stress environments like Ukraine, where employees are operating under significant physical and psychological pressure, the ability to enforce cybersecurity policies weakens. Organizations may experience:

- **Lack of Oversight:** Employees in conflict zones may prioritize safety over following security protocols. In the chaos of war, using a work device might be impractical or impossible, pushing individuals to rely on personal devices.

- **Increased Cyberthreats:** The war in Ukraine has brought an onslaught of cyberattacks from Russia, including those targeting remote workers and unsecured devices. Ukrainian sectors, including military, logistics, and healthcare, have seen a surge in ransomware, phishing, and espionage attacks.

The Ukrainian Context

Since the onset of the war, many Ukrainian employees in key sectors, including government and military, have shifted to remote work. This has resulted in the pervasive utilisation of personal devices, notwithstanding the formal organisational policies that discourage such practices. BYOD vulnerabilities in Ukraine include:

1. **Weak Endpoint Security:** Personal devices may not have robust security measures like regular patch updates, firewalls, or multi-factor authentication, exposing them to malware attacks. Attackers can exploit these devices to gain access to sensitive networks, including government databases.

2. **Lack of Encryption:** Many personal devices lack adequate encryption, especially when employees use cloud services or file-sharing applications to transfer sensitive data. Unencrypted devices are easily compromised in phishing attacks or through physical theft.

3. **Insecure Communication Channels:** Many personal devices use unsecured messaging apps, social media platforms, or email services to communicate sensitive information. This introduces multiple entry points for attackers to intercept or manipulate communications.

Addressing BYOD Risk: Strategies for Ukraine

To mitigate BYOD risks, Ukraine can adopt several strategies:

1. **Improved Endpoint Management:** Implementing Mobile Device Management (MDM) systems ensures that personal devices accessing work-related data comply with security policies. Such solutions permit organisations to remotely administer, supervise and, in the event of misplacement or theft, erase data from personal devices.

2. **Zero-Trust Architecture:** By employing zero-trust security frameworks, organizations can restrict access to only trusted devices, regardless of whether they are personal or corporate. Each access request is treated as a potential threat, ensuring continuous authentication and encryption.

3. **Employee Training:** A critical element in addressing BYOD risks is educating employees about the dangers of using unsecured personal devices, especially in conflict zones. They should be trained to recognize phishing attempts, secure their devices, and use encrypted communications channels.

4. **Securing Remote Workspaces:** Personal devices in Ukraine should be required to use virtual private networks (VPNs) and two-factor authentication to

access work-related data. This can prevent unauthorized interception and reduce exposure to cyberattacks.

5. Cybersecurity Awareness Campaigns: With the rise of politically motivated cyberattacks, Ukraine could benefit from public awareness campaigns emphasizing the importance of securing personal devices and following best cybersecurity practices in remote work scenarios.

Conclusion

In the ongoing conflict, Ukraine's reliance on remote work and BYOD practices has exposed significant cybersecurity vulnerabilities. While BYOD increases flexibility, it comes with the risk of data breaches, insecure communications, and endpoint vulnerabilities. For Ukraine, protecting its sensitive data from state-sponsored cyberattacks requires the adoption of advanced endpoint management tools, improved security protocols, and continued training of employees to handle the unique risks posed by personal devices in conflict zones.

References

1. Ivanti. (2023). Everywhere Work. Elevated.
2. Orange Cyberdefense. (2023). Security Navigator 2024: Cyber Extortion and Hacktivism).
3. Ponemon Institute. (2023). The Impact of Bring Your Own Device (BYOD) on Cybersecurity: A Global Survey.
4. Gartner. (2024). The Future of BYOD and Mobile Security in High-Stress Environments.

Key words: BYOD, cybersecurity, MDM systems, cyberattacks, personal devices

Ключові слова: BYOD, кібербезпека, системи MDM, кібератаки, персональні пристрої

Науковий керівник: *к.т.н., доцент Задерейко Олександр*

СИСТЕМА АВТОМАТИЧНОГО ЗБОРУ ДАНИХ НА ОСНОВІ ЗАПИТІВ МОБІЛЬНИХ ПРИСТРОЇВ

Оліярчук Тарас

магістр кафедри Безпеки інформаційних технологій Національний університет «Львівська Політехніка»,

В світі розвиток технологій бездротового зв'язку і мобільних пристроїв набуває дедалі більшого значення, забезпечуючи зручність і доступність комунікацій у різних сферах життя. Однак, поряд із зручностями, зростає й ризик несанкціонованого доступу до особистої інформації та відстежування місцезнаходження користувачів. На основі проведеного аналізу представлено огляд інструментів і методик, що використовуються для відстежування та аналізу бездротових мереж. Серед них розглянуті такі інструменти як Aircrack-ng, tcpdump, Tshark, MDK3, SSH [1-4], а також система керування ба-

зами даних MongoDB. Предметом дослідження є методи сканування у стандарті 802.11 [5] для бездротових мереж Wi-Fi. Це включає активні й пасивні методи, процедури пошуку та встановлення зв'язку, оцінку ефективності алгоритмів сканування та заходи безпеки для нейтралізації загроз.

Можливості та ризики wifi та bluetooth трекінгу. У сучасному світі, де технології відіграють ключову роль у нашому повсякденному житті, використання Wi-Fi та Bluetooth для трекінгу набуває все більшого значення. Ці технології дозволяють не лише забезпечувати зручний доступ до Інтернету та передачу даних, але й слугують ефективними інструментами для визначення місцезнаходження пристроїв та користувачів. Це відкриває нові можливості для бізнесу, забезпечує безпеку та підвищує комфорт користувачів, але також створює ризики зловживання та порушення приватності.

Wi-Fi трекінг базується на виявленні пристроїв через їхні запити до Wi-Fi мереж. Коли пристрій намагається підключитися до Wi-Fi точки доступу, він відправляє запити, які можуть бути перехоплені і використані для визначення його місцезнаходження. Ці запити містять інформацію про мережі, до яких пристрій підключався раніше, що дозволяє визначити його попередні місця перебування. Технологія Wi-Fi триангуляції використовує сигнали від кількох відомих точок доступу для обчислення відстані до них та визначення точної позиції пристрою. Цей метод менш точний, ніж GPS, але є незамінним у закритих приміщеннях, де сигнали супутників недоступні або слабкі.

Стандарт 802.11, розроблений Інститутом інженерів з електротехніки та електроніки (IEEE), є основою для Wi-Fi локальних мереж (WLAN). Він задає набір специфікацій для бездротового зв'язку, який забезпечує обмін даними між пристроями через радіоканали. Цей стандарт визначає протоколи передачі даних, методи шифрування та механізми аутентифікації, що забезпечують надійну та безпечну комунікацію в бездротових мережах. Сканування є важливим процесом у стандарті IEEE 802.11, який дозволяє бездротовим пристроям виявляти доступні мережі та вибирати найбільш відповідну для підключення. Існують два основних типи сканування: активне та пасивне. Кожен з цих методів має свої особливості та використовується в різних ситуаціях для забезпечення оптимальної роботи бездротових мереж.

У стандарті IEEE 802.11 Probe Request є спеціальним типом керуючого фрейму, який використовується бездротовими станціями (STA) для активного сканування мереж. Цей запит надсилається для виявлення доступних точок доступу (AP) та збору інформації про наявні бездротові мережі. Процес активного сканування з використанням Probe Request є важливим для швидкого і ефективного встановлення з'єднань у бездротових мережах. Probe Response є ключовим типом керуючого фрейму у стандарті IEEE 802.11, який використовується точками доступу (AP) для відповіді на запити Probe

Request, що надходять від бездротових станцій (STA) під час активного сканування мереж. Цей фрейм містить всю необхідну інформацію про мережу, яка дозволяє станції прийняти рішення щодо підключення.

Перехоплення та аналіз Probe Request у бездротових мережах є ключовим аспектом для розуміння поведінки клієнтських пристроїв та оптимізації мережевої безпеки. Ми розглянули процес перехоплення Probe Request, використовуючи інструменти `airmon-ng`, `tcpdump` та `tshark`, а також збереження отриманих даних у базі даних MongoDB. Цей процес включає переведення мережевого адаптера у режим моніторингу, перехоплення та фільтрацію фреймів, аналіз отриманих даних і збереження їх у базі даних.

Отже, розглянуто актуальну проблему захисту особистих даних у бездротових мережах, зокрема в контексті відстеження місцезнаходження мобільних пристроїв. Використання Wi-Fi для трекінгу, хоча й має значний потенціал для бізнесу та забезпечення безпеки, створює ризики порушення приватності користувачів. Проведений аналіз інструментів для перехоплення і обробки мережевих запитів підкреслює важливість активного та пасивного сканування в якості ключових елементів у виявленні та моніторингу пристроїв у стандарті 802.11. Використання інструментів, таких як `Aircrack-ng`, `tcpdump`, та MongoDB для збору й обробки даних, продемонструвало виклики в забезпеченні мережевої безпеки з точки зору приватності. Зокрема, перехоплення Probe Request у режимі моніторингу дозволило глибше зрозуміти поведінку клієнтських пристроїв. Це дослідження відкриває перспективи для подальших робіт у сфері забезпечення конфіденційності користувачів та створення безпечних систем автоматичного збору даних.

Список використаних джерел:

1. Опис Aircrack-ng. URL: <https://www.aircrack-ng.org> (дата звернення 02.11.2021).
2. Опис Tcpdump. URL: <https://www.tcpdump.org> (дата звернення 02.11.2021).
3. Опис Tshark. URL: <https://www.wireshark.org/docs/man-pages/tshark.html> (дата звернення 02.11.2021).
4. Опис MDK3. URL: <https://tools.kali.org/wireless-attacks/mdk3> (дата звернення 02.11.2021).
5. Опис стандарту 802.11. URL: <https://www.ieee802.org/11> (дата звернення 02.11.2021).

Ключові слова: система автоматичного збору даних, мобільні пристрої, відстежування місцезнаходження, метод сканування, режим моніторингу.

Keywords: automatic data collection system, mobile devices, location tracking, scanning method, monitoring mode.

ЗАХИСТ KUBERNETES ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО СЕКРЕТНИХ ДАНИХ ЗА ДОПОМОГОЮ ШИФРУВАННЯ

Дарієнко Дмитро

*аспірант кафедри захисту інформації Національного університету
«Львівська політехніка»*

Kubernetes, який став провідною системою оркестрації контейнерів, тепер лежить в основі величезного спектру критично важливої інфраструктури та додатків у всьому світі [1]. Його здатність оптимізувати процеси розгортання, сприяти масштабованості та оптимізувати використання ресурсів зробила його незамінним у сучасній парадигмі розробки та експлуатації програмного забезпечення. Однак це широке впровадження одночасно розширило поверхню атак, створюючи нові та складні виклики безпеці.

Kubernetes — це платформа оркестрації з відкритим вихідним кодом, розроблена для автоматизації життєвого циклу контейнеризованих додатків у розподілених обчислювальних середовищах. Ця автоматизація охоплює розгортання, масштабування та оперативне управління контейнерами. Для підтримання та управління станом кластера використовують сховище ключів-значень etcd [2].

Назва "etcd" походить від угоди про іменування Unix, де файли конфігурації системи для однієї системи зберігаються в папці під назвою "/etc". Буква «d» в etcd розшифровується як «розподілений», так як служить сховищем розподіленої конфігурації. Якщо сторонні особи отримають доступ до etcd, вони можуть захопити контроль над усім кластером. Ризик доступу до читання також значний, оскільки зломисники можуть використовувати його для отримання підвищених привілеїв. Шифрування сховища etcd здатне підвищити рівень захищеності кластера від подібних загроз. Ця функція не активована за замовчуванням, і ми можемо увімкнути її за допомогою процесу kube-apiserver, вказавши аргумент "`--encryption-provider-config=$ {path_to_encryption-config}`". Де `path_to_encryption-config` — шлях до файлу конфігурації шифрування ресурсів в Kubernetes у форматі `yaml`. Цей файл мусить містити `EncryptionConfiguration`, де прописується тип ресурсу і його шифрування. За замовчуванням для кожного ресурсу встановлено параметр `identity`. Цей параметр означає повну відсутність шифрування. А отже зломисник зможе отримати повний доступ до даних певного ресурсу. Тому підтримуються наступні системи шифрувань: AES-CBC, AES-GCM, XSalsa20 та Poly1305.

Один з найкращих варіантів — це використання сервісу управління ключами (kms), що містять в собі AES-GCM ключ. В такому разі розробник не матиме необхідності вказувати ключі в файлі конфігурацій напрямку, а лише по-

силання на них. Також EncryptionConfiguration дає можливість налаштовувати шифрування для окремих типів ресурсів. Таким чином, наприклад, secrets та configmaps можуть мати різний тип шифрування, що дає можливість покращити продуктивність без значних втрат захищеності інфраструктури.

Окремо налаштувань конфігурацій не достатньо. Якщо зловмисник отримає доступ до налаштувань шифрування, він зможе за допомогою підміни ключів доступу обрвати повний доступ до всіх даних в кластері. Тому варто ізолювати доступ з мережі до головного вузла (master node) і самого кластера [3]. Забезпечити обмеження доступу серед розробників. Чим менше персоналу має доступ до файлів – тим менша імовірність помилкової зміни налаштувань. Крім того ключі безпеки варто регулярно замінювати. Згідно з рекомендаціями GCM ключ треба змінювати кожна 200 000 записів [4]

Публічні хмари такі як Google cloud завжди мають налаштоване шифрування за замовчуванням і не надають користувачу доступу до цих налаштувань, а також інформації про алгоритм шифрування[5]. Таким чином розробник звільняється від потреби керувати налаштуваннями безпеки etcd. В той же час провайдер послуг надає гарантії безпеки, що підкріплюються різноманітними сертифікаціями. Це спрощує процес обслуговування інфраструктури, а отже зменшує фінансові витрати.

Шифрування etcd в Kubernetes є важливою стратегією безпеки, яка може бути реалізована за допомогою різних алгоритмів. По суті, система зазвичай контролюється постачальниками хмарних послуг у керованих середовищах, таких як GKE, AKS і EKS. Проте за необхідності використання не керованого Kubernetes кластеру потребує уважного налаштування, та обмеженого доступу за для забезпечення безпеки всіх даних. Метод шифрування може використовувати різних провайдерів кожен з яких демонструє різний баланс між надійністю безпеки, продуктивністю та складністю керування ключами. Обрана техніка шифрування повинна відповідати вимогам безпеки організації, враховуючи такі аспекти, як зобов'язання щодо відповідності, вимоги до продуктивності та операційні можливості, при цьому дотримуючись ефективних методів керування ключами, таких як періодична ротація, безпечні методи резервного копіювання та суворий контроль доступу до налаштувань шифрування.

Список використаних джерел:

1. CNCF SURVEY 2023, available at: <https://www.cncf.io/reports/cncf-annual-survey-2023/> (Accessed 19 Nov 2023)
2. Reddy, Dinesh. 2023. «Security in Kubernetes: A Comprehensive Review of Best Practices». International Journal of Science and Research (IJSR). 12. DOI: 10.21275/SR24304111526.

3. Shamim, Md Shazibul Islam та Bhuiyan, Farzana Ahamed та Rahman, Akond. 2020. «XI Commandments of Kubernetes Security: A Systematization of Knowledge Related to Kubernetes Security Practices». 58-64. DOI: 10.1109/SecDev45635.2020.00025
4. Encrypting Confidential Data at Rest. Available providers, available at: <https://kubernetes.io/docs/tasks/administer-cluster/encrypt-data/#providers> (Accessed 19 Nov 2023)
5. Control plane security. etcd security, available at: https://cloud.google.com/kubernetes-engine/docs/concepts/control-plane-security#etcd_security (Accessed 19 Nov 2023).

Ключові слова: Kubernetes, безпека, etcd, шифрування, сервіс управління ключами, керований кластер.

Keywords: Kubernetes, security, etcd, encryption, key management service, managed cluster.

Науковий керівник: д.т.н., професор Пархуць Л. Т.

МОДЕЛЮВАННЯ ТА РЕАЛІЗАЦІЯ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Савранчук Владислава

студентка 4 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Критична інфраструктура в сучасному світі складається з численних систем енергетики, транспорту, водопостачання, охорони здоров'я та інших. Проблеми в цих системах є одним з основних ризиків для національної безпеки, оскільки будь-яка поломка або незаконне втручання негативно впливає на економіку та здоров'я населення. Основна проблема полягає в тому, як найкраще підтримувати функціональність цих систем, водночас зменшуючи вразливість до кіберзагроз.

В.Д. Бойко, М.Д. Василенко та В.М. Слатвінська [1] дослідили питання моделювання живучості та відновлення інформаційно-комунікаційних мереж в умовах дії кіберзагроз, акцентуючи увагу на можливості забезпечення стабільності мережі в кризових ситуаціях.

Натомість для моделювання кіберзахисту критичної інфраструктури було створено демонстраційний код на Python:

```
import random
import time
# Створюємо зразковий список дозволених IP-адрес
allowed_ips = {"192.168.1.1", "192.168.1.2", "192.168.1.3"}
# Логи дій користувачів
logs = []
# Функція для імітації запитів від користувачів
def simulate_request():
```

```

    ip = f"192.168.1.{random.randint(1, 10)}"
    action = random.choice(["login", "access_file", "modify_config",
"send_data"])
    logs.append({"ip": ip, "action": action, "timestamp": time.time()})
    return ip, action
# Функція для виявлення аномальних запитів
def detect_anomalies(logs):
    anomalies = []
    for log in logs:
        ip = log["ip"]
        if ip not in allowed_ips:
            anomalies.append(log)
    return anomalies
# Імітація та перевірка запитів
for _ in range(10): # згенеруємо 10 запитів
    ip, action = simulate_request()
    print(f"Запит від {ip}, дія: {action}")
# Виявлення аномальних запитів
anomalies = detect_anomalies(logs)
if anomalies:
    print("\nАномальні запити:")
    for anomaly in anomalies:
        print(f"IP: {anomaly['ip']}, дія: {anomaly['action']}, час:
{time.ctime(anomaly['timestamp'])}")
    else:
        print("Аномальних запитів не виявлено.")

```

Джерело: авторська розробка

Цей код допомагає, коли потрібно змоделювати виявлення підозрілої активності в мережі критичної інфраструктури шляхом аналізу журналів і моніторингу портів. У системі використовується базовий алгоритм для відстеження можливих аномальних дій, включаючи несанкціонований доступ або послідовності та шаблони, які можуть становити загрозу для серверів, і на основі яких генеруються сповіщення в режимі реального часу.

Цей код є прикладом того, як працює система, що відстежує та виявляє порушення в запитах користувачів. Ось розбивка того, як це працює:

Код починається з імпорту двох модулів: `rand` для випадкових чисел і `time` для обробки часових значень.

У коді визначено два набори констант і змінних:

- `allowed_ips`: список IP-номерів, до яких дозволено доступ (в даному випадку рядок з трьох чисел 192.168.1).

- logs: список, до якого буде додано записану історію запитів користувачів.

У коді визначено дві функції:

- simulate_request(): створює випадковий вихідний IP або IP із заданого діапазону та випадкову дію, тобто спробу входу, доступ до файлу, зміну конфігурації або відправку даних. Створюється запис про подію, а IP-адреса, дія та час цієї події заносяться до списку журналу.

- detect_anomalies(logs): викликається зі списком логів як параметром і має повернути список аномалій, а точніше список запитів, зроблених з IP-адрес, яких немає в наборі allowed_ips.

Основна програма складається з наступних етапів:

Для імітації діяльності користувача використовується функція simulate_request(), яка виконує завдання 10 користувачів. Для кожного запиту на консоль виводиться IP-адреса та дія.

Після цього код викликає функцію detect_anomalies(logs) для виявлення аномалій у заданому списку логів. Якщо виявлено аномалії, вона виводить ці аномалії на консоль, показуючи IP-адресу, виконану дію та час, коли вона була виконана. Після цього програма виводить список змодельованих запитів, а потім список аномалій, якщо такі були виявлені. Якщо програма не виявила жодної аномалії, вона виводить повідомлення про те, що аномалії не виявлено.

Таким чином, цей код імітує запити користувачів, записує їх у лог-файл і виявляє небажані через порівняння відповідної адреси зі списками дозволених адрес.

Такий підхід може проілюструвати, що ідентифікація загроз для критичної інфраструктури може бути автоматизована і стати важливим інструментом у підвищенні рівня безпеки. Надалі необхідна подальша робота над розробкою методів машинного навчання для більш ефективного виявлення та класифікації загроз, а також над впровадженням цієї системи в реальне інфраструктурне середовище.

Список використаних джерел:

1. Бойко В., Василенко М., Слатвінська В. Моделювання живучості та відновлення інформаційно-комунікаційних мереж в умовах дії кіберзагроз. *Інформаційні технології та суспільство*. 2024. № 1 (12). С. 13-19. DOI: <https://doi.org/10.32689/maup.it.2024.1.2> URL: <https://journals.maup.com.ua/index.php/it/article/view/3143> (дата звернення: 07.11.2024).

Ключові слова: критична інфраструктура, логи, порти, кібербезпека.

Keywords: critical infrastructure, logs, ports, cybersecurity.

Науковий керівник: доктор філософії, асистент кафедри кібербезпеки Слатвінська В.М.

Секція 2. ШТУЧНИЙ ІНТЕЛЕКТ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЗАДАЧАХ КІБЕРБЕЗПЕКИ

РИЗИКИ ВИКОРИСТАННЯ ГРАФІЧНОГО КОНТЕНТУ, СТВОРЕНОГО ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

Логінова Наталія

*завідувачка кафедри інформаційних технологій Національного університету
«Одеська юридична академія», кандидат педагогічних наук, доцент*

У сучасних умовах розвитку інформаційного суспільства штучний інтелект (ШІ) швидко поширюється у всіх сферах життєдіяльності людини. Не стало виключення та використання його для візуалізації даних, розпізнавання образів та комп'ютерної графіки.

Алгоритми ШІ здатні створювати графічні зображення на основі аналізу та генерації заданої інформації користувача. Методи навчання нейромереж дозволяють розпізнавати графічні елементи та генерувати на їх основі необхідне зображення. Найбільш поширеними алгоритмами зараз є DALL-E, Imagine with Meta, Midjourney та Stable Diffusion.

DALL-E – це модель ШІ, яка генерує графічні зображення за текстовим описом або з готових зображень. А саме, надавши кілька коротких фраз, модель розуміє мову та створює точні зображення. Також вона може редагувати зображення користувача за заданими критеріями [1].

Imagine with Meta – це генератор зображень зі ШІ, на основі текстових описань. Даний генератор, розроблений Facebook і Instagram. Для того, щоб вказати, що зображення створено за допомогою ШІ, виробники додають невидимі водяні знаки, які можна знайти за допомогою відповідної моделі [2].

Нейромережа Midjourney працює як чат-бот в Discord. Він використовує сучасні алгоритми обробки зображень, застосовуючи різні фільтри, може змінювати кольори, додавати спеціальні графічні ефекти тощо. Для створення зображень потрібна обов'язкова реєстрація. Сервіс платний, але є 25 безкоштовних дій, таких як генерація зображень, розробка різних варіантів та інше [3].

Stable Diffusion – це модель генеративного ШІ, побудована на концепції «дифузії». Початкове зображення генерується з випадкового, а потім вдосконалюється по крокове, щоб зробити зображення, яке відповідає вимогам користувача. Модель може перетворювати текст на зображення та зображення на зображення, генерувати графічні твори, редагувати готові графічні зображення та створювати відео. Доступна за ліберальною ліцензією [4].

Аналіз алгоритмів ШІ показує, що існує багато інструментів, що дозволяють генерувати графічні зображення. Тому виникає запитання: А які ризики виникатимуть під час використання графічного контенту, створеного за допомогою ШІ?

Для навчання нейромереж необхідно використовувати готові графічні зображення, які можуть бути захищені авторським правом. Фотографії визнаються об'єктами авторського права, якщо вони є оригінальними творами, тобто результатом творчих зусиль фотографа. Відповідно до Закону України “Про авторське право та суміжні права” винятковим правом автора є право на дозвіл або заборону використання твору (у тому числі шляхом розповсюдження та переробки) [5]. Тому необхідно звернутися до автора чи правовласника контенту та офіційно отримати дозвіл на його використання.

Але є альтернатива авторському праву – вільні ліцензії Creative Commons. Автори, які розміщують свої твори під цими ліцензіями, надають іншим людям право вільно використовувати їх за певних умов, наприклад, із зазначенням авторства [6]. Отже, для навчання нейромереж треба використовувати зображення, що розповсюджуються під вільними ліцензіями або брати дозволи у авторів.

У генеративних системах ШІ для навчання нейромереж можуть використовуватися поганої якості зображення, які діятимуть неадекватно на навчальну модель та сприятимуть непередбачуваності у подальшій роботі алгоритмів. Далі такі зображення можуть мати негативні наслідки для роботи або життя людей, якщо ці зображення використовуються, наприклад, в медицині.

В інтернеті багато платформ стали підтримувати генеративний контент. Наприклад, американська компанія Shutterstock, яка розміщує стокові фотографії, відео- та аудіоконтент, оголосила, що за допомогою OpenAI почне продаж згенерованих ШІ зображень. Виникають побоювання, що моделі ШІ, які використовуються для створення зображень, створюватимуть контент, що конкуруватиме з художниками, чиї роботи використовують нейромережі для навчання. Щоб вирішити цю проблему, Shutterstock пообіцяла відшкодувати творцям, які можуть постраждати від моделей ШІ [7].

Одна з компаній, що займається розробкою програмного забезпечення для графіки, Adobe, у 2023 році розробила ШІ генеративний сервіс для створення зображень – Adobe Firefly. До застосунків Photoshop, Illustrator, Lightroom, InDesign та інших, були додані різні графічні інструменти ШІ, створені спеціально для розвитку творчості та зміни робочих процесів. На офіційному сайті компанії зазначено, що модель генеративного ШІ було навчено на наборах даних із ліцензійного вмісту Adobe Stock та вмісту суспільного надбання з простроченим терміном дії авторських прав. Також компанія розро-

била модель компенсації для авторів Adobe Stock, вміст якої використовується в наборах даних для навчання моделей Firefly [8].

Можливості генерування графічних зображень ШІ створює можливості маніпулювання реальними зображеннями, що може використовуватися для дезінформації або створення фальсифікованого контенту.

Отже, розглянуті ризики використання графічного контенту, створеного за допомогою алгоритмів ШІ важливі для розробки стратегій безпечного використання генеративного ШІ.

Список використаних джерел:

1. Dall-E Free. URL: <https://www.dall-efree.com/about-us> (дата звернення: 10.11.2024)
2. Meta презентувала свій ШІ-генератор зображень Imagine: чим особливий. URL: <http://surl.li/vaobge> (дата звернення: 10.11.2024)
3. Midjourney. URL: <https://www.midjourney.com/home> (дата звернення: 10.11.2024)
4. OpenART. <http://surl.li/pkmej1> (дата звернення: 10.11.2024).
5. Про авторське право і суміжні права: Закон України від 15.04.2023 р. // Відомості Верховної Ради (ВВР), 2023, № 57, ст.166. URL: <https://zakon.rada.gov.ua/laws/show/2811-20#n855> (дата звернення: 11.11.2024).
6. Creative Commons. URL: <https://creativecommons.org/licenses/by/4.0/deed.en> (дата звернення: 11.11.2024).
7. Стокова платформа Shutterstock.com. URL: <https://www.shutterstock.com> (дата звернення: 11.11.2024).
8. Творить за допомогою генеративного ШІ Adobe Firefly. URL: <https://www.adobe.com/ua/products/firefly.html> (дата звернення: 11.11.2024).

Ключові слова: штучний інтелект, нейромережі, графічні зображення, ризики

Keyword: artificial intelligence, neural networks, graphics, risks

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В РОБОТІ СИСТЕМНОГО АНАЛІТИКА

Трофименко Олена

*доцент кафедри інформаційних технологій Національного університету
«Одеська юридична академія», кандидат юридичних наук, доцент*

Стрілець Михайло

*магістр 2-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

Системний аналіз безпосередньо впливає на можливий успіх чи то за-непад підприємств та організацій, оскільки робота системного аналітика полягає в перевірці, проектуванні та вдосконаленні їх робочих процесів. Підприємства без системного аналітика, а для великих організацій – навіть без команди системних аналітиків, нерідко виробляють продукти та послуги, які не мають попиту. Зрештою робота системного аналітика або аналітика бізнес-

технологій полягає в аналізі даних, проєктуванні бізнес-проблем та впровадженні інформаційних систем для перетворення рішень високого рівня на матеріальні продукти. Системні аналітики (System Analysts) використовують дані для оцінки процесів, визначення вимог і надання на основі даних рекомендацій та звітів керівникам і зацікавленим сторонам (стейкхолдерам). Вони займаються стратегічним плануванням, аналізом бізнес-моделі, проєктуванням процесів і системним аналізом. Такий спектр задач потребує від системного аналітика володіння широким спектром операційних систем, програмного забезпечення та апаратних платформ. Вони можуть бути частиною проєкту від фази його аналізу до оцінювання після розгортання. Тому все частіше на ринку праці (<https://www.work.ua/jobs/>) у назві професії системного аналітика вказують приставку «ІТ» – ІТ системний аналітик (IT System Analyst), тим самим акцентуючи увагу на важливість для такого фахівця у здатності використання сучасних ІТ-засобів для системного аналізу даних.

Наразі все більше організацій покладаються на наукові дані при формуванні своїх бізнес-рішень. Наука про дані стосується збору даних із різних ресурсів і використання бізнес-аналітики, машинного навчання та аналітичної майстерності для розуміння даних. Аналітики використовують свої статистичні здібності для аналізу даних, розробляють візуалізації та інші способи передачі результатів свого аналізу.

Системний аналіз на основі штучного інтелекту (ШІ) допомагає автоматизувати повторювані завдання, дозволяючи професіоналам зосередитися на більш важливих задачах. Це зменшує кількість людських помилок і покращує продуктивність, заощаджуючи час і ресурси.

Алгоритми ШІ гарно справляються з обробленням великих обсягів даних та ідентифікацією шаблонів. ШІ дозволяє компаніям відстежувати процеси в системі в режимі реального часу, надаючи завчасні попередження про можливі проблеми чи то неефективність. Такий проактивний підхід дозволяє ефективно розв'язувати проблеми та допомагає запобігти дорогим простоям.

Алгоритми машинного навчання допомагають автоматизувати побудову аналітичних моделей в аналітиці даних. Ці алгоритми здатні навчатися на основі даних, визначати закономірності та ухвалювати рішення з мінімальним втручанням людини. Їх застосування в аналітиці даних охоплює сфери сегментації клієнтів, виявлення шахрайства та аналізу ринку [1].

Впровадження машинного навчання в аналітику даних зробило революцію в інтерпретації даних, надаючи безпрецедентну інформацію та полегшуючи прийняття рішень на основі даних у різних секторах. Розвиток машинного навчання та великих даних призвів до появи низки спеціалізованих професій у сфері системного аналізу даних, як-от: Data Scientist, Data Analyst, Data Engineer, Artificial Intelligence Engineer, Machine Learning Engineer та

Machine Learning Scientist [2]. Ці професіонали виділяють значущі шаблони з величезних масивів даних, застосовують складні алгоритми та створюють прогнознi моделі, які мають велике значення для стратегічного планування й ефективності роботи. У свою чергу, поява великих даних спричинила потребу розробки методів машинного навчання, які здатні обробляти й аналізувати набори даних, які є занадто великими, складними або швидко змінюваними для традиційних методів оброблення даних.

ІТ системний аналітик є сполучною ланкою між вимогами бізнесу та технологічними рішеннями, забезпечуючи відповідність систем та програмного забезпечення бізнес-цілям. Саме він відповідає за аналіз, проектування, впровадження та оптимізацію інформаційних систем, які підвищуватимуть ефективність і результативність діяльності організації [3]. Як показав аналіз функціональних вимог до таких фахівців на ринку праці (сайт <https://www.work.ua/jobs/>), роботодавці покладають на системного аналітика відповідальність за аналіз та оптимізацію інформаційних систем замовників, забезпечуючи їх ефективне та безперебійне функціонування. З-посеред функціональних задач системного аналітика є такі:

- аналіз бізнес-процесів та виявлення потреб в інформаційних системах;
- збір бізнес-вимог замовника щодо автоматизації процесів;
- збір та оброблення великих обсягів даних, ухвалення обґрунтованих рішень у команді та керуванні проєктами (володіння інструментами PL SQL, MySQL, MS SQL тощо);
- аналіз бізнес-процесів та виявлення поточних та перспективних потреб, розробка заходів по систематизації, оптимізації наявного функціоналу програмного забезпечення або продуктів, пропозиція і формалізація рішення;
- ідентифікація ризиків процесу та пропозиція по превентивним мірам нівелювання, крокам їх ліквідації;
- моделювання бізнес-процесів (знання нотацій UML, BPMN, IDEF0 та інструментів Miro, Draw.io тощо);
- проектування аналітичної, операційної звітності;
- робота з системами управління змінами (Atlassians, MS Project, Jira, Confluence тощо), робота з SOAP/REST вебсервісами та форматами JSON, XML тощо.

Загалом професії з аналізу даних входять у список найбільш актуальних.

Системні аналітики даних потрібні в самих різних галузях: ІТ, медицині, фінансах, сільському господарстві, логістиці тощо. Вміння використовувати ШІ в системному аналізі надає численні переваги від покращення ефективності до покращення прийняття рішень та можливості моніторингу системи у ре-

жимі реального часу. Тим самим ШІ стає невід’ємною частиною для аналізу систем у майбутньому.

Список використаних джерел:

1. Nucci R., Sevilla D. What is a IT Systems Analyst? URL: <https://www.getguru.com/reference/it-systems-analyst-a9236>.
2. The Impact of Artificial Intelligence on Systems Analysis: What You Need to Know. URL: <https://moldstud.com/articles/p-the-impact-of-artificial-intelligence-on-systems-analysis-what-you-need-to-know>
3. Crabtree M., Nehme A. What is Data Analysis? An Expert Guide With Examples. URL: <https://www.datacamp.com/blog/what-is-data-analysis-expert-guide>

Ключові слова: системний аналітик, системний аналіз, штучний інтелект, ШІ.

Keywords: system analyst, system analysis, artificial intelligence, AI.

АПАРАТНИЙ ЗАХИСТ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ NGFW МЕРЕЖЕВИХ ЕКРАНІВ

Задерейко Олександр

*доцент кафедри інформаційних технологій Національного університету
«Одеська юридична академія», кандидат технічних наук, доцент*

Модель OSI (Open Systems Interconnection) є стандартом взаємодії між мережевими пристроями, що описує 7 рівнів абстракції. Ці рівні виконують різні функції: перший — фізичний, другий — канальний, третій — мережевий, четвертий — транспортний, п’ятий — сесійний, шостий — рівень уявлення даних, і сьомий — прикладний рівень, який взаємодіє з програмним забезпеченням користувача (рис. 1).

Рівні моделі OSI ISO	Приклади протоколів
7. Прикладний	HTTP, FTP, SMTP, DNS
6. Представлення	ASII, MPEG, JPEG
5. Сеансовий	
4. Транспортний	TCP, UDP
3. Мережений	IP, IPS, RIP, OSF
2. Канальний	Ethernet
1. Фізичний	

Рис. 1. Мережева семирівнева модель OSI ISO.

Кожен мережевий пристрій функціонує на своєму конкретному рівні абстракції: веб-сервер та веб-браузер взаємодіють на рівні додатків (рівень 7 або L7), тоді як маршрутизатори обмінюються інформацією на канальному (L2) та мережевому (L3) рівнях, передаючи кадри та пакети [1].

Міжмережевий екран (брандмауер, firewall) також є мережевим пристроєм, який може виконувати функції свічу, маршрутизатора або навіть виступати як «віртуальний кабель» у мережевій топології, залежно від свого типу. Однак на ці пристрої лягає додаткове навантаження, оскільки вони повинні аналізувати вміст пакетів, що ускладнює їх роботу [2].

Глибина аналізу мережевих пакетів може варіюватися, і важливою відмінністю є те, чи здійснюється аналіз на рівнях L4 або L7. Це визначає рівень деталізації перевірки та функціональність пристрою.

Брандмауер (firewall) сам собою не є частиною рівнів моделі OSI. Натомість він має додаткові правила, доданими до функціональності різних рівнів OSI.

Найбільш типовий брандмауер працює на рівнях L3 та L4 (IP обох типів та TCP/UDP). У його функції входить можливість блокувати чи дозволяти комунікацію через різні порти, вхідні і вихідні. Брандмауери можуть бути структуровані по-різному, але насправді тісно пов'язані з мережевою реалізацією самого пристрою (особливо з його операційною системою).

Іноді брандмауер може мати додаткову логіку розуміння деяких протоколів прикладного рівня та брандмауера з їхньої основи.

L4 брандмауер — це міжмережевий екран, який пропускає мережевий трафік і перевіряє заголовки протоколів 4-го рівня: TCP, UDP, ICMP. Основними критеріями для фільтрації трафіку є IP-адреси, порти TCP/UDP та сервіси ICMP.

Сучасні L4 брандмауери зберігають стан як TCP, UDP і ICMP, а й відстежують взаємодія всього прикладного ПЗ лише на рівні L7. Наприклад, стан FTP, HTTP, SIP та іншого прикладного ПЗ, що вже залежить від конкретної реалізації firewall.

L7 брандмауери — це міжмережеві екрани, які пропускають IP-трафік і аналізують не лише заголовки 4-го рівня, але й сегмент даних кожного IP-пакета. Вони здатні розпізнавати трафік на рівні прикладного ПЗ (L7), зокрема визначати, які файли передаються і в якому напрямку. Оскільки аналізується більше даних, правила L7 брандмауера мають значно більше критеріїв перевірки, таких як ім'я користувача, тип прикладного ПЗ, категорія URL і стан ПЗ на комп'ютері користувача.

Навантаження на L7 брандмауер значно вище, оскільки його процесор повинен постійно аналізувати великі обсяги даних, які передаються прикладними програмами. Це включає мегабайти полів даних, в той час як L4 брандмауер перевіряє лише кілька байт заголовка IP-пакета, зокрема адреси джерела та призначення, а також порти. Для зберігання стану кожного прикладного ПЗ на L7 потрібен набагато більший буфер, оскільки обсяг передаваних даних на цьому рівні значно більший, ніж у заголовку TCP/IP. Через це,

при однаковому обсязі пам'яті, L7 брандмауер може одночасно зберігати менше сесій, ніж L4. Оскільки L7 брандмауер може ідентифікувати, яке прикладне ПЗ використовує мережу, правила фільтрації можуть бути сформульовані за ім'ям ПЗ, а не за номером порту, як у L4. Крім того, сучасне прикладне ПО генерує безліч з'єднань і всі вони є його частиною. Цей вид брандмауера дозволяє повернути контроль за сучасним динамічним прикладним програмним забезпеченням, що працює по будь-якому порту, наприклад, teamviewer, bittorrent, tor, про «поведінку» яких L4 firewall фактично нічого не знає. Тобто L7 firewall у сучасних реаліях потрібен, якщо необхідно забезпечити високий рівень безпеки у мережі.

Тобто L7 брандмауер отримав у мережному профільному середовищі назву Next-Generation Firewall (NGFW). Усередині цього мережевого пристрою, реалізованого L7 брандмауері основним кваліфікатором стає ім'я програми L7, то правила пишуться за новими критеріями. У NGFW завжди працює динамічне зіставлення IP адрес користувачів у мережі, тому ім'я користувача теж стає кваліфікатором (критерієм). NGFW включає функції розшифровки SSL/TLS і SSH для розпізнавання додатків і атак всередині них, IPS, антивіруса, URL фільтрації і т.д. [3].

Термін NGFW спочатку був вигаданий маркетингом компанії Palo Alto Networks. Але поступово зміцнився на мережевому ринку, і всі виробники UTM зараз теж називають себе NGFW. NGFW теж виконує кілька функцій одночасно. Відмінність NGFW від UTM важливо знати та розуміти. Воно полягає в тому, що NGFW функції безпеки додатків (IPS, антивірус, URL фільтрація) прискорені апаратно. Існують спеціалізовані апаратні чіпи: IPS перевіряє атаки на своєму чіпі, антивірус сигнатури на своєму, розшифровка SSL - на своєму і таке інше. Поділ функцій з різних процесорів дає можливість запускати захисні функції паралельно і чекати, коли закінчить працювати попередня функція, як і UTM. Наприклад, в апаратних міжмережевих екранах компанії Palo Alto Networks встановлено до 60 спеціалізованих процесорів, що виконують прискорення функцій безпеки, мережевих функцій та їх керування. Важливо, що NGFW містять єдиний програмний інтерфейс керування всіма функціями одночасно.

Ідея функціонування NGFW на відміну від UTM – реалізувати кожну функцію на окремому процесорі, який спеціалізований під необхідний функціонал.

Подібно до того, як виробники комп'ютерів колись винесли функції математичних обчислень та графіки в окремі співпроцесори, сучасні NGFW (нові покоління міжмережевих екранів) оснащуються спеціалізованими процесорами для розпізнавання прикладного ПЗ на рівні L7, для розшифрування SSL/SSH, перевірки антивірусних сигнатур, аналізу IPS-сигнатур тощо. Це

дозволяє виконувати всі ці функції одночасно, без зниження швидкості або затримок у передачі трафіку під час перевірки.

Саме тому міжмережеві екрани без прискорення купують, оскільки прискорення не потрібно на невеликих швидкостях, але коли швидкості аналізу трафіку виходять за 1-5 Гігабіт — реалізувати всі функції безпеки вже неможливо без апаратного прискорення.

Мета пристрою NGFW: дати можливість безпечно працювати кінцевому користувачеві не уповільнюючи мережевий трафік. Це дозволяє постійно перевіряти, що прикладне ПЗ передає потрібний користувачеві безпечний контент, і паралельна робота рушіїв захисту з одним потоком мережного трафіку гарантує задану продуктивність при всіх включених функціях безпеки і мінімальну затримку мережевого трафіку.

Список використаних джерел:

1. Задерейко О. В., Логінова Н. І., Толокнов А. А. Комп'ютерні мережі : навчальний посібник [Електронне видання], Одеса : Фенікс, 2022, 249 с. ISBN 978-966-928-828-8. URL: <http://dspace.onua.edu.ua/handle/11300/19423>.
2. Ільге, І. Г., Ільге, О. І., & Запорожцев, С. Ю. (2021). Особливості вибору міжмережевих екранів для захисту комп'ютерної мережі організації. URL: <https://api.dspace.khadi.kharkov.ua/server/api/core/bitstreams/c3b62d41-3c08-4307-b0e9-ddd2d08d8ad0/content>.
3. Brar, M. K., Kaur, B., Singh, G., Jindal, P. K., & Sood, S. (2024, July). Traditional firewall vs. next-generation firewall: A review. In AIP Conference Proceedings (Vol. 3121, No. 1). AIP Publishing.

Ключові слова: NGFW, UTM, сетевая инфраструктура, сетевое устройство, фильтрация трафика, проверка сигнатур, расшифровка SSL/TLS

Keywords: NGFW, UTM, network infrastructure, network device, traffic filtering, signature checking, SSL/TLS decryption

ШТУЧНИЙ ІНТЕЛЕКТ У КІБЕРБЕЗПЕЦІ ЕНЕРГЕТИЧНИХ СИСТЕМ

Куклінова Тетяна

доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат економічних наук, доцент

Стабільне й безперебійне енергопостачання лежить в основі національної безпеки будь-якої країни. Водночас вразливість енергетичної інфраструктури може стати фактором дестабілізації для всієї соціально-економічної системи держави. Військові дії, руйнування енергетичної інфраструктури, брак фінансових ресурсів та заборгованість енергетичних компаній створюють великі проблеми для енергетики України. На окупованих територіях знаходяться Запорізька АЕС, Луганська Вуглегірська ТЕС, Каховська ГЕС, Луганська ТЕС.

Атомна генерація залишається базовою для України. Атаки Росії на АЕС загрожують ядерній та радіаційній безпеці всього світу. Зазначається, що станом на 01.05.24 прямі збитки енергетичного сектору України перевищили 16,1 млрд. дол. США [1].

Більшість енергетичної інфраструктури в Україні була збудована ще за радянських часів і потребує оновлення. Застаріле обладнання працює неефективно та призводить до значних енергетичних втрат. Основним завданням для України є зміцнення енергетичної безпеки. Українська енергосистема є частиною європейської, тому її розвиток та модернізація повинні відповідати європейським стандартам. Цифровізація енергетичних мереж є одним із головних напрямків у розвитку сучасної енергетичної інфраструктури. Зазначається, що найбільший вплив на енергетичний сектор має автоматизація. Так, О. Кириленко, С. Денисюк, І. Блінов наводять перелік цифрових технологій зі зниженням їхнього впливу на системи передачі та розподілу електроенергії: автоматизація та цифровий робочий процес, кібербезпека, розширена аналітика, IoT, візуалізація даних, хмарні обчислення, дрони, розподілені обчислення, блокчейн, Augmented Reality, AR, Virtual Reality, VR, кодування [2].

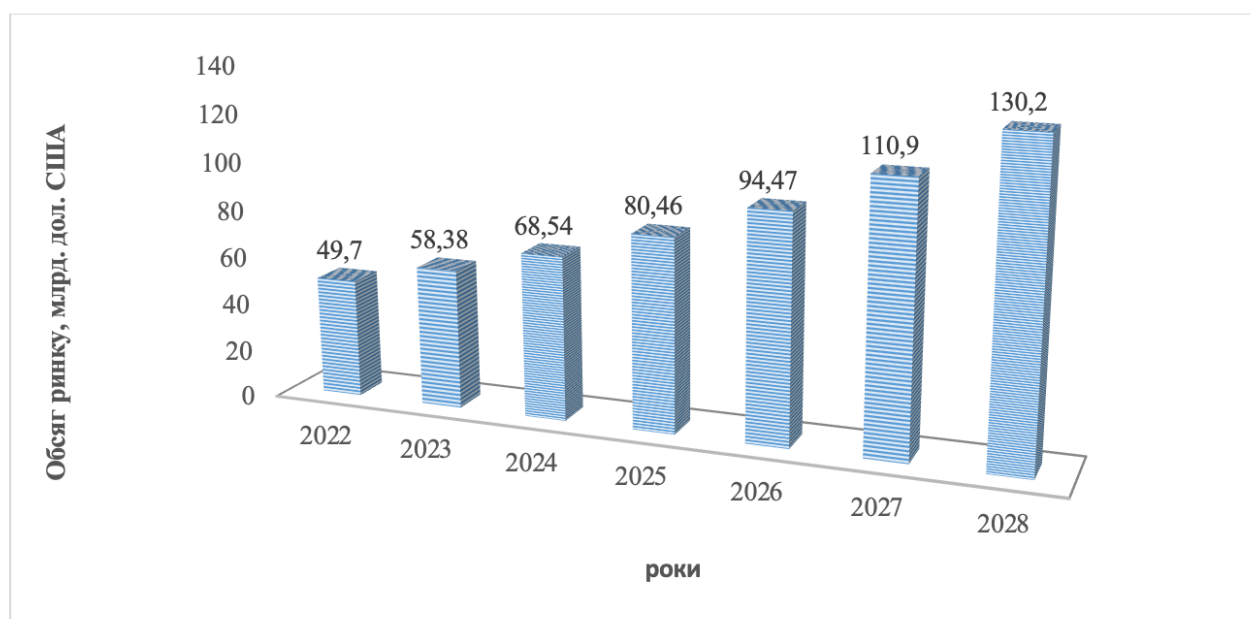


Рис.1. Обсяг ринку технологій Smart Grid у світі з 2022 по 2028 рр. [3].

Швидкий прогрес цифрових технологій за останні десятиліття спричинив їх широке впровадження в електричні мережі, а також розвиток «розумних» мереж (Smart Grid). Як свідчить Рис.1 у 2022 році ринок технологій Smart Grid оцінювався майже в 50 мільярдів доларів США, і, за прогнозами, до 2028 року він зростатиме з середньорічним темпом зростання 17,4%, та

досягне приблизно 130 мільярдів доларів США. Оскільки технології Smart Grid продовжують розвиватися, вони стають невід'ємною частиною створення більш стійких, стійких та ефективних енергетичних систем у всьому світі. Ця тенденція підкреслює важливість впровадження рішень на основі штучного інтелекту (ШІ) та модернізації інфраструктури для вирішення глобальних енергетичних викликів.

Але високий рівень цифровізації призводить до кіберзагроз, які спрямовані на безпеку електромереж і створюють серйозну проблему через численні атаки. Тому кібербезпека стає важливим елементом енергетичної безпеки.

Так, до повномасштабного вторгнення Україну атакували окремі угруповання хакерів. Підкреслюється, що зараз хакерів координує один центр. Росія витрачає на кожну кібератаку мільйони доларів. У 2023 році було зафіксовано близько 55 кібератак на енергооб'єкти. Кібератаки комбінуються з ракетними ударами та атаками дронів по енергооб'єктах. З 24 лютого 2022 року кількість кіберінцидентів на держкомпанії «Укренерго» зростає втричі, порівняно з попереднім роком. До повномасштабної війни російських хакерів цікавила фінансова вигода: викуп за повернення систем у лад чи крадіжку даних із метою продажу. Зараз дестабілізація критичної інфраструктури, щоб припинити енергопостачання. Російські хакери використовують різні підходи: від сканування IT-периметра до DDoS-атак. Під час однієї з DDoS-атак на Укренерго кількість запитів могла перевищувати 5 млн за кілька годин [4].

Крім того, кібератаки можуть впливати не лише на енергетичну систему України, а й на енергосистеми сусідніх країн. Подібні кібератаки мають ризик повторення в інших державах. Це обумовлено тим, що структура українських мереж є типовою для багатьох країн. Типи обладнання, що використовуються в українській енергосистемі, також широко розповсюджені за її межами.

ШІ оптимізує виробничі процеси, підвищує ефективність використання ресурсів та сприяє зниженню витрат. Впровадження ШІ у енергосектор є необхідним кроком для підвищення ефективності та надійності енергопостачання в Україні в умовах відновлення після ракетних обстрілів. У своєму дослідженні О. М. Суходоля підкреслює, що рівень застосування ШІ в українських енергетичних компаніях є низьким [5].

На наш погляд, використання ШІ має стати ключовою складовою енергетичної сфери, що сприятиме покращенню стану електромереж. Це дозволить оптимізувати процеси виробництва, передачі та споживання електроенергії, зменшуючи втрати та підвищуючи стабільність мережі.

ШІ здатен виявляти аномалії в мережевому трафіку, аналізувати поведінку систем у реальному часі та прогнозувати потенційні загрози ще до того, як вони стануть критичними. Завдяки алгоритмам машинного навчання, ШІ може навчатися на основі попередніх атак, що дозволяє системам захисту енергетичного сектора постійно вдосконалюватися та адаптуватися до нових типів загроз. Також ШІ допомагає автоматизувати процеси реагування на кібератаки, що скорочує час реакції та мінімізує збиток та допомагає покращити системи ідентифікації користувачів і управління доступом, відкриваючи аномальні запити і спроби несанкціонованого доступу. Поєднуючи інструменти ШІ з різними цілями, технологіями, функціями та можливостями, можна мінімізувати енергетичні ризики та підвищити безпеку енергетичної інфраструктури країни.

Отже, з огляду на значення електроенергії в сучасній економіці та суспільстві, забезпечення кібербезпеки в енергетичних системах потребує сучасних і надійних цифрових рішень. Необхідність використання ШІ у кібербезпеці енергетичного сектора обумовлена зростанням складності та частоти кібератак на критичну інфраструктуру. Використання ШІ у кібербезпеці енергетики забезпечує підвищену стійкість та надійність систем, знижуючи ризики несанкціонованого доступу і, відповідно, забезпечуючи безперервність роботи енергетичних об'єктів.

Список використаних джерел:

- 1.Збитки та втрати енергетичного сектору України. Київська школа економіки URL:<https://kse.ua/ua/about-the-school/news/zbitki-ta-vtrati-energetichnogo-sektoru-ukrayini-vnaslidok-povnomasshtabnogo-vtorgnennya-rosiyi-perevishhili-56-mlrd-otsinka-kse-institute-stanom-na-traven-2024-roku/> (Дата звернення 09.11.2024).
2. Кириленко О., Денисюк С., Блінов І. Цифрова трансформація енергетики: сучасні тенденції та завдання. *Збірник наукових праць Інституту електродинаміки НАН України*. 65. 2023. С. 5-14.
3. Smart grid technology market size worldwide from 2022 to 2028. URL: <https://www.statista.com/statistics/1301566/global-smart-grid-market-value/> (Дата звернення 09.11.2024).
4. Чайка О. Російські хакери координують дії з військовими та посилюють атаки напередодні зими. Як Україна протистоїть кібератакам на енергосистему. November 15. 2023. Forbes Ukraine. URL: <https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energositemu-08112023-17242> (Дата звернення 09.11.2024).
5. Суходоля О.М. Штучний інтелект в енергетиці : аналіт. доповідь. К. : НІСД, 2022. 49 с.

Ключові слова : штучний інтелект, розумна електромережа, кібербезпека.

Keywords: artificial intelligence, Smart Grid, cyber security.

СИСТЕМИ АВТОРИЗАЦІЇ ТА АВТЕНТИФІКАЦІЇ ЯК ОСНОВА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Головашич Сергій

ТОВ «Мікрокрипт Текнолоджис»

Половінкін Миколай

Аспірант Державного університету інформаційно-комунікаційних технологій

Ровда Володимир

Аспірант Державного університету інформаційно-комунікаційних технологій

Постановка проблеми

У сучасному світі інформаційна безпека є одним із ключових аспектів функціонування будь-якої системи. Особливе значення має захист даних користувачів, доступ до яких здійснюється через системи авторизації та автентифікації. Ці два механізми забезпечують різні етапи контролю доступу, і їх правильна реалізація дозволяє мінімізувати ризики несанкціонованого доступу. Тому забезпечення надійної авторизації та автентифікації є актуальним науковим завданням.

Ціль дослідження

Дослідити різні системи авторизації та автентифікації, зробити науковий аналіз та запропонувати надійну систему автентифікації.

Системи авторизації та автентифікації, як основа забезпечення безпеки інформаційних систем

Автентифікація – це процес перевірки особи або системи, яка намагається отримати доступ до ресурсів. Іншими словами, автентифікація підтверджує, що користувач є тим, за кого себе видає. Найпоширенішими методами є:

- Що знає користувач: пароль або PIN-код.
- Що має користувач: токен, картка доступу.
- Що є у користувача: біометричні дані, такі як відбитки пальців або скан обличчя.

Авторизація, у свою чергу, визначає рівень доступу користувача після успішної автентифікації. Цей етап контролює, які ресурси доступні для використання і які дії дозволені. Наприклад, менеджер у фінансовій системі може мати доступ до даних про доходи, тоді як рядовий працівник – лише до власних облікових записів.

Сучасні системи часто використовують багатофакторну автентифікацію (MFA), що значно підвищує рівень безпеки. Це поєднання кількох факторів: паролю, токenu і біометричних даних. Використання MFA значно знижує ризик злому навіть при компрометації одного з факторів.

Додатково, застосовуються такі технології, як єдиний вхід (SSO) та керування ідентифікацією і доступом (IAM). SSO дозволяє користувачам входити в різні системи та сервіси через один обліковий запис, що зручно та підвищує продуктивність. IAM же забезпечує централізоване управління ролями та доступом, дозволяючи ефективно контролювати політику безпеки в організації.

Одна з основних проблем сучасних систем автентифікації – це забезпечення зручності для користувача без шкоди для безпеки. Біометричні дані, хоч і є зручними, можуть бути уразливими до атак на зразок підробки обличчя або відбитків пальців. Тому важливо інтегрувати біометричні методи із іншими способами автентифікації.

У майбутньому очікується активний розвиток таких технологій, як автентифікація за допомогою поведінкових моделей. Наприклад, аналіз звичок користувача під час введення тексту або використання пристроїв. Також активно розробляються системи, що базуються на квантовій криптографії, які гарантують абсолютну безпеку передачі даних. Для наочного представлення результатів дослідження наведемо графічне представлення. Так на рис. 1. наведено графік, який показує порівняння різних методів автентифікації за рівнем ризику.

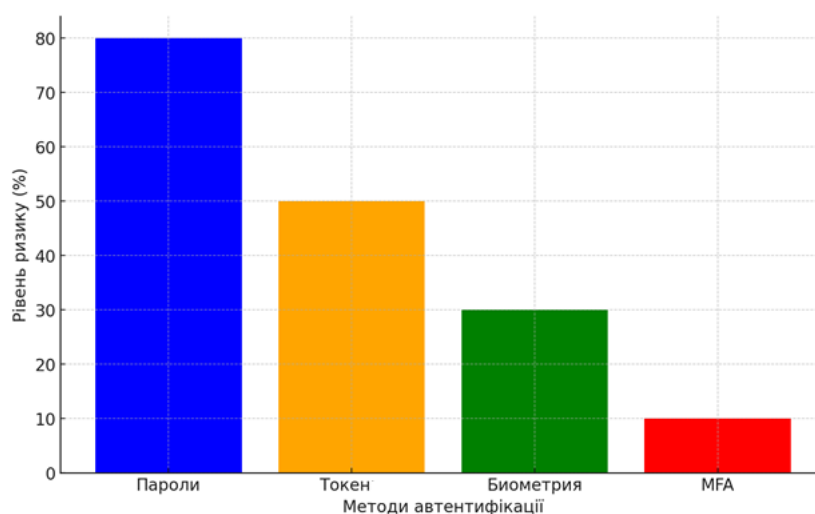


Рис. 1 Порівняння різних методів автентифікації за рівнем ризику

Аналіз наведеного графіку свідчить про те, що найбільш вразливим є парольна автентифікація, рівень ризику несанкціонованої автентифікації досягає 80%, на другому місці знаходяться метод автентифікації за допомогою токенів. Але метод автентифікації за допомогою токенів може забезпечити безпеку на рівні 50%. Біометричний метод, вже надає 70% безпеки. Самим безпечним є комбінований метод багатофакторної автентифікації.

Висновки

Системи авторизації та автентифікації залишаються ключовими елементами у захисті інформації. Їх інтеграція, адаптація до нових викликів та впровадження сучасних технологій дозволяє забезпечити надійний захист у цифровому середовищі. Дослідження довели, що завдяки використанню багатофакторної автентифікації та інноваційних методів, організації можуть ефективно протистояти сучасним кіберзагрозам.

Список використаних джерел:

1. Богдан А. С., Лаптев С. О., Лаптева Т. О., Кітура О. В. Ідентифікація та верифікація особистостей, як складова комплексної системи захисту об'єкта. XXVII Міжнародна науково-практична конференція «*Multidisciplinary academic research and innovation*», 25-28 мая 2021р. Амстердам, Нідерланди. С.674 – 680.
2. Крупенко С.В., Лаптев С.О., Лаптева Т.О., Кітура О.В. Побудова системи контролю та управління доступом за допомогою акустичного методу автентифікації та авторизації. «*Science of post-industrial society: globalization and transformation processes*» 04.06.2021 Вінниця, UKR - Відень, AUT. <https://ojs.ukrlogos.in.ua/index.php/grail-of-science/issue/archive>

Ключові слова: автентифікація, авторизація, токен, пароль, MFA.

Key words: authentication, authorization, token, password, MFA.

ЗАХИСТ ЧУТЛИВОЇ ІНФОРМАЦІЇ ОРГАНІЗАЦІЇ ПРИ ВИКОРИСТАННІ ХМАРНИХ СЕРВІСІВ

Чепурна Олена

Доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат фізико-математичних наук, доцент

Литвин Олександра

студентка магістратури 2 курсу, спеціальність 124 «Системний аналіз» Національного університету «Одеська юридична академія»

Використання хмарних сервісів стало невід'ємною частиною роботи багатьох організацій, від невеликих стартапів до великих корпорацій. Вони пропонують безліч переваг, таких як масштабованість, ефективність і зниження витрат, але водночас відкривають нові вразливості. Захист чутливої інформації у хмарних середовищах — це складне і багатогранне завдання, яке вимагає інтеграції сучасних технологій, глибокого розуміння ризиків та ретельного планування. Зрештою, будь-яка невдача у забезпеченні захисту може мати серйозні наслідки для репутації компанії, фінансової стабільності та довіри клієнтів [1].

Однією з основних проблем у хмарних середовищах є забезпечення конфіденційності даних, оскільки в таких умовах доступ до інформації часто

має не лише власник, але й сторонні постачальники послуг. Наприклад, у випадку з Capital One, який став публічним у 2019 році, витік даних понад 100 мільйонів клієнтів був пов'язаний з хмарною інфраструктурою. Вразливість виникла через помилку конфігурації, яку злоумисники змогли використати для доступу до даних, що зберігалися в обліковому записі AWS компанії. Цей випадок став знаковим, оскільки показав, наскільки небезпечними можуть бути навіть дрібні помилки у налаштуваннях. Безпека у хмарі є спільною відповідальністю постачальника та клієнта, а це означає, що як неухважність одного, так і іншого може мати серйозні наслідки [2].

Ключовим завданням є забезпечення шифрування даних як на етапі їхнього зберігання, так і під час передачі. Великі провайдери, такі як Amazon Web Services та Microsoft Azure, пропонують власні рішення для шифрування, але навіть при використанні цих інструментів клієнти повинні розуміти принципи їхньої роботи. Наприклад, AWS надає можливість шифрувати дані за допомогою сервісу Key Management Service (KMS), який дозволяє створювати, зберігати та керувати криптографічними ключами. Шифрування має критичне значення, оскільки навіть у разі несанкціонованого доступу до файлів злоумисники не зможуть їх розшифрувати без відповідних ключів. Це забезпечує додатковий рівень захисту, роблячи хмарні середовища більш стійкими до кібератак.

Іншим важливим аспектом є управління доступом. Занадто часто працівники отримують надмірні права доступу, що створює додаткові ризики, особливо в умовах роботи з віддаленими ресурсами. В організаціях, які користуються такими платформами, як AWS, Microsoft Azure або Google Cloud Platform, розроблено системи контролю доступу, які дозволяють налаштувати ролі та права доступу. Це дає змогу обмежити доступ працівників до лише тих ресурсів, які їм дійсно необхідні для виконання своїх обов'язків, що значно знижує ризик несанкціонованих дій [3].

Додатковий рівень захисту забезпечує багатофакторна аутентифікація (MFA). Це підхід, при якому користувач повинен пройти кілька етапів верифікації для доступу до облікового запису. Наприклад, працівник, який отримує доступ до важливих документів компанії в Google Cloud Platform, може додатково ввести код, надісланий на мобільний пристрій, або використовувати спеціальний додаток для підтвердження. Це дозволяє значно ускладнити завдання для потенційних злоумисників, оскільки навіть у разі викрадення пароля доступ до ресурсів залишиться заблокованим.

Моніторинг активності у хмарних середовищах також є важливим елементом безпеки. Хмарні провайдери, такі як AWS і Microsoft, надають інструменти для відстеження дій користувачів і ресурсів, дозволяючи організаціям не лише реагувати на підозрілі активності, але й запобігати їм. Наприклад,

якщо працівник завантажує великі обсяги інформації у незвичний час або з нової локації, система може згенерувати попередження, яке дозволить IT-відділу швидко реагувати на можливу загрозу. У деяких випадках організація може використовувати автоматизовані правила для обмеження доступу або блокування дій, що відхиляються від стандартних параметрів безпеки. Це дає змогу не лише вчасно виявляти проблеми, а й запобігати можливим порушенням.

Важливу роль у захисті інформації у хмарних середовищах відіграє модель Zero Trust, яка ґрунтується на принципі відсутності автоматичної довіри до жодного користувача чи пристрою. Це означає, що для кожного доступу до хмарних ресурсів вимагається підтвердження особи, а сам доступ постійно контролюється і перевіряється. Наприклад, Microsoft Azure активно впроваджує підхід Zero Trust, при якому система перевіряє кожну спробу доступу, незалежно від того, чи був цей користувач раніше аутентифікований. Такий підхід підвищує загальний рівень безпеки, зменшуючи можливість несанкціонованого доступу до критичних даних.

Також одним важливим аспектом є захист від внутрішніх загроз. Часто працівники компаній можуть випадково або навмисно створювати ризики для інформаційної безпеки. Наприклад, відомий випадок із Uber, коли працівник компанії випадково опублікував ключі доступу до облікового запису Amazon Web Services у публічному репозиторії GitHub. Це дозволило зловмисникам отримати доступ до конфіденційної інформації користувачів, що мало значний вплив на репутацію компанії. Для уникнення подібних ситуацій організаціям необхідно регулярно навчати працівників і впроваджувати суворі політики безпеки, які регламентують використання та обмін даними [4].

Загалом захист чутливої інформації у хмарних середовищах є важливим стратегічним завданням для будь-якої сучасної організації. Це завдання вимагає не лише використання передових технологій, але й створення культури безпеки всередині компанії, де кожен працівник усвідомлює свої обов'язки і відповідальність за збереження даних. У поєднанні з інструментами, які забезпечують автоматизацію процесів безпеки, систематичним моніторингом активності і ефективним управлінням доступом, організація може значно підвищити рівень захисту чутливих даних, використовуючи всі переваги хмарних технологій без ризику для безпеки.

Список використаних джерел:

1. Рудий С. В., Сєверінов О. В. Дослідження моделі безпеки при використанні хмарних сервісів. Проблеми інформатизації : десята міжнар. наук.-техн. конф, 2022. С. 61.
2. Банк Capital One піддався кібератаці, що торкнулася 106 млн клієнтів, 2019. URL: <https://interfax.com.ua/news/general/604594.html> (дата звернення: 25.10.2024)

3. Панченко Т., Тузова І., Тузов О., Чумак О. Хмарні сервіси та огляд їх постачальників. *Scientific Collection «InterConf+»*, 2024. №43 (193), С. 550–559.
4. Чепурна ОЄ Сучасні математичні методи оптимізації заходів кібербезпеки. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень: у 2 т.: матеріали Міжнар. наук.-практ. конф. 19 трав. 2023 р., Одеса: Юридика, 2023. Том 1. С. 618–621.*

Ключові слова: конфіденційність, хмарні сервіси, шифрування, управління доступом, Zero Trust.

Keywords: privacy, cloud services, encryption, access control, Zero Trust.

ПОШУК ВЕЛИКИХ ПРОСТИХ ЧИСЕЛ ПЕРЕВІРКОЮ ЗА ТЕСТОМ ФЕРМА НА ПЛАТФОРМІ CUDA

Чикунів Павло

доцент кафедри інформаційних технологій Національного університету
«Одеська юридична академія», кандидат педагогічних наук, доцент

Ковальський Олександр

студент Національного університету «Одеська юридична академія»

Дослідження прискорення пошуку великих простих чисел є актуальним через їхнє ключове значення для криптографії, теорії чисел та блокчейн-технологій. Ця задача сприяє розвитку алгоритмів, оптимізації процесів і ефективного використання обчислювальних ресурсів для підвищення безпеки та продуктивності криптографічних систем і транзакцій.

Тест на простоту чисел Ферма заснований на теоремі, яку сформулював П'єр Ферма в XVII столітті. Ця теорема стверджує, що якщо p є простим числом, ціле число a не ділиться на p , то вираз $a^{p-1} \equiv 1 \pmod{p}$ є правильним [1]. Для визначення, чи є число p простим, вибирається випадкове число a , яке менше за p . Перевіряється, чи задовольняє це число виразу $a^{p-1} \equiv 1 \pmod{p}$. Якщо вираз правильний, то число може бути простим, однак це не гарантія, що число дійсно просте. Якщо рівняння не виконується, то число p є складеним. Основним недоліком тесту Ферма є наявність псевдопростих чисел. Щоб покращити надійність тесту, виконують кілька повторів для різних випадкових значень a .

Асимптотична складність тесту Ферма залежить від кількості ітерацій з випадковими числами, над якими виконується операція швидкого піднесення числа до ступеня, для k ітерацій складність тесту становить $O(k(\log n)^3)$.

Аналіз досліджень [1-2] свідчить, що в останні роки зосереджено увагу на оптимізації алгоритмів пошуку простих чисел і тестів на їх простоту за допомогою паралельних та розподілених обчислень. Це відкриває перспективи подальшого вдосконалення процесу пошуку шляхом використання графічних процесорів.

Технологія GPGPU [2], яка дозволяє використовувати графічні процесори для загальних обчислень, набула широкого поширення завдяки високій швидкості обробки з використанням API, таких як NVIDIA CUDA чи ATI Stream Technology. Ще у 2007 році компанія NVIDIA представила платформу CUDA для роботи з графічними процесорами GeForce, що сприяло популяризації GPGPU, особливо у навчанні моделей машинного навчання та нейромереж [3]. Однак ця технологія також ефективна для паралельних обчислень загального призначення. Для інтеграції GPGPU у Visual Studio доступні інструменти, зокрема NVIDIA Toolkit CUDA, ATI Stream SDK, Alea GPU, ILGPU тощо.

Метою виконання роботи є дослідження ефективності систематичного пошуку великих простих чисел тестом Ферма на платформі CUDA.

Програми для CUDA складаються з основного коду, який виконується на центральному процесорі (CPU), та коду, що запускається на CUDA-ядрах графічного процесора (GPU). CUDA-ядра можна оптимізувати для паралельного виконання певних завдань. Платформа CUDA надає доступ до різних типів пам'яті GPU, таких як глобальна пам'ять, константна пам'ять, текстурна пам'ять і спільна пам'ять, що відкриває широкі можливості для налаштування та оптимізації обчислень.

Щоб реалізувати пошук великих простих чисел тестом Ферма з використанням платформи CUDA, потрібно рівномірно розподілити навантаження на блоки та потоки GPU для максимальної ефективності алгоритму.

Для дослідження ефективності платформи CUDA виконана програмна реалізація трьох версій тесту Ферма для пошуку простих чисел в діапазоні до десяти мільйонів: а) з використанням CUDA; б) у однопотоковому послідовному режимі; в) у багатопотоковому режимі з використанням бібліотеки TPL.

Аналіз метрик, отриманий за допомогою Concurrency Visualizer показав, що на платформі CUDA пошук простих чисел зайняв 6.5 секунд з навантаженням на CPU 14%, на GPU 11%. В послідовному режимі пошук тривав 46 секунд з навантаженням на CPU 8%, на GPU 0%. Багатопотокова реалізація тривала 5.7 секунд з навантаженням на CPU 33%, GPU 0%. Таким чином, застосування багатопотокового програмування можна вважати конкурентним по відношенню до CUDA.

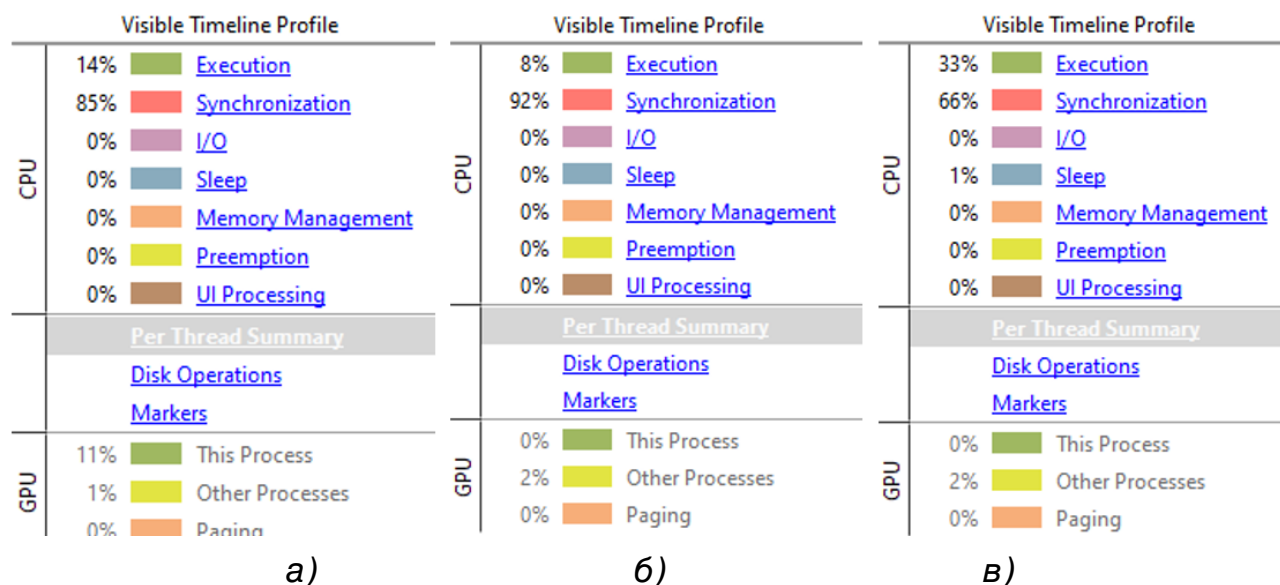


Рисунок 1 – Порівняння швидкодії реалізацій тесту Ферма: а) Nvidia CUDA, б) однопоточковий послідовний режим, в) багатопоточковий паралельний режим

Рівень міжпоточної синхронізації CUDA-реалізації сягає 85%, що свідчить про погану реалізацію міжпроцесорних та міжпоточкових обмінів даними.

Той факт, що багатопоточна версія програми виконалась швидше ніж CUDA-версія, можна пояснити тим, що GPU витрачав багато часу на синхронізацію результатів.

Виконана верифікація отриманих даних, тобто наявність хибних спрацьовувань (знайдене просте число насправді є складним) або пропуск простих чисел. Для CPU-реалізацій тестів на простоту виявлено до 60 пропусків та до 350 хибних спрацьовувань. Верифікація даних CUDA-реалізації тесту простоти Ферма показала відсутність пропусків та хибних спрацьовувань, тобто серед знайдених простих чисел немає складних.

Можна зробити висновок, що явним аутсайдером за часом виконання, завантаженням CPU та рівнем синхронізації, є послідовна реалізація тесту Ферма, що не дивно. Багатопотокова версія та CUDA-реалізація показали за часом виконання майже однакові результати, але наочно виглядає перенос навантаження з CPU на GPU. На думку авторів, подальші дослідження, зокрема при збільшенні діапазону пошуку до мільярда чисел та збільшення ступеня паралелізму алгоритму пошуку, можуть продемонструвати перевагу платформи CUDA.

Список використаних джерел:

1. Pevnev V., Yudin O., Sedlaček P., Kuchuk N. Method of testing large numbers for primality. Advanced Information Systems. – 2024. – Т. 8, № 2. – С. 99-106.
2. Månsson J. Comparative Study of CPU and GPGPU Implementations of the Sieves of Eratosthenes, Sundaram and Atkin. Master of Science in Engineering: Game and Software Engineering. 2021.

3. Яровий А.А., Кулик О.О., Арсенюк І.Р. Комп'ютерне моделювання процесу паралельного оброблення зображень на основі технологій OpenMP та NVIDIA CUDA. Оптико-електронні інформаційно-енергетичні технології. – 2015. – №2(30). – С. 33-39.

Ключові слова: прості числа, GPGPU, тест на простоту Ферма, потоки, синхронізація

Keyword: prime numbers, GPGPU, Fermat primality test, threads, synchronization

ГЕНЕРАТИВНИЙ ШТУЧНИЙ ІНТЕЛЕКТ В GAMEDEV

Трофименко Олена

*доцент кафедри інформаційних технологій Національного університету
«Одеська юридична академія», кандидат юридичних наук, доцент*

Бондаренко Максим

*студент факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

Індустрія відеоігор наразі є однією з важливих культурних та економічних явищ сучасності. Прогнозується, що до 2027 року доходи ігрової індустрії сягнуть 213.3 мільярдів доларів США [1]. Ігрова індустрія стрімко розвивається і з часом у ній постає проблема у генерації нових ідей. Зі збільшенням кількості ігор створювати нові унікальні ігри, що б використовували нові ігрові механіки та давали гравцям по новому відчуття ігрового процесу дедалі складніше.

Питання використання генеративного штучного інтелекту (ШІ) у відеоігровій індустрії відкриє нові можливості для автоматизованого створення контенту та адаптивних ігрових світів, оскільки дозволяє долати обмеження традиційного процесу розробки. Як впливає з назви, генеративний ШІ призначений для створення, наприклад, тексту, зображень, аудіо та відео. Це робиться за допомогою обробки природної мови (NLP), машинного навчання (ML) і навчальних даних. Враховуючи потенціал породжувальних моделей для динамічного відтворення ігрових середовищ, його детальніше дослідження може позитивно вплинути на розвиток відеоігор та ШІ.

Для розуміння можливостей від впровадження генеративного ШІ в процес розробки ігор (GameDev) доречно класифікувати області задач, в яких ШІ здатен виконувати певні завдання. До них можна віднести [2, 3]:

- створення та оброблення зображень;
- генерація та обробка відео з текстового опису та/або на основі зображення;
- обробка та створення аудіоефектів та музики;
- написання будь-якого тексту, в тому числі і програмний код засобами різних мов програмування;

- генерація 3D-моделей ігрових об'єктів;
- імітація створення голосів та озвучування тексту;
- аналіз зображень, відеозаписів в реальному часі тощо.

На сьогодні використання генеративного ШІ в ігровому процесі не є поширеним. Є лише деякі експериментальні демонстрації, які показують можливі перспективи розвитку такого виду використання ШІ. Так, технічна демонстрація Covert Protocol [4] була розроблена в результаті співпраці NVIDIA та Inworld AI з використанням ігрового рушія Unreal Engine 5. Covert Protocol демонструє можливості симуляції людської поведінки з використанням різних технологій ШІ. У ній гравець виступає в ролі приватного детектива, що розслідує справу за допомогою взаємодії з персонажами, за функціонування яких відповідають декілька ШІ, кожен з яких відіграє свою роль. Кожен ігровий досвід є унікальним, бо фрази гравців та їхні задачі заздалегідь не створюються. Вони є результатом комбінованої роботи Inworld SDK та рушія ШІ від Inworld [5]. Симуляція реалістичної поведінки та міміки ігрових персонажів реалізовано засобами фреймворка MetaHuman та технологій NVIDIA ACE, в які входить NVIDIA Riva Automatic Speech Recognition для розпізнавання мовлення [6] та NVIDIA Audio2Face для генерації реалістичної міміки персонажів по наявному аудіозапису [7].

Тим самим розвиток генеративного штучного інтелекту у сфері відеоігор відкриває нові можливості як для розробників, так і для гравців. Його використання зможе кардинально змінити сучасні уявлення про відеоігри та їх обмеження. Створення адаптивних світів з живим оточенням за простим запитом може стати майбутнім для відеоігрової індустрії.

Список використаних джерел:

1. Global Games Market Report 2024. *Newzoo*. URL: https://best-of-gaming.be/wp-content/uploads/2024/09/2024_Newzoo_Global_Games_Market_Report.pdf
2. Saerssenbek K., Chinibayeva T. Affective computing methods for simulation of action scenarios in video games. *Procedia Computer Science*. 2024. Vol. 231. P. 341-346. <https://doi.org/10.1016/j.procs.2023.12.214>.
3. Humble N. AI Supported Game Development: Exploring Opportunities and Challenges. *2nd Symposium on AI Opportunities and Challenges (SAIOC)*. (2024). <https://doi.org/10.13140/RG.2.2.30170.76480>.
4. Burnes A. NVIDIA Digital Human Technologies Bring AI Game Characters To Life. URL: <https://www.nvidia.com/en-us/geforce/news/nvidia-ace-gdc-gtc-2024-ai-character-game-and-app-demo-videos/>
5. Getting started. *InWorld*. URL: <https://docs.inworld.ai/docs/intro/>
6. NVIDIA Riva. *NVIDIA*. URL: <https://www.nvidia.com/en-us/ai-data-science/products/riva/>
7. Audio2Face Overview. *NVIDIA*. URL: <https://docs.omniverse.nvidia.com/audio2face/latest/index.html>

Ключові слова: штучний інтелект, ШІ, генеративний ШІ, GameDev, розробка ігор.

Keywords: Artificial intelligence, AI, Generative AI, GameDev, Game Development.

MESHU AI ЯК АЛЬТЕРНАТИВА ПРОГРАМАМ 3D МОДЕЛЮВАННЯ

Толокнов Анатолій

*асистент кафедри інформаційних технологій Національного університету
«Одеська юридична академія»*

Шляхтицький Дмитро

*студент 3-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

3D моделювання – це процес створення тривимірних об'єктів за допомогою комп'ютерних програм [1]. Однак з розвитком штучного інтелекту (ШІ) з'явилися нові інструменти, такі як Meshy AI, які пропонують альтернативні підходи до створення 3D моделей. Ці рішення можуть значно спростити процес моделювання і зробити його більш доступним для широкого кола користувачів.

Meshy AI – це платформа, яка використовує алгоритми машинного навчання для автоматизації процесу 3D моделювання. Завдяки цьому інструменту користувачі можуть генерувати тривимірні моделі за допомогою простих команд або візуальних інтерфейсів, що значно зменшує час та зусилля, необхідні для створення моделей [2].

Основні переваги Meshy AI:

- **Автоматизація процесу:** Meshy AI дозволяє автоматично створювати моделі на основі заданих параметрів або ескізів. Це зменшує необхідність в ручному моделюванні та пришвидшує робочий процес.
- **Доступність:** Застосування штучного інтелекту робить 3D моделювання більш доступним для людей без спеціальних навичок. Інтуїтивно зрозумілий інтерфейс дозволяє користувачам створювати моделі, не маючи попереднього досвіду.
- **Економія часу:** Автоматизація різних етапів, таких як текстурювання та освітлення, дозволяє значно скоротити час, необхідний для завершення проєктів.
- **Креативність:** Meshy AI може пропонувати ідеї та варіанти моделювання, що відкриває нові можливості для творчого самовираження.

У той час як традиційні програми 3D моделювання, такі як Blender [3], Autodesk Maya [4] і 3ds Max [5], вимагають від користувача глибоких знань та досвіду, Meshy AI пропонує більш спрощений підхід. Користувачі можуть генерувати складні моделі з мінімальними зусиллями, зосереджуючи увагу на креативності, а не на технічних деталях.

Meshy AI можна інтегрувати з популярними ігровими рушіями, такими як Unity та Unreal Engine, що дозволяє легко імплементувати згенеровані мо-

делі у проєкти. Це забезпечує гнучкість у використанні та оптимізує робочий процес для розробників.

3D моделювання стало важливим інструментом у багатьох галузях, від ігрової індустрії до архітектури та анімації. З розвитком штучного інтелекту (ШІ) з'являються нові платформи, такі як Meshy AI, які обіцяють спростити і оптимізувати процес моделювання. У порівнянні з традиційними програмами 3D моделювання, такими як Blender, Meshy AI пропонує інші можливості, які заслуговують на детальний аналіз.

1. Процес створення моделей.

Blender: Ця програма забезпечує широкий спектр інструментів для 3D моделювання, анімації, текстурювання та рендерингу. Хоча Blender є потужним інструментом, він вимагає значних зусиль для освоєння, особливо для новачків. Користувачі повинні вивчити численні комбінації клавіш, меню та налаштування для створення та редагування моделей.

Meshy AI: Використовуючи алгоритми машинного навчання, Meshy AI автоматизує процес створення моделей. Користувач може задати прості параметри або завантажити ескіз, а платформа згенерує 3D модель на основі цих даних. Це дозволяє заощадити час і зменшити навчальний бар'єр, що робить моделювання доступнішим для тих, хто не має технічного досвіду.

2. Текстурювання та освітлення.

Blender: Програма пропонує детальні інструменти для текстурювання та налаштування освітлення. Користувачі можуть вручну налаштовувати текстури, освітлення та матеріали, щоб досягти високоякісних візуальних ефектів. Однак цей процес може бути складним і вимагати часу.

Meshy AI: Штучний інтелект автоматизує текстурювання та освітлення, пропонуючи згенеровані текстури відповідно до стилю та типу моделі. Це спрощує процес, зменшуючи час на ручну роботу, але може обмежувати творчість для тих, хто хоче мати повний контроль над деталями.

3. Креативність та гнучкість.

Blender: Забезпечує велику свободу для творчих рішень, дозволяючи користувачам створювати складні та індивідуальні моделі. Однак, щоб реалізувати свої ідеї, користувачі повинні мати глибокі знання про функції програми.

Meshy AI: Хоча Meshy AI дозволяє швидко генерувати моделі, креативність користувача може бути обмежена. Автоматизація процесів може призвести до стандартних рішень, які не завжди відображають унікальність задуму. Однак, у поєднанні з ручним редагуванням, Meshy AI може слугувати потужним інструментом для натхнення.

4. Інтеграція з платформами

Blender: Програма підтримує експорт моделей у різні формати, що дозволяє інтегрувати їх у популярні рушії, такі як Unity та Unreal Engine. Однак цей процес може бути більш складним і вимагати додаткових налаштувань.

Meshy AI: Інтеграція з ігровими рушіями, такими як Unity та Unreal Engine, є простішою, оскільки моделі генеруються вже в оптимізованих форматах. Це забезпечує швидший робочий процес для розробників, дозволяючи їм зосередитися на створенні ігор, а не на підготовці моделей.

Список використаних джерел:

1. Fabio Remondino, Sabry El-Hakim, Image-based 3D Modelling: A Review. URL: https://www.researchgate.net/publication/227786426_Image-based_3D_Modelling_A_Review.
2. Meshy AI. Text to 3D – Features. URL: <https://www.meshy.ai/features/text-to-3d>
3. Blender Official Site. URL: <https://www.blender.org/>
4. Autodesk Maya: Create expansive worlds, complex characters, and dazzling effects. URL: <https://www.autodesk.com/products/maya/overview>
5. Autodesk 3ds Max: Create massive worlds and high-quality designs. URL: <https://www.autodesk.com/products/3ds-max/overview>

Ключові слова: 3D моделювання, Meshy AI, Blender, штучний інтелект, ігрові рушії, Unity, Unreal Engine, текстурування, моделі, автоматизація.

Key words: 3D modeling, Meshy AI, Blender, artificial intelligence, game engines, Unity, Unreal Engine, texturing, models, automation.

РОЗРОБКА ІНТЕРАКТИВНИХ СИСТЕМ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Мільченко Олександр

аспірант 1-го курсу факультету факультету кібербезпеки та інформаційних технологій Національного університету "Одеська юридична академія"

Розробка інтерактивних систем на основі штучного інтелекту (ШІ) для підтримки прийняття рішень у складних середовищах є важливим напрямком сучасних технологій. Такі системи допомагають користувачам ефективно аналізувати великі обсяги даних, знаходити необхідні закономірності та робити обґрунтовані рішення у невизначених умовах.

Основні компоненти інтерактивних систем для підтримки прийняття рішень на основі ШІ:

1. **Збір і обробка даних.** Збір та обробка даних є ключовими компонентами інтерактивних систем для підтримки прийняття рішень на основі штучного інтелекту (ШІ). Зібрані дані виступають фундаментом, на якому будується аналітика, прогнозування та інші функції ШІ.

2. Аналіз даних та прогнозування. Використовуючи методи машинного навчання, системи ШІ можуть виявляти потрібні закономірності у великих наборах даних. Це допомагає передбачати бажанні результати та ризики.

3. Візуалізація результатів. Інтерактивні системи повинні надавати інтуїтивно зрозумілі інтерфейси для користувачів, щоб вони могли легко сприймати результати виконаного аналізу. Візуалізації, такі як графіки, діаграми, теплові карти, можуть допомагати користувачам швидше приймати рішення.

4. Моделювання та симуляції. Деякі системи підтримки рішень дозволяють моделювати можливі сценарії розвитку подій, що дозволяє оцінювати наслідки різних варіантів рішень.

5. Інтерактивність. Користувачі можуть безпосередньо взаємодіяти із системою, налаштовувати параметри аналізу та отримувати адаптовані рекомендації на основі конкретних потреб або умов середовища [1].

Системи підтримки рішень на основі ШІ можуть застосовуватися в різних галузях, включаючи:

- управління ризиками в фінансовому секторі;
- планування логістики та операцій у виробництві;
- медицину для діагностики та вибору лікувальних стратегій;
- керування ресурсами в енергетиці або сільському господарстві.

Також до теми розробки інтерактивних систем на основі ШІ для підтримки прийняття рішень можна додати кілька важливих аспектів:

Адаптивність і навчання. Сучасні системи повинні бути здатні до самонавчання на основі нових даних. Це дозволяє їм постійно покращувати свої рекомендації і точність, підлаштовуючись до мінливих умов середовища. Наприклад, в умовах швидких змін, таких як стан фінансових ринків або кліматичних умов, система може швидко адаптувати процес свого навчання.

Співпраця людини і ШІ. У складних ситуаціях повна автоматизація може бути небажаною або неможливою, тому важливо, щоб системи підтримували тісну взаємодію з користувачами. Кінцевий користувач повинен мати змогу впливати на процес прийняття рішень, комбінуючи власну інтуїцію з аналітичними можливостями ШІ [2].

Етичні аспекти та прозорість. Прийняття рішень на основі ШІ вимагає забезпечення етичності, прозорості та відповідальності. Важливо, щоб такі системи були прозорими у пропонованих рішеннях, щоб користувачі розуміли, на основі яких даних і алгоритмів було прийняте рішення. Це допоможе запобігти упередженням і зловживанням [3].

Інтеграція з іншими системами. Інтерактивні системи на основі ШІ повинні легко інтегруватися з існуючими інформаційними системами, включаючи ERP (Enterprise Resource Planning), CRM (Customer Relationship

Management), системи моніторингу, тощо. Це дозволяє забезпечити доступ до різномірних даних і максимізувати ефективність прийняття рішень.

Безпека та конфіденційність даних. Оскільки інтерактивні системи підтримки рішень обробляють великі обсяги даних, часто конфіденційних або чутливих, питання кібербезпеки і захисту даних мають бути пріоритетними. Забезпечення належного рівня безпеки допоможе уникнути витоків даних та маніпуляцій з боку сторонніх осіб.

Масштабованість. Системи повинні бути здатні ефективно працювати з різними обсягами даних і масштабуватися відповідно до потреб користувача чи організації. В умовах зростання кількості інформації система повинна зберігати свою продуктивність та оперативність.

Часова критичність. У деяких середовищах рішення мають бути прийняті дуже швидко, як, наприклад, у випадку катастроф або фінансових коливань. Тому важливо, щоб система могла працювати в реальному часі, надаючи рекомендації без затримок.

Висновок

З огляду на все вищесказане, можна стверджувати, що розвиток інтерактивних систем на основі ШІ дозволяє зменшити кількість людських помилок, підвищити ефективність і точність рішень та сприяти кращому управлінню складними системами різного призначення. Ці системи стають ключовим інструментом в умовах складних і невизначених середовищ. Вони поєднують збір та аналіз даних, візуалізацію результатів, моделювання можливих сценаріїв і забезпечують адаптивність. Важливою є співпраця людини і ШІ, а також увага до етичних аспектів, прозорості, безпеки та конфіденційності даних. Інтеграція з іншими системами та масштабованість дозволяють таким системам ефективно допомагати людині приймати рішення в різних галузях.

Список використаних джерел:

1. Dix, A., Finlay, J., Abowd, G., & Beale, R. (2003). Human-Computer Interaction. *Pearson Education*. URL: https://paragnachaliya.in/wp-content/uploads/2017/08/HCI_Alan_Dix.pdf (дата звернення: 09.10.2024).
2. Amershi, S., Cakmak, M., Knox, W. B., & Kulesza, T. Power to the People: The Role of Humans in Interactive Machine Learning. AI Magazine, 35(4), 2014. [DOI: 10.1609/aimag.v35i4.2513]. URL: <https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/2513> (дата звернення: 10.10.2024).
3. European Commission (2019). Ethics Guidelines for Trustworthy AI. URL: <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1> (дата звернення 10.10.2024).

Ключові слова: інтерактивні системи, штучний інтелект, ШІ, прийняття рішень у складних середовищах, ефективний аналіз даних

Keywords: interactive systems, artificial intelligence, AI, decision-making in complex environments, effective data analysis

Науковий керівник: к.т.н., доцент **Задерейко О.В.**

ПРИНЦИПИ АНАЛІЗАТОРА ПЕРЕНАПРАВЛЕННЯ DOH-ТРАФІКУ

Федчук Тарас

*аспірант, асистент кафедри Безпеки інформаційних технологій
Національного університету «Львівська політехніка»*

Багато країн запроваджують цензуру та блокування веб-сайтів відповідно до національного законодавства Існує безліч способів блокування веб-контенту [1-2]. Цей процес підробки DNS показано на Рис. 1, а. Використання DoH дозволяє обійти цей метод блокування, що можуть використовувати інтернет-провайдери, залишаючи користувачів неусвідомленими щодо їхньої потенційно незаконної активності.

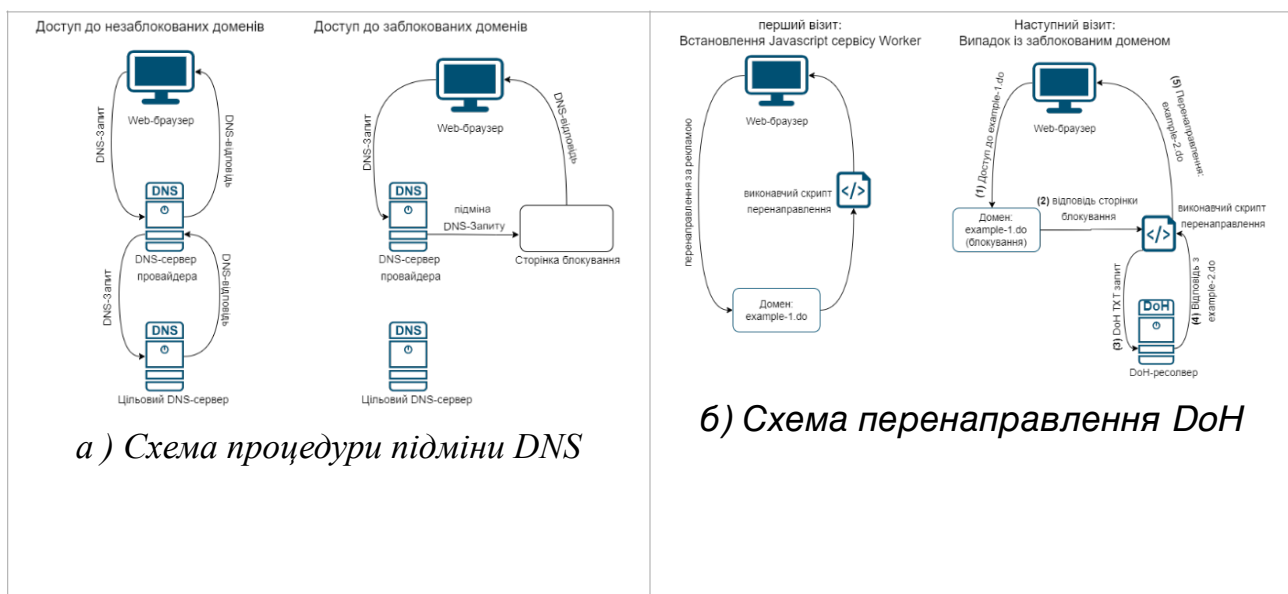


Рис. 1 Схеми маніпуляції DNS-трафіком і його перенаправлення

Комунікація через C2 є одним з найпоширеніших зловживань незашифрованим DNS. Приклад такого зловживання DoH описала Huntresslabs [4]: JSON-запит на основі TXT для DKIM здійснювався через dns.google.com. Відповідь TXT містила IP-адреси зовнішніх серверів, які завантажували додатковий контент для встановлення зв'язку з C2. Обидва підходи використовують популярність Google DNS, тому доступність цього ресолвера ймовірно висока.

Сценарій зловживання 1: Зміна клієнта для доступу до заблокованих сайтів.

Клієнт прагне встановити зв'язок із сервером, однак пряма комунікація заблокована, що реалізується через підробку DNS на локальному DNS-ресолвері. Клієнтська програма змінюється, щоб використовувати DoH для обходу блокувань і отримання робочої IP-адреси сервера, що дозволяє встановити прямий зв'язок.

Ізраїльський сайт sdarot.tv, розробив плагін на Python для медіапрограми Kodi. Плагін використовує доменні імена, закодовані в base64, для трансляції. Після трансляції всі URL-адреси містять IP-адреси напряду, обходячи DNS-ресолвери операційної системи і провайдерів.

Сценарій зловживання 2: Перенаправлення з використанням DoH на web-сайті.

Цей сценарій зловживання включає три сторони: клієнта, сервер і домен C2. Клієнт переходить на сервер або спрямовується на нього. Під час першого відвідування сервер змінює браузер клієнта, налаштовуючи механізм перенаправлення. Згодом сервер ідентифікується як шкідливий, і DNS-підробка блокує доступ до нього.

Для моніторингу доменних імен, пов'язаних з обраною IP-адресою казино, використовувалась система пасивного DNS Security Trails. Як видно з Рис. 2, а понад 100 доменів були зареєстровані для одного і того ж веб-сайту згідно з даними пасивного DNS.

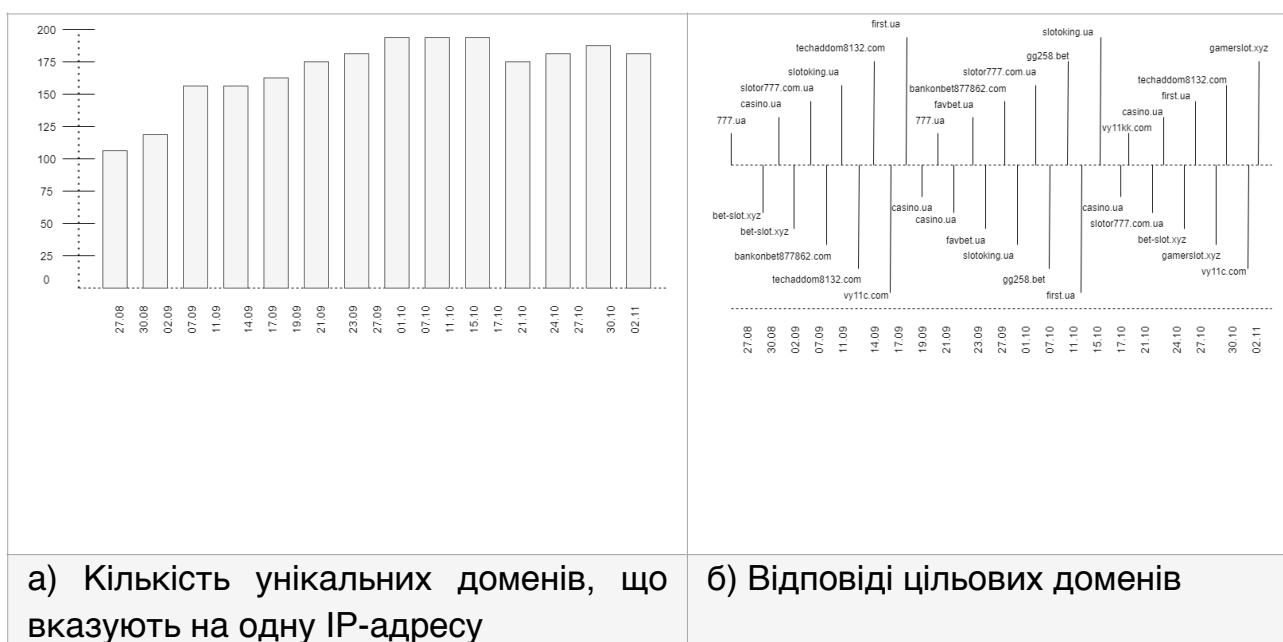


Рис. 2. Статистичні дані по цільових доменах

Стратегія швидкої зміни доменних імен майже аналогічна інфраструктурі C2 шкідливого ПЗ, яка використовує генерацію доменних імен (DGA). Однак казино залежать від користувачів, які не бажають перевіряти підключення до сотень доменів. Для цього створено інфраструктуру перенаправлення, яка забезпечує доступ до функціонуючого розблокованого сайту казино.

Service Worker для перенаправлення встановлюється в браузері, коли користувач відвідує сайт казино. При наступному доступі користувача до сайту, перенаправлення активується. В усіх аналізованих web-сайтах перенаправник здійснював DoH-запит типу TXT до домену C2 та отримував закодований у base64 JSON-об'єкт.

За вказівками від C2, сервіс worker перевіряє, чи заблоковано домен. Якщо доступ дозволено, користувач переходить на web-сторінку, а у випадку блокування перенаправляється на цільовий домен через JavaScript, де встановлюється новий JavaScript Service Worker. Це дозволяє користувачам запам'ятовувати лише початковий URL і завжди отримувати доступ до активного незаблокованого web-сайту. Загальна схема перенаправлення представлена на Рис.1, б.

Відповіді C2 було досліджено з плином часу за допомогою системи Security Trails Passive DNS System. Усі унікальні доменні імена, що використовувалися з 27 серпня до 2 листопада 2024 року, показані на Рис. 2, б. За спостережуваний період цільовий домен змінювався 35 разів.

Підхід на основі DoH може стати альтернативою техніці домен-фронтингу [5] (метод обходу цензури з використанням багатосервісної інфраструктури), що вже заборонений багатьма великими провайдерами CDN. Масштабне впровадження сценарію 2 може призвести до створення прихованої мережі, схожої на «dark web». Це дозволяє web-сайтам швидко змінювати свої домени й IP-адреси (протягом хвилин), не знижуючи швидкості для користувачів.

Сценарій зловживання 3: використання DoH у рекламі та спам-кампаніях.

У цьому сценарії зловживання залучені клієнт і домен C2. Клієнт ненавмисно ініціює один або кілька DoH-запитів до домену C2, на які отримує відповіді з JavaScript-кодом або його фрагментами. Після цього клієнт виконує цей код і діє згідно з інструкціями C2. Відмінність від сценарію 2 полягає в тому, що ці скрипти не використовують JavaScript Service Worker API, а отримують JavaScript-код безпосередньо з каналу C2.

У випадку спам-кампаній HTML-документ надсилається як вкладення (або як MIME-частина) і вимагає відкриття в поштовому клієнті. У проаналізованих випадках відповідь завжди містила скрипт перенаправлення з ці-

льовою URL-адресою, вбудованою в код, що використовує JavaScript window API. Потім JavaScript-інтерпретатор виконував цей код, ініціюючи перенаправлення.

Ці приклади демонструють реальні сценарії зловживання DoH. Сценарій 1 використовує DoH для обходу обмежень DNS, сценарій 2 — для виявлення підробки DNS та блокування вебсайтів, забезпечуючи перенаправлення. Також у сценарії 2 DoH використовується як канал C2 для розрізнення заблокованих сторінок і активних вебсторінок. Сценарій 3 застосовує DoH як канал C2 для завантаження шкідливого коду. Відмінності між сценаріями також показані в таблиці 1. (СБК – секретні багатофункціональні канали, C2 – доступ і комунікація C2).

Таблиця.1. Резюме характеристик представлених сценаріїв зловживання.

	Сценарій 1	Сценарій 2	Сценарій 3
Потребує спеціалізованого	+		
DoH як прихований канал для обходу DNS	+	+	+
DoH як C2 канал		+	+
Отримання шкідливого коду з			+
Орієнтовано тільки на web-		+	
Виявлення закриття web-сайту		+	
Категорія зловживання	СБК	C2	C2

Висновок

У результаті дослідження роботи аналізатора перенаправлення DoH-трафіку було розроблено сценарії, що є робочими прикладами механізмів на основі DoH, які: 1) були проаналізовані із застосуванням відповідного зловмисного ПЗ, 2) можуть бути корисними для майбутніх досліджень у галузі кібербезпеки, та 3) легко використовуються для імітації різних видів зловмисної діяльності в рамках навчання моделей машинного навчання. Кожен із сценаріїв демонструє унікальний спосіб використання DoH: сценарій 1 — для обходу обмежень DNS, сценарій 2 — для виявлення втручання в DNS і блокування сайтів із подальшим перенаправленням, а також для розпізнавання дійсних вебсторінок через DoH як C2. Сценарій 3 також використовує DoH як C2, але для отримання шкідливого коду.

Список використаних джерел:

1. J. L. Hall, M. D. Aaron, S. Adams, B. Jones, and N. Feamster. Survey of Worldwide Censorship Techniques. Internet Engineering Task Force, Internet-Draft draft-hall-censorship-tech-07. 2019. URL: <https://datatracker:ietf.org/doc/html/draft-hall-censorship-tech-07> (Last accessed: 21.08.2024).
2. R. Deibert, J. Palfrey, R. Rohozinski, J. Zittrain. Access denied: The practice and policy of global internet filtering. The MIT Press, 2008 (Last accessed: 07.09.2024).
3. Korobeynikova T, Fedchuk T. Overview of secure access to domain name system resources. Information Technologies and Computer Engineering 21(1), 40-53. 2024. DOI: 10.31649/1999-9941-2024-59-1-40-53.
4. J. Hammond. Hiding in plain sight. Part 2,” Sep 2020. URL: <https://blog:huntresslabs.com/hiding-in-plain-sightpart-2-dfec817c036f>
5. D. Fifield, C. Lan, R. Hynes, P. Wegmann, and V. Paxson. Blockingresistant communication through domain fronting. Proceedings on Privacy Enhancing Technologies. Vol. 2015, no. 2, pp. 46 – 64. Jun. 2015. URL: <https://content.sciendo.com/view/journals/popets/2015/2/article-p46.xml>
6. Pink, a botnet that competed with the vendor to control the massive infected devices. Jul 2021. URL: <https://blog:netlab:360.com/pink-en/> (Last accessed: 11.10.2024).
7. E. Rubin, N. Tucker. Technation: Pitango launches seventh venture fund with projected \$175 million. Dec 2020. URL: <https://www:haaretz.com/israel-news/business/technation-1:5474071> (Last accessed: 15.10.2024).
8. Anonymous. The collateral damage of internet censorship by dns injection. ACM SIGCOMM Computer Communication Review, Jun 2012. Vol. 42, no. 3, p. 21–27.

Ключові слова: Система доменних імен, web-сайт перенаправлення, сценарій зловживання DoH, C2-комунікація.

Keywords: Domain Name System (DNS), redirect website, DoH abuse scenario, C2 communication.

ВБУДОВАНІ РУШІЇ 3D МОДЕЛЮВАННЯ ЯК ЗАМІНА ПОВНИХ ПРОГРАМ ДЛЯ МОДЕЛЮВАННЯ

Толокнов Анатолій

*асистент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»*

Бондарева Анна

*студентка 3-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

3D моделювання – це процес створення тривимірних об’єктів за допомогою спеціалізованих комп’ютерних програм. Ці моделі можуть знаходити застосування в різних галузях, таких як ігрова індустрія, анімація, архітектурна візуалізація та наукові дослідження. Процес моделювання охоплює кілька ключових етапів: створення форм, текстурування, налаштування освітлення та анімацію об’єктів [1].

Основні етапи 3D моделювання:

- створення базової геометрії: моделі починаються зі створення простих форм, які згодом деталізуються.
- текстурювання: накладення текстур на поверхні моделей для надання їм реалістичного вигляду.
- освітлення: налаштування джерел світла для створення ефекту об'єму та глибини.
- анімація: додавання руху до моделей для їх інтерактивності та динаміки.

Програмне забезпечення для 3D моделювання:

- Blender: безкоштовна програма з відкритим вихідним кодом, що пропонує потужні інструменти для моделювання, анімації та рендерингу [2].
- Autodesk Maya: професійний інструмент, широко використовуваний в індустрії анімації та ігор для створення складних моделей та анімацій [3].
- 3ds Max: популярний серед архітекторів та дизайнерів завдяки своїм можливостям для візуалізації та моделювання [4].
- Cinema 4D: інтуїтивно зрозуміла програма, часто використовувана в моушн-дизайні та візуальних ефектах [5].

Рушії для 3D моделювання, такі як Unity, Unreal Engine 5 та Roblox, надають можливості для створення об'єктів безпосередньо в ігровому середовищі. Це полегшує робочий процес, дозволяє швидко створювати прототипи та оптимізувати використання ресурсів [6].

Unity (рис. 1):

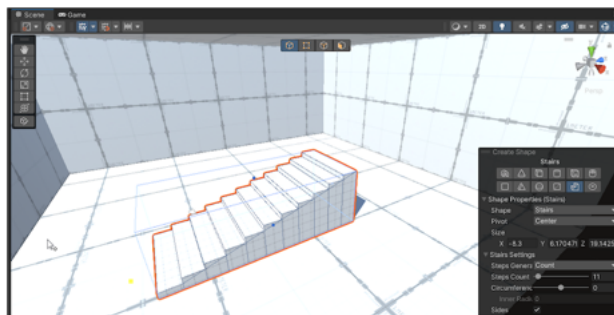


Рис. 1. Вбудований моделер Unity.

- ProBuilder: інструмент в Unity, що дозволяє створювати і редагувати 3D-об'єкти безпосередньо в редакторі. ProBuilder дозволяє швидко створювати рівні, будівлі та інші об'єкти з простими формами, надаючи гнучкість у моделюванні [7].
- Mesh Tool: дозволяє редагувати геометрію об'єктів, працюючи з вершинними даними [8].

Unreal Engine 5 (рис. 2):

- Modeling Mode: режим моделювання, що дозволяє створювати та редагувати 3D-моделі прямо в редакторі [9].

· Geometry Editing Tools: інструменти редагування геометрії для модифікації моделей [10].

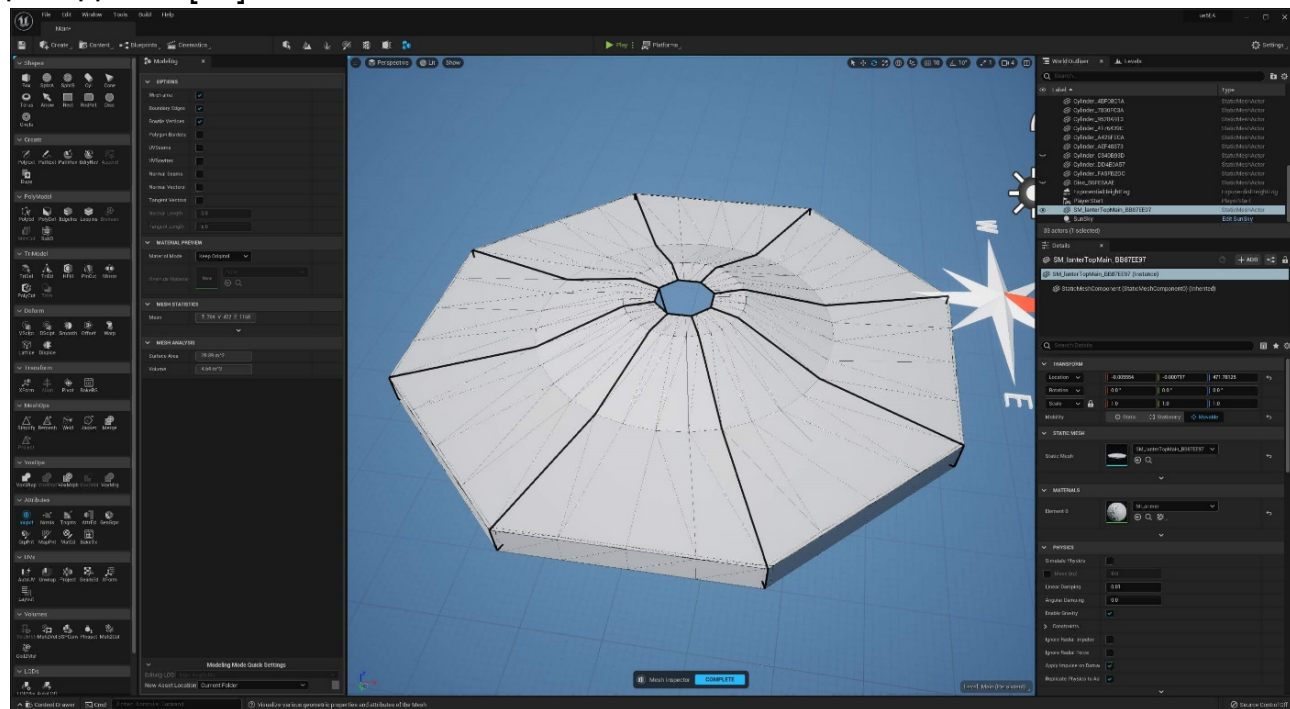


Рис. 2. Вбудований моделер UE5.

Roblox (рис. 3):

Part Instances: Моделі створюються за допомогою частин, які можна комбінувати для створення складних об'єктів [11].

Union i Negate: Інструменти для об'єднання частин або створення специфічних деталей [12].

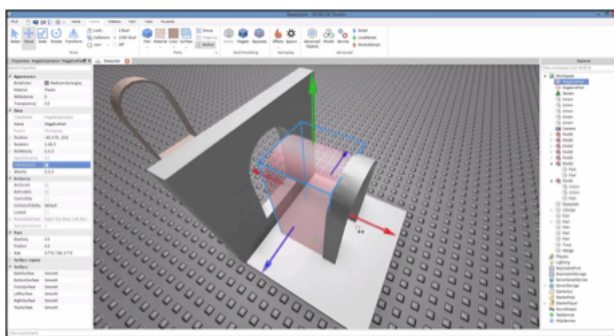


Рис. 3. Вбудований моделер Roblox Studio.

Вбудовані інструменти для 3D моделювання, такі як Unity, Unreal Engine 5 та Roblox, пропонують ефективні альтернативи традиційним програмам для моделювання. Вони забезпечують зручний і інтегрований підхід до створення ігор та об'єктів, відкриваючи нові можливості для творчості та інновацій у гейм-дизайні [13].

Список використаних джерел:

1. Fabio Remondino, Sabry El-Hakim, Image-based 3D Modelling: A Review. URL: https://www.researchgate.net/publication/227786426_Image-based_3D_Modelling_A_Review.

2. Blender Official Site. URL: <https://www.blender.org/>
3. Autodesk Maya Official Site. URL: <https://www.autodesk.com/products/maya/overview>
4. 3ds Max Official Site. URL: <https://www.autodesk.com/products/3ds-max/overview>
5. Cinema 4D Official Site. URL: <https://www.maxon.net/en/cinema-4d>
6. Unity Official Site. URL: <https://unity.com/>
7. Unity ProBuilder. URL: <https://unity.com/features/probuilder>
8. Unity Mesh Tool. URL: <https://docs.unity3d.com/Manual/MeshEditing.html>
9. Unreal Engine 5 Official Site. URL: <https://www.unrealengine.com/en-US/unreal-engine-5>
10. UE5 Modeling Mode. URL: <https://docs.unrealengine.com/5.0/en-US/modeling-mode-in-unreal-engine-5/>
11. Roblox Developer Hub. URL: <https://developer.roblox.com/en-us/>
12. Roblox Union and Negate. URL: <https://developer.roblox.com/en-us/articles/unioning-parts>
13. Game Developer. URL: <https://www.gamedeveloper.com/>

Ключові слова: 3D моделювання, тривимірні об'єкти, комп'ютерні програми, ігрова індустрія, анімація, архітектурна візуалізація, наукові дослідження.

Key words: Unity, Unreal Engine 5, Roblox, 3D modeling, three-dimensional objects, computer programs, game industry, animation, architectural visualization, scientific research.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ЗАДАЧАХ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ

Кухаренко Сергій

доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Стрілець Михайло

магістр факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Кібертероризм став одним із ключових викликів для безпеки країн і корпорацій, з огляду на високу ефективність методів атак, що спрямовані як на приватний сектор, так і на державні установи. У цьому контексті, штучний інтелект постає потужним інструментом, що здатний допомогти у виявленні, аналізі та протидії кібертерористичним загрозам.

Робота зі штучним інтелектом (ШІ) і машинним навчанням (МН) використовується для вирішення низки задач у сфері кібербезпеки, оскільки системи на основі ШІ аналізують величезні обсяги даних для виявлення аномальних патернів і прогнозування потенційних кіберзагроз, забезпечуючи ефективне реагування, зокрема це виявлення аномалій, моніторингу мережевого трафіку, ідентифікації загроз у режимі реального часу та автоматизації реакції на інциденти. Одним із основних методів ШІ у кібербезпеці є машинне нав-

чання, яке дає змогу алгоритмам самонавчатися на основі даних про попередні кіберінциденти, покращуючи їх точність і швидкість виявлення загроз.

Завдяки штучному інтелекту зараз стало більш зручніше отримувати обробку та аналіз звітів безпеки, моніторинг та аналіз трафіку, фіксування вторгнень у систему, прогнозування загроз тощо [1].

Також для аналізу великих обсягів даних, зокрема для обробки тексту, відео та інших медіафайлів, які можуть містити індикатори кібертерористичної діяльності застосовуються методи глибинного навчання [2].

Наприклад, платформа Darktrace, що використовує алгоритми машинного навчання та глибинного аналізу даних, дозволяє виявляти підозрілі активності в мережі та реагувати на потенційні загрози автоматично. Компанія застосовує принципи «імунної системи», яка самонавчається і адаптується до нових загроз, вивчаючи «поведінковий патерн» нормальної роботи мережі. При виявленні будь-якої аномалії, яка може вказувати на загрозу, система автоматично сповіщає адміністратора або ж навіть блокує небезпечний трафік у режимі реального часу.

Аналіз поведінки користувачів (User Behavior Analytics, UBA) – один із важливих напрямків використання ШІ у кібербезпеці. UBA дозволяє системам вивчати та фіксувати нормальні шаблони поведінки користувачів у мережі та виявляти відхилення, які можуть вказувати на зловмисну активність. Завдяки UBA, можна виявити, наприклад, коли користувачі здійснюють незвичайні дії, такі як спроби доступу до даних у незвичний час доби або завантаження великих обсягів даних [3].

Один із реальних прикладів цього підходу – продукт Splunk, який використовує машинне навчання для моніторингу мереж і виявлення аномалій у поведінці користувачів. Splunk допомагає організаціям відстежувати мережеві активності та виявляти дії, що можуть вказувати на потенційну кібертерористичну активність, наприклад, спроби викрадення конфіденційних даних. Завдяки вбудованому ШІ, платформа швидко ідентифікує підозрілі патерни поведінки та генерує автоматичні попередження для відповідальних осіб.

Штучний інтелект також застосовується для прогнозування та виявлення нових загроз за допомогою кіберрозвідки (Cyber Threat Intelligence, CTI). Використовуючи методи глибинного навчання та обробки природної мови (Natural Language Processing, NLP), системи ШІ можуть аналізувати відкриті джерела інформації, такі як форуми, соціальні мережі, Dark Web тощо, для виявлення потенційних загроз і індикаторів компрометації. Такі системи сканують великі обсяги даних і знаходять згадки про вразливості, атаки або інші ризики.

Компанія Recorded Future пропонує рішення, яке об'єднує ШІ з методами кіберрозвідки, надаючи організаціям можливість отримувати інформацію про нові загрози в режимі реального часу. Продукт використовує ШІ для аналізу величезних обсягів даних з різних джерел і надає аналітику про потенційні загрози, допомагаючи своєчасно реагувати на можливі атаки.

Одним із основних завдань у протидії кібертероризму є забезпечення швидкого реагування на інциденти. Штучний інтелект сприяє автоматизації цього процесу, дозволяючи зменшити час між виявленням загрози та її нейтралізацією. Алгоритми ШІ можуть автоматично реагувати на певні типи атак, такі як фішингові атаки або спроби проникнення до мережі.

Платформа IBM QRadar використовує штучний інтелект для автоматичного аналізу інцидентів, визначення їх пріоритетності та рекомендацій щодо подальших дій. QRadar поєднує методи аналітики та машинного навчання для класифікації інцидентів за рівнем ризику, що дозволяє фахівцям з безпеки швидко зосередитися на найнебезпечніших загрозах.

Кібертероризм часто націлений на критичну інфраструктуру, таку як енергетичні системи, транспортні мережі та фінансові установи. Ці об'єкти мають особливу важливість для національної безпеки, тому їхній захист є пріоритетом. ШІ дозволяє моніторити і аналізувати великі масиви даних, що генеруються критичними об'єктами, для виявлення потенційних загроз.

У сфері енергетики відома американська компанія Siemens активно використовує ШІ для моніторингу енергосистем. Їхні рішення, розроблені спільно з компанією SparkCognition, дозволяють виявляти кібератаки на об'єкти енергетичної інфраструктури та вживати заходів щодо їх нейтралізації. Такі технології особливо важливі для захисту від атак типу «удар віддаленого коду» (Remote Code Execution), які можуть призвести до серйозних наслідків, таких як відключення електропостачання або збій систем управління [4].

Штучний інтелект відіграє надзвичайно важливу роль у сучасних технологіях протидії кібертероризму. Він може значно збагатити стратегію кібербезпеки, додаючи необхідний захист від серйозних кіберзагроз. Використання методів машинного навчання, аналізу поведінки, кіберрозвідки та автоматизації реагування на інциденти значно підвищує ефективність і швидкість реагування на загрози. У той же час, розвиток ШІ створює нові виклики, такі як потенційна небезпека використання ШІ зловмисниками для удосконалення атак, а також етичні питання щодо автоматизації та приватності. Проте, застосування ШІ у сфері кібербезпеки продовжує розширюватися, надаючи нові інструменти для захисту суспільства від кіберзагроз.

Список використаних джерел:

1. Застосування ШІ у кібербезпеці: роль та переваги. URL: <https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi>
2. Черевко К. Штучний інтелект як інструмент протидії злочинності. Вісник Кримінологічної асоціації України, 2023. №28(1). С. 124-133.
3. Мужанова Т., Лехомінова С., Якіменко Я. Мордас І. Технології моніторингу й аналізу діяльності користувачів у запобіганні внутрішнім загрозам інформаційній безпеці організації», Кібербезпека: освіта, наука, техніка, 2021. № 1(13). С. 50–62.
4. Ільєнко А., Ільєнко С., Яковенко О., Галич Є., Павленко В. Перспективи інтеграції штучного інтелекту в системи кібербезпеки. Кібербезпека: освіта, наука, техніка, 2024. №1(25). С. 318-329.

Ключові слова: кібербезпека, кібертероризм, захист даних, штучний інтелект, аналіз даних, загроза, інцидент.

Keywords: cybersecurity, cyber terrorism, data protection, artificial intelligence, data analysis, threat, incident.

ОРГАНІЗАЦІЯ ТА РОЗГОРТАННЯ СИСТЕМИ РЕЗЕРВНОГО КОПІЮВАННЯ З ВИКОРИСТАННЯМ BORG

Бойко Віктор

*доцент кафедри кібербезпеки Національного університету
«Одеська юридична академія», кандидат технічних наук*

Хорус Олександр

*студент 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

У сучасному світі, коли обсяг і значення даних зростають дуже швидкими темпами, питання резервного копіювання стає критично важливим для забезпечення безперервності ведення бізнесу та захисту інформаційних активів[1]. Втрата важливих даних приведе до серйозних фінансових та репутаційних ризиків, тому компанії все частіше шукають надійні та ефективні рішення для організації систем резервного копіювання[2].

Для більшості організацій актуальною проблемою є надмірний обсяг даних, що накопичувався з часом. Це не тільки збільшує витрати на зберігання, але й досить сильно ускладнює процес резервного копіювання та відновлення. Багато традиційних рішень не беруть до уваги дедуплікацію і шифрування, що також значно підвищує ризики витоку або дублювання даних.

Резервне копіювання баз даних (далі БД) вимагає врахування певних специфічних вимог, щоб забезпечити їх цілісність, доступність та можливість швидкого відновлення. Основні вимоги включають в себе[3, 4]:

1. Цілісність даних: резервне копіювання повинно забезпечувати цілісність даних, зберігаючи усі залежності та зв'язки між таблицями, індексами

та іншими елементами БД. Це особливо важливо для транзакційних баз, де навіть незначне порушення цілісності може призвести до досить серйозних проблем з даними при відновленні.

2. Мінімальний час простою: процес резервного копіювання не повинен створювати досить тривалих перерв у роботі системи. Це досить важливо для БД, які обробляють запити в режимі реального часу, таких як електронна комерція чи банківські системи. Підтримка функцій, як-от "гаряче резервне копіювання" (backup online), дозволяє зберігати дані без зупинки у роботі.

3. Швидкість відновлення: важливим параметром резервного копіювання є швидкість відновлення БД. У разі збою в роботі або втрати даних, резервне копіювання має бути структурованим так, щоб забезпечити якнайшвидше відновлення для мінімізації простою. Зазвичай використовуються інкрементні копії або диференційне резервне копіювання для зменшення потрібного часу для відновлення.

4. Частота резервного копіювання: регулярне створення резервних копій має здійснюватися відповідно до критичності даних і частоти їх змін. Наприклад, критично важливі бази даних можуть потребувати щогодинного резервного копіювання, тоді як менш важливі системи можуть потребувати щоденного або щотижневого резервного копіювання.

5. Масштабованість і оптимізація місця зберігання: резервне копіювання баз даних має бути масштабованим, щоб відповідати зростанню обсягу даних. Це включає використання технологій дедуплікації та стиснення для зниження потреби в сховищі без втрати інформації.

6. Шифрування і безпека: резервні копії мають бути захищені від несанкціонованого доступу, особливо якщо вони містять надважливу, конфіденційну або особисту інформацію. Використання шифрування як під час створення резервних копій, так і під час їхнього зберігання, забезпечує безпеку даних.

7. Відстеження та моніторинг процесу резервного копіювання: необхідно мати інструменти для моніторингу й аудиту процесів резервного копіювання, щоб швидко виявляти збої або недоліки в їх реалізації та вчасно вживати заходів. Це також передбачає тестове відновлення даних для перевірки працездатності копій.

8. Автоматизація та планування: автоматизовані процеси резервного копіювання допомагають значно зменшити ризик людського фактору і дозволяють встановлювати чіткий розклад для створення копій у зручний для нас час, не зупиняючи роботу всієї системи.

9. Збереження декількох копій: важливо зберігати декілька копій резервних даних, зокрема і в різних фізичних чи хмарних локаціях (стратегія 3-

2-1), щоб забезпечити додатковий рівень безпеки на випадок локальних збоїв або катастроф.

10. Регулярне тестування відновлення: тестування відновлення є важливим елементом перевірки ефективності процесу резервного копіювання, що допомагає виявити проблеми і забезпечити працездатність резервних копій у разі потреби.

Одним із таких рішень є Borg[5], який забезпечує гнучкість, ефективність і надійність процесу резервного копіювання. Borg дозволяє забезпечити резервне копіювання з використанням сучасних методів дедуплікації, інкрементного збереження даних і шифрування, що робить його особливо актуальним для організацій, які потребують високого рівня захисту і збереження великих обсягів інформації.

Система Borg Backup (або просто Borg) є інструментом для створення резервних копій даних з особливим акцентом на ефективність, безпеку та економію місця для зберігання [6,7]. Borg підтримує інкрементне резервне копіювання, дедуплікацію та шифрування, що робить її потужним рішенням для управління резервними копіями великих обсягів даних. Основні принципи її роботи включають:

1. Інкрементне резервне копіювання: Borg дозволяє створювати резервні копії лише змінених або нових файлів, що значно зменшує час і обсяг даних для кожної нової копії. Завдяки цим методам Borg знижує навантаження на систему та економить простір у сховищі.

2. Дедуплікація даних: Borg реалізує дедуплікацію на рівні блоків, що означає, що система виявляє та зберігає унікальні блоки даних лише один раз. Це дозволяє зменшити загальний обсяг збережених резервних копій, особливо у випадках, коли копіюються схожі файли або файли, що містять однакові блоки (наприклад, різні версії одного документа).

3. Стиснення даних: Borg дозволяє налаштувати стиснення даних для зменшення об'єму збережених резервних копій. Підтримуються кілька алгоритмів, що дає змогу обрати кращий варіант залежно від вимог до продуктивності та місця зберігання.

4. Шифрування: Borg підтримує опціональне шифрування резервних копій за допомогою алгоритму AES-256, що забезпечує конфіденційність даних. Шифрування гарантує, що навіть у разі доступу до сховища, сторонні особи не зможуть прочитати дані без відповідного ключа.

5. Принцип неперервності версій: Borg дозволяє зберігати безліч версій резервних копій, що дає змогу відновити дані з будь-якої точки в часі. Кожна версія створюється з урахуванням дедуплікації, тому навіть багатоверсійне резервне копіювання не потребує значних обсягів дискового простору.

6. Відновлення даних: Borg забезпечує досить швидке відновлення даних завдяки індексації та організації сховища. Завдяки підтримці інкрементних копій і дедуплікації, Borg може досить ефективно відновлювати дані, зберігаючи лише необхідні блоки.

7. Сумісність із різними платформами: Borg є платформонезалежним інструментом і підтримує різні операційні системи, що робить його гнучким для впровадження в різних ІТ-інфраструктурах.

Резервне копіювання є основним елементом захисту даних для сучасних організацій, і його важливість досить важко переоцінити. Розгортання ефективної системи резервного копіювання, такої як Borg, дозволяє не лише захистити інформаційні активи компанії, але й забезпечити безперервність бізнесу, знизити фінансові та репутаційні ризики, пов'язані з можливою витоку даних. Borg надає потужні можливості для інкрементного копіювання, дедуплікації, стиснення та шифрування, що робить його ефективним рішенням для забезпечення надійного резервного копіювання при значній економії дискового простору.

Список використаних джерел:

1. A. Abdi, H. Bennouri and A. Keane, "Cyber Resilience, Risk Management, and Security Challenges in Enterprise-Scale Cloud Systems: Comprehensive Review," 2024 13th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2024, pp. 1-8, doi: 10.1109/MECO62516.2024.10577956.
2. O. P. Suman, L. K. Saini and S. Kumar, "Cloud-Based Data Protection and Secure Backup Solutions: A Comprehensive Review of Ensuring Business Continuity," 2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 2023, pp. 821-826, doi: 10.1109/ICSCCC58608.2023.10176503.
3. Kiss Á., Nehéz K. Efficiency and Performance Evaluation of Open-Source Backup Tools: An Empirical Analysis of Storage Footprint and Execution Time // Production Systems and Information Engineering. 2023. Vol. 11, No. 1. P. 7. DOI:10.32968/psaie.2023.1.7.
4. Tirmazi M., Barker A., Deng N., Haque M., Qin Z., Hand S., Harchol-Balter M., Wilkes J. Borg: The Next Generation // In Proceedings of the 15th European Conference on Computer Systems (EuroSys '20). Heraklion, Crete, Greece: ACM, 2020. pp. 30:1–30:14. DOI: 10.1145/3342195.3387517.
5. BorgBackup – Deduplicating archiver with compression and authenticated encryption [Електронний ресурс]. – Режим доступу : <https://www.borgbackup.org/> (дата звернення: 2024-10-20). – Назва з екрана.
6. Keep It Safe Linux Magazine [Електронний ресурс]. – Режим доступу : [https://www.linuxpromagazine.com/Issues/2023/267/BorgBackup/\(offset\)/3](https://www.linuxpromagazine.com/Issues/2023/267/BorgBackup/(offset)/3) . (дата звернення: 2024-10-20). – Назва з екрана.

Ключові слова: відмовостійкі системи, резервне копіювання, керування сховищем, узгодженість даних, безпека даних, конфіденційність даних, резервне копіювання даних.

Keywords: fault tolerant systems, backup, distributed databases, storage management, data consistency, data security, data privacy, redundant data backup.

РОЗРОБКА ПРОГРАМНОЇ СИСТЕМИ З ЕЛЕМЕНТАМИ ШІ ДЛЯ ОЦІНКИ НАСТРОЇВ ТА ПОВЕДІНКИ КОРИСТУВАЧІВ ТА ВИЯВЛЕННЯ БОТ-АКТИВНОСТІ

Ольвінська Аліна

*студентка 1 курсу магістратури кафедри інженерії програмного
забезпечення Інституту комп'ютерних систем, Національного університету
«Одеська Політехніка»*

Петрова Марія

*студентка 1 курсу магістратури кафедри інженерії програмного забезпечення
Інституту комп'ютерних систем Національного університету
«Одеська Політехніка»*

Лойшин Максим

*студент 1 курсу магістратури кафедри інженерії програмного забезпечення
Інституту комп'ютерних систем Національного університету
«Одеська Політехніка»*

У наш час питання кібербезпеки та кібергігієни є актуальними не тільки з боку захисту персональних даних користувачів та критично важливих систем, але й з боку звичайної взаємодії між користувачами та інформацією, яку вони отримують у мережі. Останні роки в Україні, у зв'язку з повномасштабним вторгненням та загальним розвитком інформаційних технологій, відсоток людей, які отримують інформацію в першу чергу з інтернет-джерел відчутно виріс. Згідно з дослідженням Київського міжнародного інституту соціології (KMIC) у вересні-жовтні 2023 80% респондентів були регулярними користувачами інтернету, що користуються їм 3 та більше годин на день. До того ж зросла й частка регулярних користувачів інтернету серед людей похилого віку: з 32% до 50%. При цьому частка людей похилого віку, що не є користувачами мережі знизилась з 48% до 30% [1].

Як результат така діджиталізація населення призводить й до змін у переліку джерел з яких воно отримує інформацію. Згідно з опитуванням соціологічної групи “Рейтинг” на вересень 2024 року 47% респондентів зазначили, що отримують інформацію та новини з Telegram, 26% - з YouTube, 15% - з українських онлайн-медіа, новини та дописи у Facebook є джерелом перевіреної інформації для 12% опитаних. Таким чином інтернет-джерела на цей рік вже переважають над традиційними медіа, такими як телебачення, радіо, газети та журнали. Усе це породжує відповідні ризики, такі як зростання дезінформації та мізінформації серед населення, а також зріст кіберзлочинності у вигляді фішингу та інших типів шахрайства, що помітно серед респондентів опитування. Згідно з ним 89% людей вважають дезінформацію

серйозною проблемою. Соціальні мережі 53% респондентів вважають основним джерелом дезінформації, за ними йдуть месенджери - 35% [2].

Через це відкритим залишається питання про надання звичайним користувачам методів та інструментів для виявлення та попередження їх про можливу взаємодію з підозрілим контентом. Таким контентом можна вважати дописи, що ставлять на меті викликати у користувача конкретні емоції, користувачі з відсутньою або абнормальною поведінкою та дописи або повідомлення з невідомими посиланнями. Виявлення такого контенту потребує враховувати різні ознаки та швидко підлаштовуватися під зміни тактик злочинців.

Для проектування та подальшої розробки такого програмного інструменту необхідно розібрати методи досягнення необхідного функціоналу. Для виявлення ботоферм або одиноких бот-акаунтів та попередження про небезпечність взаємодії з таким користувачем потрібно знайти та проаналізувати як даний акаунт взаємодіє з іншими сторінками та дописами. Одним таким методом виявлення бот-мереж є виявлення фрагментів бот-мереж на основі аналізу мережевого трафіку. У цьому методі активність мережі становить собою зважений граф, де вершини виступають у ролі хостів мережі, а ребра — їх зв'язку. Ваги ребер описують вірогідність того, що два вузли представляють частину спільної бот-мережі [3]. Таке виявлення схожої активності допоможе виявляти усю частину бот-мережі та швидко і зручно нейтралізувати її вузли, а також попереджати про її активність звичайних користувачів.

Для оцінки емоційної забарвленості допису або коментаря можна використати методи сентимент аналізу. Хоча вони використовуються загалом компаніями для оцінки настроїв та відношення клієнтів до своїх продуктів, сентимент аналіз можна також використовувати для виявлення інформаційно-психологічних впливів [4]. Для вирішення такого завдання краще використовувати нейронні мережі. Наприклад, використання Convolutional Neural Networks у комбінації з Long Short-Term Memory - ConvLSTM або CNN+Bi-LSTM - показує підвищену точність та перевершує традиційні моделі для сентимент аналізу завдяки захопленню як локальних, так і послідовних особливостей тексту [5][6].

Отже, нами пропонується система на основі ШІ для оцінки настроїв та поведінки користувачів та виявлення підозрілої бот-активності. Дана система може бути представлена у вигляді розширення для браузерів, що буде автоматично помічати дописи або коментарі, а також акаунти інших користувачів та пояснювати причини через які дані тексти або акаунти можна вважати підозрілими. Також користувачі самі зможуть додатково помічати контент який вважають підозрілим, що допоможе розвивати модель ШІ та будувати

базу даних підозрілих акаунтів. Така система допоможе не тільки звичайним користувачам, але й надасть інструменти для боротьби з бот-атаками власникам інтернет-ресурсів.

Для аналізу тональності дописів та коментарів та наявності серед них інформаційно-психологічного впливу будемо використовувати модель ШІ для лінгвістичного аналізу. Її основний функціонал у системі це обробка тексту та визначення його тону, визначення мовних структур та ключових слів, а також виявлення нових мовних шаблонів та перевірка тексту на шаблонність. Такі функції не тільки допомагають зрозуміти тон та зміст тексту, але й допомагають самій моделі розвиватися та адаптуватися до постійних змін у мові.

Існуватиме 3 основні модулі системи:

1. Джерела даних – збір та базове впорядкування даних
2. Компонент ШІ – основний модуль, який проводитиме аналіз даних в кілька етапів з метою отримання якомога точнішої характеристики
3. Виведення результатів – модуль, який підсумовуватиме отримані з попереднього етапу, та представлятиме аналіз у вигляді, зрозумілому для користувача.

Своєю чергою компонент ШІ також складається з трьох підмодулів:

1. Підготовка даних – процес аналізу коментарів, які не несуть ніякого змістовного сенсу, є просто набором символів і, власне, не піддаються подальшому контекстному аналізу або аналізу настрою, а також розбиття даних на групи та вибірки для подальшого тренування
2. Аналіз текстів – основний етап, на якому проводяться 3 загалом незалежних аналізи різними моделями (визначення настрою коментаря, контекстної залежності від допису та визначення можливості авторства ШІ у цьому коментарі). Кожний з цих аналізів формує свою оцінку для кожного з коментарів, яка пізніше і перейде до модуля, відповідального за виведення результатів у зрозумілому вигляді
3. Постобробка - допоможе визначити нові шаблони або оновити старі, для того, щоб відстежувати повторення поведінки ботів або тригер-слів, які викликають активність такої мережі.

Зважаючи на великі обсяги даних, які обробляються, велику кількість шаблонів, які мають зберігатися та оброблятися, постійне їх оновлення та додавання, а також високе навантаження на систему через використання засобів ШІ/МН, найдоцільнішим буде використання хмарної архітектури.

На момент проєктування системи припускається, що вона носитиме суто інформаційний характер, тобто всі важливі рішення з приводу подальших маніпуляцій з потенційно небезпечними коментарями, користувачами та мережами прийматимуться відповідальною за модерування особою. Але на-

далі для системи існує перспектива розвитку для автоматизованого приховування або видалення підозрілих коментарів та користувачів та блокування бот-мережі, тим самим зменшуючи необхідність втручання людини та знижуючи час реакції на бот-атаки.

Список використаних джерел:

1. Аналітичний звіт «Думки і погляди населення України щодо державних електронних послуг у 2023 році». UNDP. URL: <https://www.undp.org/uk/ukraine/publications/analitichnyy-zvit-dumky-i-pohlyady-naselennya-ukrayiny-shchodo-derzhavnykh-elektronnykh-posluh-u-2023-rotsi> (дата звернення: 30.10.2024)
2. Успіх чи ні? Як українці оцінюють реформування органів правопорядку та підтримку ЄС. Група «Рейтинг». URL: <https://ratinggroup.ua/research/ukraine/uspik-chi-ni-yak-ukrayinci-ocinyuyut-reformuvannya-organiv-pravoporyadku-ta-pidtrimku-yes.html> (дата звернення: 30.10.2024)
3. Нічепорук А. О., Нічепорук А. А., Нічепорук Ю. О., Казанцев А. Д. Метод виокремлення фрагментів бот-мереж на основі аналізу мережевого трафіку. Вісник Хмельницького національного університету. Серія: «Технічні науки». 2020. № 2. С. 141—149. DOI: 10.31891/2307-5732-2020-283-2-141-149 (дата звернення: 31.10.2024)
4. Шингалов Д. В., Мелешко Є. В., Минайленко Р. М., Резніченко В. А. Метод автоматичного аналізу тональності контенту у соціальних мережах для виявлення інформаційно-психологічних впливів. Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. 2017. Вип. 30. С. 196-202. URL: http://nbuv.gov.ua/UJRN/znpkntu_2017_30_29 (дата звернення: 01.11.2024).
5. Makin A. Modern Approaches in Sentiment Analysis Models for Reviews. 2024. DOI: 10.13140/RG.2.2.35746.03521 (дата звернення: 01.11.2024)
6. Jang Y., Park J., Kim S. Word2Vec and SVM Fusion for Advanced Sentiment Analysis. Journal of Information Science, vol. 45, no. 4, pp. 564-577. 2019. DOI: 10.1177/0165551519837184 (дата звернення: 01.11.2024)

Ключові слова: кібербезпека, штучний інтелект, аналіз настроїв, виявлення ботів, дезінформація

Keywords: cybersecurity, artificial intelligence, sentiment analysis, bot detection, disinformation

Науковий керівник: *к.і.н., доцент кафедри інженерії програмного забезпечення Прокоп Ю. В.*

ЗАСТОСУВАННЯ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ КОМП'ЮТЕРНОГО ЗОРУ

Артем Ткачук

студент 3 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Розглянемо використання згорткових нейронних мереж (CNNs) для задач комп'ютерного зору з особливим акцентом на виявленні та відстеженні

об'єктів у реальному часі. За допомогою CNNs стає можливим автоматизувати процес виявлення об'єктів на відео або подібному зображенні, що є необхідним у багатьох галузях, таких як охорона, медицина, автомобільна промисловість тощо.

Однією з найбільш ефективних і широко використовуваних технологій виявлення об'єктів є YOLO (You Only Look Once), яка дозволяє визначати об'єкти та їхні контури за допомогою кадрів. Це допомагає розділити їх на категорії і відповідно назвати, що важливо для розпізнавання одного об'єкта від іншого, наприклад, обличчя і статі, і навіть частин тіла, таких як вуха, ніс, очі і так далі. Виявлення об'єктів у реальному часі здійснюється за допомогою технології YOLO, яка застосовується для відстеження об'єктів. Виявлення об'єктів здійснюється за допомогою кадру, а YOLO визначає характеристики об'єкта та присвоює йому ім'я. Модель використовує збір даних за допомогою бази даних YOLO Cvg Weights, включаючи ім'я об'єкта, для ідентифікації в реальному часі вхідних об'єктів користувачів і людей, таких як обличчя, стать, вуха, ніс, очі тощо. Особливістю цієї технології штучного інтелекту є диверсифікація об'єктів і здатність виявляти деталі з великою деталізацією; робота моделі швидка і ефективна, не перевантажує систему і додатки і споживає мало обчислювальних ресурсів. Див. приклад за ілюстрації нижче:

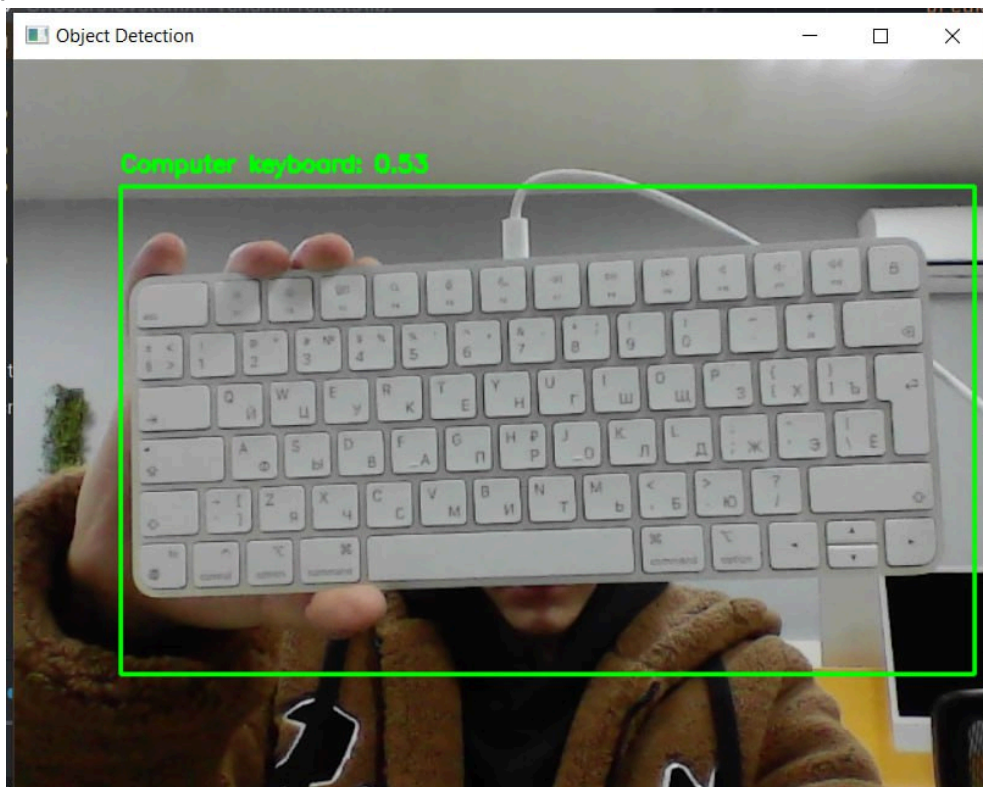


Рис. Розпізнавання об'єкта завдяки веб камері в режимі реального часу

Знову ж таки, для підвищення швидкості роботи мережі, а також для підтримки коректності виявлення об'єктів, включена база даних YOLO з по-

передньо навченими вагами (YOLO Cvg Weights), яка містить ознаки різноманітних об'єктів. Таким чином, в режимі реального часу система здатна ідентифікувати багато об'єктів і людей, що корисно, наприклад, для контролю доступу, а також для аналізу поведінки.

Модель YOLO має перевагу в одному аспекті - вона швидка та ефективна. Модель має дуже низьке обчислювальне навантаження, що дозволяє використовувати її на слабких пристроях, таких як смартфони або низькопродуктивні ноутбуки.

Для ілюстрації функціонального використання згорткових нейронних мереж було використано ідентифікацію об'єктів за допомогою веб-камери в реальному часі. Розпізнавання обличчя та інших об'єктів у кадрі також можна ідентифікувати за допомогою алгоритму комп'ютерного зору, який включає YOLO.

Отже, згорткові нейронні мережі для розпізнавання об'єктів є популярним напрямком у багатьох галузях для розробки системи розпізнавання об'єктів. Це може бути використано в обробці даних безпеки, моніторингу та розробці інтелектуальних систем, які потребують високошвидкісного аналізу та ідентифікації об'єктів у реальному часі.

Список використаних джерел:

1. Бойко В., Василенко М., Слатвінська В. Програмування за допомогою систем генеративного штучного інтелекту: ризики та виклики. *Інформаційні технології та суспільство*. 2023. № 2 (8), С. 18–26. DOI: <https://doi.org/10.32689/maup.it.2023.2.2> URL: <http://journals.maup.com.ua/index.php/it/article/view/2664> (дата звернення: 08.11.2024).

Ключові слова: згорткові нейронні мережі, розпізнавання обличчя, YOLO, комп'ютерний зір, обробка зображень у реальному часі.

Keywords: згорткові нейронні мережі, розпізнавання обличчя, YOLO, комп'ютерний зір, обробка зображень у реальному часі.

Науковий керівник: доктор філософії, асистент кафедри кібербезпеки
Слатвінська В.М.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАХИСТУ ВІД КІБЕР-ЗАГРОЗ ІНФОРМАЦІЙНИХ МОДЕЛЕЙ СКЛАДНИХ СИСТЕМ

Куклінова Софія

студентка 1 курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасний стан побудови інформаційних моделей складних систем потребує отримання достатньо точних значень параметрів на етапі проектування і коригування під час їх експлуатації. Також зазначимо, що коригування параметрів інформаційних моделей зумовлене необхідністю досягнення

режиму, що відповідає оптимальному значенню цільової функції для наявного поля змінних величин. Це в свою чергу вимагає методологічно точної основи для перевірки достовірності моделі та її фрагментів на етапі проектування, формування інформаційних вимог, які необхідно перевіряти в процесі експлуатації.

Так, класичні описи деяких економічних моделей складних систем та цільових функцій зазвичай формулюються як системи алгебраїчно-лінійних рівнянь. А сама задача опису зводиться до вирішення системи лінійних рівнянь, що дозволяє отримати аналітикам неточні результати.

Зазначимо, що використання таких методів ставить перед науковцями нові виклики. Постає питання не тільки про те, наскільки точно модель складної системи відображає реальність, а й про те, як інтерпретувати результати моделювання і чи можна їм довіряти у прийнятті управлінських рішень.

Отже, у зв'язку зі швидким розвитком інформаційних технологій, виникає гостра необхідність удосконалення класичних підходів до побудови моделей. Для отримання більш точних прогнозів треба використовувати більш складні обчислювальні методи і алгоритми.

На сучасному етапі побудова інформаційних моделей складних систем вимагає інтеграції класичних методів із сучасними підходами, такими як штучний інтелект (ШІ) та машинне навчання, для підвищення точності, гнучкості та адаптивності моделей.

ШІ є саме системою, яка здатна оперувати знаннями, вивчати методи розв'язання задач, моделювати людську вищу нервову діяльність та приймати рішення методом розв'язання задач, які потребують людського розуміння [1, с. 360]. ШІ дозволяє автоматизувати процеси аналізу, що знижує ймовірність людських помилок та значно підвищує ефективність процесу побудови моделей.

Загальновідомо, що однією з ключових переваг використання ШІ в аналізі складних систем є можливість швидкої обробки та аналізу великих обсягів даних. У складних технічних системах або економічних моделях накопичуються великі масиви інформації, що можуть змінюватись у часі або залежати від різних зовнішніх факторів.

Традиційні методи аналізу не завжди здатні ефективно справлятися з такими обсягами даних, тоді як алгоритми ШІ можуть ідентифікувати приховані закономірності та тренди, пропонуючи оптимальні рішення [2, с.384].

ШІ дозволяє покращити процес прогнозування моделей складних систем. А завдяки машинному навчанню, ці моделі можуть «вчитися» на історичних даних та адаптуватися до нових умов. Це особливо важливо для си-

стем, де зміни можуть бути швидкими та непередбачуваними, наприклад у сфері забезпечення кібернетичної безпеки енергетичної галузі. [3, 4]

Сучасні електричні системи керуються за допомогою комп'ютерних систем. Людина не може обробити обсяг даних, що надходять з усіх елементів системи одночасно та контролювати всі параметри власноруч. Проведений аналіз наукової літератури показав, що з розвитком енергетики та технологій енергосистеми стають все більш складними і потребують оптимізації для забезпечення їх стабільної та ефективної роботи [5 - 9].

Адже питання про використання енергії актуальні для всіх періодів існування людства. Так, однією з цілей сталого розвитку до 2030 року є забезпечення загального доступу до недорогих, надійних, стійких і сучасних джерел енергії і збільшення частки енергії з відновлюваних джерел [10].

Зазначається, що станом на 01.05.24 прямі збитки енергетичного сектору України перевищили 16,1 млрд. дол. США. Найбільші втрати, спричинені руйнуванням об'єктів генерації електроенергії склали 8,5 млрд. дол. США, ліній електропередач склали 2,1 млрд. дол. США. Непрямі збитки енергетичного сектору оцінюються майже в 40,4 млрд. дол. США, основна частка — це втрачені доходи енергетичних компаній — 39,9 млрд. дол. США. Решта — витрати на розбір завалів і демонтаж пошкоджених об'єктів — \$0,5 млрд. дол. США [11].

Зазначимо, що енергетика є однією з ключових галузей сучасної економіки, яка вимагає ефективного управління ресурсами, безперебійного постачання енергії та забезпечення надійної кібербезпеки. Зростання кількості кібератак на енергетичні системи вимагає впровадження надійних систем захисту. Кіберзагрози можуть включати як проникнення в інформаційні системи, так і атаки на фізичні елементи інфраструктури, що може призвести до відключення енергопостачання.

З розвитком інформаційних технологій та цифрових рішень побудова складних інформаційних систем в енергетиці стала необхідністю для досягнення цих цілей. Інформаційні системи в цій галузі охоплюють та вирішують широкий спектр завдань: від моніторингу та управління енергетичними мережами до прогнозування споживання енергії та виявлення аномалій в роботі їхньої інфраструктури.

Використання ШІ в сфері кібербезпеки, відкриває нові можливості для підвищення точності, гнучкості та ефективності складних систем. Завдяки своїй здатності швидко обробляти великі обсяги даних, прогнозувати загрози та адаптуватися до змін. Саме тому використання ШІ зможе допомогти захистити критичну інфраструктуру держави від кібератак, а також дозволить мінімізувати їх потенційні наслідки.

Використання ШІ може значно прискорити визначення незвичайної поведінки в енергосистемі, що може вказувати на проведення потенційної кібератаки або на імовірність виводу з ладу енергосистеми. Завдяки своїй здатності швидко обробляти великі обсяги даних, прогнозувати загрози та адаптуватися до змін, використання ШІ допомагає захищати критичну інфраструктуру енергосистем від кібератак.

Традиційні методи аналізу та моделювання складних систем, таких як вирішення алгебраїчно-лінійних рівнянь, мають свої обмеження в сучасних умовах. Накопичення великих обсягів даних, швидкі зміни параметрів систем та випадкові збурення вимагають побудову більш гнучких та адаптивних моделей. Водночас, для максимально ефективного використання цих технологій необхідно враховувати виклики, пов'язані з достовірністю алгоритмів та їхньою захищеністю. Іншим викликом є питання захищеності самих алгоритмів ШІ від кіберзагроз. Оскільки ШІ стає важливим елементом захистом від кіберзагроз, він також стає ціллю для атак. Це може включати атаки на моделі машинного навчання, спрямовані на спотворення результатів аналізу або на зміну поведінки систем. Тому, при розробці таких систем необхідно враховувати їхню стійкість до зовнішніх втручань. Саме ШІ, завдяки своїм алгоритмічним можливостям, стає вирішальним інструментом для подолання цих викликів.

Список використаних джерел:

1. Дегтярьова О.О., Куклінова С.І. Системи штучного інтелекту в оптимізації енергетичних процесів: інноваційні підходи до ефективного управління сталим розвитком підприємства. Вісник Хмельницького національного університету. 2024. №1. С.359-362.
2. Глушко А. Д., Бородай А. В. Штучний інтелект як драйвер розвитку національної економіки. Тези 76-ї наукової конференції професорів, викладачів, наукових працівників, аспірантів та студентів університету "Національний університет" Полтавська політехніка імені Юрія Кондратюка" 14 травня – 23 травня 2024 р . Полтава 2024. ТОМ 2 .С.384-385
3. Могилевська О. Ю., Слободяник А.М., Сідак І.В. Вплив штучного інтелекту на українську і міжнародну економіку. Київський економічний науковий журнал. № 1. 2023. С. 45-52.
4. Живцова Л. І. Штучний інтелект: сутність та перспективи розвитку. Український журнал будівництва та архітектури. № 3 (015). 2023. С. 66-71.
5. Бараннік В. О. Енергетична безпека держави: обґрунтування основних складників, залежностей та взаємозалежностей. Стратегічні пріоритети. 2012. № 2 (23). С. 40-46.
6. Лір В. Е. Національна енергетична безпека в контексті глобальних цілей сталого розвитку. Східна Європа: економіка, бізнес та управління. 2018. Вип. 1 (12). С. 77-83.
7. Земляний М. Г. До оцінки рівня енергетичної безпеки. Концептуальні підходи. Стратегічна панорама. 2009. № 2. С. 56–63.

8. Харазішвілі Ю. М. Ідентифікація рівня енергетичної безпеки України з позицій сталого розвитку. Економіка промисловості. 2019. № 4 (88). С. 5-27.
9. Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. Стратегічні пріоритети. 2016. № 3. С. 62-76.
10. A 2030 framework for climate and energy policies. Green Paper. Brussels, 27.03.2013. URL: http://ec.europa.eu/energy/green_paper_2030_en.htm
11. Збитки та втрати енергетичного сектору України. Київська школа економіки URL: <https://kse.ua/ua/about-the-school/news/zbitki-ta-vtrati-energetichnogo-sektoru-ukrayini-vnaslidok-povnomasshtabnogo-vtorgnennya-rosiyi-perevishhili-56-mlrd-otsinka-kse-institute-stanom-na-traven-2024-roku/> (дата звернення: 21.10.2024).

Ключові слова: модель, складна система, штучний інтелект, машинне навчання

Keywords: Model, complex system, artificial intelligence, machine learning

Науковий керівник: к.т.н., доцент **Задерейко Олександр**

ІНТЕГРАЦІЯ СУЧАСНИХ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В МОБІЛЬНИХ ЗАСТОСУНКАХ ДЛЯ ВІРТУАЛЬНИХ КОНСУЛЬТАЦІЙ

Брума Крістіна

*студентка 4 курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

Мобільні застосунки для віртуальних консультацій стали популярним інструментом саморефлексії та пошуку відповідей на життєві питання. Вони надають користувачам можливість здійснювати розклади карт Таро в будь-який час і будь-де, що сприяє зручності і доступності для широкої аудиторії. Багато таких застосунків дозволяють користувачам взаємодіяти з інтерфейсом, який пропонує різні види розкладів, пояснює значення кожної карти та надає базову інтерпретацію ситуацій. Однак, більшість існуючих рішень обмежені простими алгоритмами та фіксованими шаблонами, що знижує персоналізованість і глибину взаємодії з користувачем.

З розвитком сучасних технологій штучного інтелекту (ШІ), зокрема моделей природної мови, таких як GPT (Generative Pre-trained Transformer), мобільні застосунки для віртуальних консультацій Таро можуть зробити значний крок уперед у напрямку інтерактивності та персоналізації. GPT, розроблений OpenAI [1], є потужною мовною моделлю, яка здатна генерувати людські відповіді на основі контексту, ставити додаткові запитання та враховувати індивідуальні особливості кожного користувача.

Інтеграція GPT у мобільні застосунки відкриває нові можливості для взаємодії користувача з віртуальним консультантом. Завдяки ШІ, можна не лише отримувати розклад карт та їхню інтерпретацію, але й вести діалог з

ботом, який надаватиме глибші тлумачення, запитуватиме додаткову інформацію для уточнення ситуації та допомагатиме краще розуміти символіку Таро. Така інтерактивність значно підвищує якість консультацій і дозволяє користувачам відчувати індивідуальний підхід, що є важливою частиною процесу саморефлексії.

Дослідження теми

Інтеграція сучасних технологій штучного інтелекту в мобільних застосунках для віртуальних консультацій

Інтеграція штучного інтелекту, зокрема моделей на зразок GPT, у мобільні застосунки для віртуальних консультацій відкриває нові горизонти в розвитку користувацького досвіду. Основна мета такого дослідження полягає в тому, щоб поєднати традиційні практики з сучасними можливостями інтерактивного штучного інтелекту, створюючи глибші і персоналізовані консультації.

Інтеграція в Android Studio

Для реалізації мобільного застосунку на базі Android з інтеграцією GPT використовуються сучасні інструменти розробки, такі як Android Studio [2]. Ця платформа є офіційним середовищем для створення мобільних додатків під операційну систему Android, що дозволяє розробляти додатки на мові програмування **Kotlin** або **Java**.

Основні етапи інтеграції GPT у мобільний додаток на платформі Android Studio включають:

1. Створення проєкту

Розробник починає з налаштування нового проєкту в Android Studio, визначаючи базову архітектуру застосунку. Моделі взаємодії із користувачем, такі як вибір карт Таро та перегляд результатів, будуються через UI-компоненти Android.

2. Інтеграція API OpenAI

Для інтеграції GPT використовується API [\[1\]](#) OpenAI, яке дозволяє звертатися до потужної мовної моделі та отримувати динамічні відповіді на запити користувача. Це API надає можливість надсилати текстові запити та отримувати розширені текстові відповіді, що забезпечує гнучкість у генерації відповідей.

3. Налаштування мережевої взаємодії

Важливо правильно налаштувати мережеву взаємодію між мобільним додатком і сервером OpenAI. Для цього в Android застосовуються такі бібліотеки, як Retrofit або Volley, які спрощують процес надсилання HTTP-запитів та обробку відповідей від API [3].

4. Обробка результатів GPT

Отримані від GPT відповіді обробляються в застосунку та відображаються у зручному для користувача форматі. Наприклад, GPT може генерувати інтерпретації карт Таро та відповідати на запитання, пов'язані з конкретними розкладами карт.

У додатку це може виглядати у вигляді текстових повідомлень у чаті, де користувач взаємодіє з ШІ-консультантом.

Ось приклад інтеграції [4] API OpenAI на Java для Android Studio:

1. Інтерфейс для API-запиту

```
import retrofit2.Call;
import retrofit2.http.Body;
import retrofit2.http.Headers;
import retrofit2.http.POST;

public interface OpenAIApiService {
    @Headers("Authorization: Bearer YOUR_API_KEY")
    @POST("v1/completions")
    Call<GPTResponse> getGPTResponse(@Body GPTRequest request);
}
```

2. Клас для запиту (GPTRequest)

```
public class GPTRequest {
    private String model;
    private String prompt;
    private int max_tokens;

    public GPTRequest(String prompt) {
        this.model = "text-davinci-003";
        this.prompt = prompt;
        this.max_tokens = 150;
    }

    // Getters and Setters
    public String getModel() {
        return model;
    }

    public void setModel(String model) {
        this.model = model;
    }

    public String getPrompt() {
        return prompt;
    }
}
```

```
    public void setPrompt(String prompt) {  
        this.prompt = prompt;  
    }  
    public int getMaxTokens() {  
        return max_tokens;  
    }  
    public void setMaxTokens(int max_tokens) {  
        this.max_tokens = max_tokens;  
    }  
}
```

3. Клас для відповіді (GPTResponse)

```
import java.util.List;
```

```
public class GPTResponse {  
    private String id;  
    private List<Choice> choices;  
    // Getters and Setters  
    public String getId() {  
        return id;  
    }  
    public void setId(String id) {  
        this.id = id;  
    }  
    public List<Choice> getChoices() {  
        return choices;  
    }  
    public void setChoices(List<Choice> choices) {  
        this.choices = choices;  
    }  
}
```

4. Клас для елементів вибору (Choice)

```
public class Choice {  
    private String text;  
    // Getters and Setters  
    public String getText() {  
        return text;  
    }  
    public void setText(String text) {  
        this.text = text;  
    }  
}
```

}

Пояснення:

1. Інтерфейс OpenAIApiService – тут використовується анотація @POST для надсилання HTTP POST-запиту до OpenAI API. @Headers додає ключ API до кожного запиту.

2. Клас GPTRequest – містить параметри для запиту до OpenAI API, такі як модель (text-davinci-003), текстовий запит (prompt) і максимальну кількість токенів для відповіді.

3. Клас GPTResponse – використовується для отримання відповіді від API. Він містить список об'єктів типу Choice, кожен з яких представляє варіант відповіді GPT.

4. Клас Choice – представляє один варіант відповіді, який генерує GPT.

Можливості API OpenAI у мобільних додатках

API OpenAI надає потужні інструменти для створення інтерактивного досвіду користувачів. У контексті мобільних застосунків для віртуальних консультацій, GPT може виконувати кілька важливих функцій:

1. Динамічна інтерпретація розкладів

Замість шаблонних пояснень, GPT здатен генерувати відповіді, враховуючи запитання користувача і конкретний розклад карт. Це дозволяє надати кожному користувачу індивідуальну інтерпретацію з урахуванням його ситуації.

Наприклад, користувач може задати конкретне питання стосовно своєї кар'єри чи відносин, а GPT відповість з урахуванням символіки карт та контексту питання.

2. Інтерактивний чат

Однією з ключових можливостей є ведення діалогу між користувачем і ШІ. Користувач може задавати запитання, уточнювати свої наміри або просити про додаткові пояснення щодо розкладу, а GPT буде відповідати, створюючи ефект справжнього віртуального консультанта.

Це робить процес використання карт Таро більш привабливим і цікавим.

3. Постійне навчання та адаптація

Модель GPT можна навчати на основі запитів користувача, аналізуючи, які відповіді були найбільш корисними. Це дозволяє покращувати якість консультацій з часом, забезпечуючи більш персоналізовані відповіді для кожного користувача.

4. Підтримка різних мов

Завдяки тому, що GPT підтримує безліч мов, застосунок може легко бути адаптований для користувачів з різних країн, пропонуючи інтерпретації

карт Таро та консультації різними мовами. Це відкриває можливість залучення глобальної аудиторії.

Виклики та перспективи

Інтеграція штучного інтелекту в мобільні застосунки, особливо для таких специфічних сфер несе як технічні виклики, так і етичні аспекти. Потрібно ретельно продумати питання конфіденційності користувачів, адже під час консультацій можуть виникати особисті дані. Крім того, важливо, щоб користувачі розуміли, що вони взаємодіють з ШІ, а не справжнім фахівцем з Таро.

Однак такі інновації дозволяють створювати нові формати цифрового досвіду, де поєднуються елементи традиційних практик і сучасних технологій. Можливість взаємодії з мобільним застосунком через ШІ GPT може значно підвищити залученість користувачів, надавши їм більш інтерактивний і персоналізований сервіс.

Це дослідження дає змогу оцінити потенціал штучного інтелекту в контексті віртуальних консультацій і може бути важливою сходинкою на шляху до створення інноваційних рішень у цій сфері.

Висновок

Інтеграція OpenAI GPT через API у мобільні застосунки на базі Android, зокрема для таких специфічних цілей, як віртуальні консультації, відкриває нові можливості для покращення користувацького досвіду. Перехід від фіксованих, заздалегідь визначених шаблонів до динамічної взаємодії через штучний інтелект дозволяє створювати персоналізовані і інтерактивні рішення.

Використання Android Studio разом з мовами Java або Kotlin, а також потужного фреймворку Retrofit для обробки HTTP-запитів до OpenAI API, значно спрощує реалізацію цієї інтеграції. Модель GPT забезпечує можливість генерації гнучких та інтелектуальних відповідей на основі запитів користувача, створюючи ефект живого спілкування.

Застосування таких технологій в поєднанні з традиційними практиками може залучити нову аудиторію, зробивши процес саморефлексії та отримання консультацій не лише доступнішим, але й більш привабливим та цікавим. Інтеграція GPT також пропонує широкий простір для адаптації й розширення функціоналу мобільних додатків, з можливістю подальшого вдосконалення та навчання ШІ на основі запитів користувачів.

Таким чином, дослідження та реалізація таких проектів є перспективним напрямком у розвитку мобільних застосунків із залученням технологій штучного інтелекту.

[1] API - це програмний інтерфейс, який дозволяє двом програмним компонентам взаємодіяти один з одним, використовуючи набір визначень та протоколів.

[1] CNN (Convolutional Teural Tetwork) - згорткова нейронна мережа, орієнтована на ефективне розпізнавання образів

Список використаних джерел:

1. OpenAI API Documentation. OpenAI. URL: <https://beta.openai.com/docs> (дата звернення: 04.10.2024).
2. Android Developers. Офіційна документація. URL: <https://developer.android.com/docs> (дата звернення: 04.10.2024).
3. Retrofit Documentation. Retrofit: A type-safe HTTP client for Android and Java. URL: <https://square.github.io/retrofit/> (дата звернення: 04.10.2024).
4. OpenAI GPT-3 Integration Examples on GitHub. GitHub. URL: <https://github.com/topics/openai-gpt3> (дата звернення: 04.10.2024).

Ключові слова: Застосунок, штучний інтелект, Android Studio, OpenAI, Java

Keywords: Application, artificial intelligence, Android Studio, OpenAI, Java

Науковий керівник: *к.т.н., доцент Задерейко Олександр*

ІНФОРМАЦІЙНА СИСТЕМА ВИКОРИСТАННЯ НЕЙРОМЕРЕЖЕВОГО ПІДХОДУ ДЛЯ ВИРІШЕННЯ ЗАВДАННЯ ПРОГНОЗУВАННЯ ЗМІСТУ ЦИФРОВИХ ЗОБРАЖЕНЬ

Бондаренко Сергій

студент 2 курсу магістратури, факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасні інформаційні системи відіграють вирішальну роль у підвищенні ефективності обробки, аналізу та прогнозування даних, особливо у галузі обробки зображень. Серед новітніх підходів вирізняється застосування нейронних мереж для аналізу та розпізнавання об'єктів на цифрових зображеннях. Нейронні мережі дозволяють отримати новий рівень точності та деталізації у вирішенні завдань прогнозування змісту, що має велике значення у різних сферах, від медичної діагностики до безпілотних технологій. Розглянемо, як інформаційна система на основі нейромережевого підходу може сприяти автоматичному аналізу вмісту зображень, підвищуючи ефективність і точність цього процесу [1].

Нейронні мережі стали основою для створення штучного інтелекту, здатного «навчатися» та адаптуватися до вирішення різних завдань. Підхід передбачає використання моделей глибинного навчання, таких як згорткові нейронні мережі (CNN[1]), які відмінно підходять для роботи з цифровими зображеннями. CNN ефективно виявляють патерни та особливості, які лю-

дина може не помітити, що підвищує точність прогнозування. Вони складаються з великої кількості шарів нейронів, кожен з яких виконує певну роль в обробці зображення.

Перший шар мережі, як правило, відповідає за вхідні дані, після чого інформація проходить через численні шари, що здійснюють різні трансформації та виділення ознак. Цей ієрархічний підхід дозволяє мережі навчатися на базі великих обсягів даних, автоматично адаптуючись до змін у структурі даних, що зменшує потребу в ручному налаштуванні параметрів [2].

Інформаційна система з прогнозування змісту зображень включає кілька основних компонентів, які працюють у комплексі для досягнення високих результатів:

1. Збір та підготовка даних: Система спочатку збирає зображення для навчання нейронної мережі. Потім дані проходять етапи попередньої обробки — зміну розміру, нормалізацію та маркування, щоб забезпечити якісне навчання. На цьому етапі важливо також усунути шум і артефакти, що можуть негативно вплинути на результати.

2. Навчання та тестування моделі: На цьому етапі відбувається навчання і тестування нейромережі, що включає в себе застосування значної кількості навчальних і тестувальних зображень. Процес навчання полягає у оптимізації ваг нейронів, щоб досягти високої точності розпізнавання. Модель може використовувати різні алгоритми навчання, включаючи навчання з вчителем, де кожне зображення супроводжується етикеткою, або без вчителя, де система сама виявляє структури в даних. Процес тестування полягає в перевірці правильності навчання та виявлення необхідних перенавчань.

3. Аналіз та прогнозування: Після навчання модель може прогнозувати зміст нових зображень, автоматично визначаючи категорії об'єктів, типи зображень чи сцени. Цей етап є критично важливим, оскільки забезпечує безпосередній зв'язок між навчанням і практичним застосуванням.

4. Виведення результатів та їх візуалізація: Результати прогнозування подаються у зрозумілому вигляді, що може включати текстові підписи, мітки або інші індикатори, які допомагають користувачу швидко зрозуміти зміст зображення. Важливим аспектом є зручність інтерфейсу, що дозволяє користувачам легко інтерпретувати результати роботи системи [3].

Переваги та недоліки нейромережевого підходу:

Нейронні мережі мають значні переваги у порівнянні з традиційними методами прогнозування та класифікації. Вони демонструють високу точність, здатність до самонавчання, а також адаптацію до нових умов, що є важливим фактором для роботи з великими обсягами даних. Однак, слід зазначити, що такий підхід має певні обмеження, такі як висока обчислювальна складність та потреба в значних ресурсах для навчання моделей.

Серед інших мінусів - потреба у великих наборах навчальних даних, що може бути складним і витратним процесом, а також складність у поясненні процесів, що відбуваються у глибоких шарах нейронної мережі. Це часто призводить до того, що нейронні мережі сприймаються як "чорні скриньки", де важко зрозуміти, як саме приймаються рішення [4].

Будь яка система, що використовує нейромережевий підхід для прогнозування змісту цифрових зображень, є важливим інструментом для автоматизації аналізу та обробки візуальних даних. Вона знаходить застосування в різних сферах, від медицини до розпізнавання об'єктів різної складності, допомагаючи автоматизованим системам приймати або формувати потрібні рішення. З огляду на значний прогрес у галузі глибинного навчання, такі системи мають великий потенціал для подальшого розвитку та впровадження в різних галузях, де обробка зображень є ключовим елементом. Таким чином, нейромережевий підхід стає незамінним інструментом у світі інформаційних технологій, що відкриває горизонти для досліджень і практичного використання.

Список використаних джерел:

1. Згорткова нейронна мережа. Електронний режим доступу: URL: <https://evergreens.com.ua/ua/articles/cnn.html> (дата звернення 6.11.2024).
2. A Gentle Introduction to k-fold Cross-Validation. Електронний режим доступу: URL: <https://machinelearningmastery.com/k-fold-cross-validation/> (дата звернення 6.11.2024).
3. "Deep Learning" by Ian Goodfellow, Yoshua Bengio, and Aaron Courville. Електронний режим доступу: <https://www.deeplearningbook.org/> (дата звернення 6.11.2024).
4. Рекурентна нейронна мережа. Електронний режим доступу: URL: https://www.wikiwand.com/en/articles/Recurrent_neural_network (дата звернення 6.11.2024)

Ключові слова: нейромережевий підхід, Нейронні мережі, навчання нейронної мережі, тестування нейромережі

Keywords: neural network approach, Neural networks, neural network training, neural network testing

Науковий керівник: *к.т.н., доцент Задерейко Олександр*

МЕТОДИ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ ДЛЯ ЗАХИСТУ ВІД КІБЕРАТАК

Вавілов Микита

студент 1 курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сьогодні кібератаки з використанням соціальної інженерії становлять серйозну загрозу для бізнесу та громадськості. Зловмисники часто використовують методи соціальної інженерії для обходу систем безпеки. Це пов'я-

зано з тим, що ці методи відносно дешеві і не вимагають глибоких технічних знань у галузі ІТ.

Соціальна інженерія є ефективною значною мірою через недбале ставлення людей до безпеки в Інтернеті. Поведінкові звички користувачів дозволяють зловмисникам легко маніпулювати своїми жертвами. Статистика показує, що більшість хакерських атак здійснюється наступними способами.

Серед найбільш поширених атак цього типу можна виокремити:

1. Фішинг: Часто можна зіткнутися з фальшивими повідомленнями від банків та інших онлайн-сервісів з проханням підтвердити особисті дані, такі як імена користувачів, паролі та номери кредитних карток. Це класичний приклад фішингової атаки, спрямованої на викрадення конфіденційної інформації для подальшого використання або продажу. Вперше ця технологія була згадана в 1987 році, коли обговорювалися методи імітації легальних організацій та послуг. Фішинг «Назва “фішинг” пов'язана з принципом “вилову” користувачів» [1].

2. Pretexting: цей тип атаки створює хибні приводи або сценарії, щоб змусити іншу сторону розкрити критичні дані. Зловмисник видає себе за співробітника служби технічної підтримки або представника банку, щоб створити атмосферу довіри. Цей тип маніпуляцій може відбуватися через будь-який вид комунікації, включаючи особисті зустрічі, а також онлайн-взаємодію.

3. Quid Pro Quo: В основі цього методу лежить принцип «послуга за послугу». Зловмисник використовує психологічну схильність людини відповідати на послуги, створюючи ситуацію, в якій жертва відчуває себе зобов'язаною запропонувати щось натомість.

Також до технічно організованих атак відносять:

1. Атака HTTP-флуд - це тип масової розподіленої атаки на відмову в обслуговуванні, яка бомбардує сервер HTTP-запитами, внаслідок чого він стає перенавантаженим і не може відповідати на звичайний трафік. Як наслідок, це призводить до відмови в обслуговуванні додаткових запитів від існуючих користувачів.

2. У випадку DDoS-атаки зловмисник генерує величезну кількість пакетів або запитів, які зрештою перевантажують цільову систему.

Атака на відмову в обслуговуванні (англ. Denial-of-Service attack – DoS attack. Якщо атака відбувається одночасно з великої кількості IP-адрес, то її називають розподіленою (англ. Distributed Denial-of-Service – DDoS). У розподіленій атаці на відмову одночасно можуть брати участь від кількох одиниць до кількох сотень тисяч, а іноді - кількох мільйонів хостів [2]. Мета атаки: зробити так, щоб система перестала працювати, і користувачі не могли от-

римати доступ до системних ресурсів. Щоб DDoS-атака була успішною, атакуючому потрібно посилати більше запитів, ніж може обробити сервер.

Види DDoS-атак

DDoS-атаки на каналному рівні. Ці атаки можуть бути декількох типів:

UDP-флуд: У цій атаці на сервер, що атакується, надходить величезна кількість фальшивих UDP-пакетів [2] з різних IP-адрес. В результаті сервер або мережеве обладнання перед ним перевантажується фальшивими пакетами, що призводить до переповнення пропускної здатності каналу і перевантаження мережевого інтерфейсу.

ICMP-флуд: У цій атаці на сервер надсилаються підроблені ICMP-пакети з різних IP-адрес. В результаті ресурси сервера вичерпуються і він не в змозі обробити запити.

Ping-флудінг: Зловмисники надсилають фальшиві Ping-пакети з широкого спектру IP-адрес. Недоліком таких атак є те, що їх можна сплутати зі звичайним трафіком.

SYN-флуд: Зловмисники використовують вразливість в протоколі TCP в процесі «рукоштовування» між клієнтом і сервером. Відправляючи кілька запитів на з'єднання, хакер перевантажує чергу сервера. В результаті сервер стає недоступним для нових з'єднань або відбувається затримка у встановленні з'єднання.

DDoS-атаки на рівні додатків зазвичай спрямовані на веб-сервери, такі як Windows IIS і Apache, та платформи CMS, такі як WordPress, Joomla, Drupal і Magento. Ці атаки виводять з ладу компоненти додатків, впливаючи на їхню продуктивність і доступність.

DDoS-атаки, які використовують вразливості протоколу, включають

«Пінг смерті», який надсилає на сервер-жертву пакети, розмір яких перевищує 65535 байт, що спричиняє помилки і може призвести до вимкнення сервера. Цей тип атаки був популярним у 1990-х роках і використовується досі, але вже проти додатків та апаратних пристроїв. Ця атака може призвести до перезавантаження або повного падіння сервера.

Мета такої атаки - вимкнути додаток, онлайн-сервіс або сайт. Зазвичай кількість цих атак є невеликою, особливо у порівнянні кількістю атак на рівні мережі, але вони можуть завдати такої ж шкоди [4] [5]. У розподіленій атаці на відмову одночасно можуть брати участь від кількох одиниць до кількох сотень тисяч, а іноді - кількох мільйонів хостів.

Атаки на рівні додатків включають:

Атака на DNS-сервери. Ця атака перенаправляє не тільки окремих клієнтів-жертв, але й усіх користувачів, які звертаються до скомпрометованого DNS-сервера, на фальшиву IP-адресу. Для цього зловмисник надсилає запити, які змушують сервер запитувати відповіді від інших вузлів мережі.

Потім зловмисник починає надсилати потік фальшивих пакетів відповідей на DNS-сервер. Коли сервер отримує фальшиву відповідь з дійсним ідентифікатором, він розпізнає хакера як легітимного DNS і видає клієнту IP-адресу, вказану зловмисником. Результат кешується, і наступні запити перенаправляють користувача на фальшиву IP-адресу.

Атака переповнення HTTP 7-го рівня. Цей тип атаки перевантажує і де-стабілізує окремі елементи сайту або сервера. Виявити її складно, оскільки запити виглядають як звичайний трафік. Запити, надіслані зловмисниками, можуть споживати ресурси сервера і призвести до падіння сайту. Часто такі запити надсилають боти, що посилює атаку. Оскільки ці атаки майже не залежать від ширини каналу, зловмисники можуть вивести з ладу сервери навіть з мінімальними ресурсами. На деяких веб-серверах навіть невелика кількість запитів в секунду може уповільнити роботу додатків і баз даних. В середньому, атаки, що перевищують 100 запитів на секунду, можуть вивести з ладу веб-сайти середнього розміру.

Методи захисту від мережевих загроз перехопленням пакетів

Елементи, які можна перехопити, залежать від типу мережі. Видимість трафіку в дротових мережах залежить від конфігурації мережевих комутаторів, які централізують зв'язок між кількома підключеними пристроями. Комутатори можуть дозволити інструменту переглядати трафік з усієї мережі або обмежити його до певної частини мережі.

Інструменти перехоплення пакетів у бездротових мережах зазвичай мають можливість перехоплювати лише один канал за раз, якщо тільки хост-комп'ютер не має декількох бездротових інтерфейсів.

У випадку DDoS-атаки зловмисник генерує величезну кількість пакетів або запитів, які зрештою перевантажують цільову систему.

Зловмисник використовує кілька контрольованих або скомпрометованих джерел для підтримки атаки. Використання сигнатурних методів призвело до розробки систем виявлення вторгнень (IDS), які ідентифікують потенційні вторгнення шляхом виявлення відомих шаблонів атак. Тому дуже важливо визначити, що є нормальним, а що - аномальним пакетним трафіком в мережі. Щоб забезпечити доступність хоста, він повинен отримувати лише стільки трафіку, скільки він може обробити; це називається обмеженням швидкості.

Сучасні методи безпеки можуть розрізняти легальний і нелегальний трафік, аналізуючи окремі пакети. Для цього необхідно розуміти типові характеристики трафіку, який отримує хост, і порівнювати кожен пакет з цим базовим рівнем. Такий підхід може ефективно запобігати зовнішнім атакам. Для захисту від таких атак, як SQL-ін'єкції або підробка міжсайтових запитів,

що використовують уразливості в додатку, рекомендується використовувати брандмауер веб-додатків (WAF).

Крім того, важливо створити захист від нелегітимних запитів, які можуть надходити від шкідливих API з неочікуваних пулів IP-адрес регіонів через їхні унікальні характеристики. Іноді зловмисники можуть створювати індивідуальні засоби захисту, вивчаючи шаблони трафіку. Тому ця техніка може бути корисною для зменшення кількості атак [5].

Для запобігання HTTP-флуду важливо впровадити відповідні заходи безпеки. Ця атака відбувається на 7-му рівні моделі OSI, який охоплює інтернет протоколи, в тому числі і HTTP.

Щоб зменшити кількість первинних і вторинних помилок на 5%, класифікація на основі корисного навантаження однорангового трафіку передбачає перевірку його сигнатур на прикладному рівні.

Класифікація запитів мережевого трафіку за корисним навантаженням може бути виконана за допомогою наступних методів аналізу та обробки даних

- PBNS (на основі пакетів зі збереженням стану без збереження стану);
- PBFS (на основі пакетів зі збереженням стану для кожного потоку);
- MBFS (на основі повідомлень зі збереженням стану для кожного потоку);
- MBPS (на основі повідомлень зі збереженням стану для кожного протоколу).

Поширення розподілених загроз і атак, в тому числі DDoS-атак, вимагає створення методів, здатних надійно виявляти і відбивати ці загрози на різних рівнях мережі. Для забезпечення комплексної стратегії безпеки сучасні системи аналізу трафіку повинні доповнюватися додатковими заходами безпеки, такими як системи виявлення вторгнень (IDS/IPS), брандмауерами, антивірусним програмним забезпеченням та іншими інструменти.

Ці сучасні методи аналізу трафіку дозволяють проводити високорівневий аналіз протоколів і додатків, полегшуючи ідентифікацію і класифікацію різних типів трафіку з додатків.

Автоматизовані та інтелектуальні інструменти дозволяють швидше виявляти загрози та автоматично реагувати на заходи безпеки.

Вищезгадані тенденції свідчать про те, що сучасні методи аналізу трафіку виходять за рамки простого спостереження і переходять до більш складних і розумних систем, які можуть кваліфіковано виявляти і захищати від цілого ряду загроз в складних мережевих умовах.

На сьогоднішній день одним з найпоширеніших методів виявлення аномалій є інструменти виявлення атак (ADT) [6].

Список використаних джерел:

1. Застосування інформаційних технологій у діяльності правоохоронних органів : зб. матеріалів кругл. столу (м. Харків, 9 груд. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2020. – С. 113-116.
2. Левандовський А. О. Метод аналізу трафіку з метою виявлення атак на комплексні системи захисту інформації: кваліфікаційна робота магістра : 125 Кібербезпека / А. О. Левандовський ; Хмельниц. нац. ун-т. – Хмельницький, 2023. – 96 с.
3. Колодчак О. "Сучасні методи виявлення аномалій в системах виявлення вторгнень." Вісник Національного ун-т «Львівська політехніка». Комп'ютерні системи та мережі 745 (2012): 98-104. Conference on Advanced Information Technologies (ICAIT). IEEE, 2019.
4. Застосування інформаційних технологій у діяльності правоохоронних органів : зб. матеріалів кругл. столу (м. Харків, 9 груд. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2020. – С. 113-116.
5. Світличний В. А. Дослідження атак на відмову в обслуговуванні інформаційно-телекомунікаційних систем // Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р. Одеса : ОДУВС, 2018. С. 88-89.
6. Що таке DDoS-атака? URL: <https://cip.gov.ua/ua/faqs/sho-take-ddos-ataka> (дата звернення: 21.10.2024).

Ключові слова: фішинг, HTTP-флуд, DDoS-атаки, синхронна атака, ping-флуд, UDP-флуд, ICMP-флуд.

Keywords: phishing, HTTP flood, DDoS attacks, synchronous attack, ping flood, UDP flood, ICMP flood.

Науковий керівник: *к.т.н., доцент Задерейко Олександр*

АНАЛІЗ ВИТОКІВ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ СИСТЕМ

Власенко Даніїл

студент 2 курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Створення захищеної інформаційно-комп'ютерної системи (ІКС) неможливе без ретельної розробки та оптимізації алгоритмів, які забезпечують захист цієї системи. Будь-яка захищена ІКС потребує дослідження методів захисту конфіденційності та захищеності використовуваного програмного забезпечення (ПЗ). Досягнення високого рівня захисту вимагає ефективного аналізу потенційних витоків даних користувача, що обумовлює необхідність детального вивчення сучасних методик аналізу і способів запобігання таким витокам.

З практичної точки зору, головна мета захисту ІКС від витоків даних користувача полягає у впровадженні інформаційних технологій, які забезпечать аналіз можливих каналів витоку та реалізацію заходів захисту на про-

грамному та апаратному рівнях. Функціональним середовищем для реалізації таких технологій є системне програмне забезпечення (СПЗ), яке виконує завдання управління та забезпечення взаємодії компонентів ІКС, а також надає користувачу та прикладним процесам інтерфейси до апаратної частини ІКС. Основним елементом СПЗ є операційна система (ОС), архітектура і функціонування якої визначають вимоги до конфігурації прикладного ПЗ в ІКС.

Таким чином, комплекс усіх перерахованих напрямів діяльності дозволяє систематизувати питання захисту від витоків даних і всебічно аналізувати процеси у функціонуванні ПЗ системи. Це визначає необхідність розробки спеціальних методів захисту ІКС від витоків персональних даних користувача.

Для виявлення потенційних витоків персональних даних в ІКС необхідно аналізувати ТСП-з'єднання на рівні мережевого інтерфейсу користувацького пристрою (КП) [1]. Це можна реалізувати за допомогою інструментів, що забезпечують перехоплення мережевого трафіку на мережевому інтерфейсі користувача [2].

Для отримання достовірних результатів фіксація мережевого трафіку, ініційованого в ІКС (включаючи ОС, веб-браузери та месенджери), має проводитися протягом тривалого часу, бажано упродовж типового робочого дня користувача.

Ці обставини зумовлюють необхідність фіксації всіх мережевих з'єднань на користувацькому пристрої (КП), які здійснюються під управлінням як мобільних, так і стаціонарних операційних систем. Після фіксації важливо провести аналіз для класифікації з'єднань на функціональні та нефункціональні. Класифікацію доцільно здійснювати за наступними критеріями:

1) Функціональні з'єднання – це з'єднання, які забезпечують стабільне функціонування системного і прикладного ПЗ в ІКС; їх блокування призводить до збоїв у роботі або до повної втрати працездатності системи.

2) Нефункціональні з'єднання – це з'єднання з хостами, які не мають безпосереднього зв'язку з офіційними хостами системного чи прикладного ПЗ.

Для ефективної класифікації мережевих з'єднань на основі цих критеріїв необхідно експериментально перевірити працездатність ОС, веб-браузерів і месенджерів, поетапно блокуючи їх з'єднання.

Для дослідження мережевих з'єднань КП під керуванням ОС Android і ОС Windows було підготовлено КП користувача, які складаються з:

- стаціонарного ПК, на який встановлено офіційний дистрибутив ОС Windows;
- смартфона з ОС Android;

- ПЗ No Root Firewall [3];
- комунікаційне ПО:
- веб-браузери: Google Chrome, Microsoft Edge, Mozilla Firefox, Opera, Safari;
- месенджери: Telegram, Viber, Signal;
- ПЗ TCPview[1];
- ПЗ Wireshark [2];
- ПЗ Windows Firewall Control [4];

Загальний процес збору інформації щодо визначення потенційних витоків даних користувача з КП представлений на рис. 1.



Рис. 1. Процес збору та аналізу потенційних витоків даних користувача з КП.

У ході збору та аналізу мережеских з'єднань КП було виявлено, що операційні системи, веб-браузери та месенджери здійснюють підключення до доменів і IP-адрес, які належать ІТ-компаніям, що займаються транзитом, збором, обробкою та монетизацією даних користувачів. Це свідчить про високу ймовірність існування угод між розробниками веб-браузерів та месенджерів і великими ІТ-компаніями, які фактично займають монопольне поло-

ження на ринку інтернет-послуг зі збору, обробки та монетизації даних користувачів [5].

Таким чином, поточна ситуація є неприйнятною з точки зору захисту конфіденційності користувачів, які застосовують безкоштовно доступні веб-браузери та месенджери, що працюють під управлінням мобільних і стаціонарних операційних систем.

Список використаних джерел:

1. TCPView. URL: <https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview> (дата звернення 10.11.2024).
2. Wireshark. URL: <https://wireshark.org> (дата звернення 10.11.2024).
3. No Root Firewall. URL: <https://firewall-ohne-root.en.download.it/android/download> (дата звернення 10.11.2024).
4. Windows Firewall Control. URL: <https://www.binisoft.org/wfc> (дата звернення 10.11.2024).
5. Дослідження потенційних витоків даних в інформаційних і комунікаційних системах / О. В. Задерейко, О. Г. Трофименко, Ю. В. Прокоп, Н. І. Логінова, А. І. Дика, С. В. Кухаренко // Радіоелектронні і комп'ютерні системи. : науково-технічний журнал. - Харків : «ХАІ», 2022. - № 4 (104). - С. 64-84. – Режим доступу : <https://doi.org/10.32620/reks.2022.4.05>.

Ключові слова: інформаційно-комп'ютерна система, веб-браузер, месенджер, ІТ-компанії, комунікаційний пристрій, аналіз витоків даних.

Keywords: information and computer system, web-browser, messenger, IT companies, communication device, data leak analysis.

Науковий керівник: *к.т.н., доцент Юрій Щербина*

СТВОРЕННЯ МОБІЛЬНОГО ЗАСТОСУНКУ ДЛЯ ПОШУКУ ВОДІЇВ ТА ПОПУТНИКІВ. АНАЛІЗ КОНКУРЕНТІВ

Косяк Микола

*студент 4 курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

Мобільні додатки для пасажирських перевезень вже стали невід'ємною частиною транспортної інфраструктури сучасних міст, забезпечуючи швидкий та зручний доступ до транспорту. Завдяки таким онлайн платформам, як Uber та InDrive, користувачі можуть організувати поїздки, не виходячи з дому, а водії отримують можливість працювати гнучко, використовуючи свій автомобіль для додаткового заробітку. Однак, попри цих популярних додатків, існують певні обмеження в їх функціональності, що спонукає розробників до створення нових рішень, які могли б ефективніше задовольняти потреби користувачів.

Наприклад, платформа Uber надає користувачам чіткі переваги завдяки фіксованій ціні за поїздку, що розраховується автоматично. Це дозволяє пасажиром заздалегідь знати вартість поїздки, що забезпечує певний рівень передбачуваності та комфорту. Однак така система має і свої недоліки: водії не можуть обирати замовлення самостійно, а система не дозволяє взяти попутників, що обмежує можливість оптимізувати витрати або зменшити вартість поїздки для пасажирів. Крім того, Uber жорстко контролює ціноутворення, що може не відповідати очікуванням водіїв у певних ситуаціях.

З іншого боку, такі сервіси, як InDrive, пропонують більше гнучкості, дозволяючи водіям і пасажиром домовлятися про вартість поїздки. Це відкриває можливість для більш персоналізованого досвіду, де водії можуть самостійно обирати найзручніші для них замовлення та регулювати свій графік. Проте InDrive не надає достатніх можливостей для фільтрації замовлень за певними критеріями, такими як наявність дітей, тварин або багажу, що може створювати незручності для обох сторін. До того ж, у сервісі відсутні механізми, що дозволяють водіям брати попутників, обмежуючи можливість знижувати вартість поїздки через поділ витрат.

З огляду на ці обмеження, виникає потреба в розробці більш універсальних рішень, які б поєднували в собі переваги обох підходів та забезпечували ширші можливості для користувачів. Саме тому існує необхідність у розробці мобільного додатку для пошуку водіїв і попутників, що орієнтований саме на вирішення цих проблем. Він має поєднувати в собі найкращі аспекти існуючих рішень, додаючи нові функції, які роблять користування ним більш зручним і гнучким як для водіїв, так і для пасажирів.

Основною перевагою такого додатку є надання можливості водіям самостійно вибирати замовлення зі списку, що дає їм більше контролю над своїм графіком та умовами роботи. Крім того, додаток передбачає функцію фільтрації замовлень за різними критеріями (наприклад, наявність дітей, тварин, багажу), що значно підвищує зручність для водіїв та пасажирів. Одна з ключових особливостей додатку — можливість брати попутників під час поїздки, що дозволяє знизити витрати на паливе та оптимізувати маршрут.

Дослідження предметної області з цього напрямку вказує, що ринок мобільних додатків для пасажирських перевезень є надзвичайно динамічним та швидко розвивається. За останні роки попит на сервіси такого типу значно зріс, що пояснюється зручністю, яку вони надають користувачам. Водночас конкуренція між платформами стимулює розвиток нових функцій та можливостей, які б робили поїздки ще більш гнучкими та доступними. Тому розробка такого додатка спрямована на те, щоб поєднати переваги вже існуючих рішень із додатковими опціями для користувачів, що відповідають сучасним вимогам ринку [1]. Це дозволить досягнути значного поліпшення

якості перевезень, оптимізації маршрутів та зниження собівартості поїздок. Саме тому такий додаток прагне запропонувати рішення, яке стане ефективною альтернативою існуючим сервісам, забезпечуючи більше можливостей як для водіїв, так і для пасажирів, при цьому враховуючи потреби сучасного ринку послуг з перевезень.

Аналіз та порівняння конкурентів

У сфері мобільних додатків для пасажирських перевезень найвідомішими гравцями на ринку є Uber та InDrive. Кожен із цих сервісів має свої унікальні характеристики, які залучають мільйони користувачів по всьому світу. Проте їхня функціональність також має певні обмеження, що залишає простір для нових рішень і розвитку.

1. Платформа Uber

Uber — це одна з найбільших та найвідоміших платформ для таксі та перевезень, яка пропонує пасажирам зручний спосіб замовлення поїздок через мобільний додаток [2]. Платформа використовує автоматизовану систему підбору водіїв та розрахунку вартості поїздки, що базується на таких факторах, як відстань, час у дорозі та поточний попит на послуги.

Переваги проекту Uber:

- Фіксована ціна. Ціна за поїздку розраховується автоматично на основі алгоритмів, що робить сервіс зручним для пасажирів, які заздалегідь знають, скільки вони заплатять.

- Акції та знижки. Платформа часто пропонує різноманітні акційні пропозиції та знижки як для нових користувачів, так і для постійних клієнтів, що підвищує привабливість сервісу.

- Додаткові опції замовлення. Платформа надає користувачам можливість додавати додаткові умови до замовлення, наприклад, вибір автомобіля певного класу або включення спеціальних вимог (наявність дитячого крісла).

- Верифікація користувачів. Платформа здійснює ретельну перевірку водіїв та пасажирів, що підвищує рівень безпеки поїздок.

Недоліки Uber:

- Відсутність вибору водіїв. Водії не можуть самостійно обирати замовлення — платформа автоматично розподіляє замовлення за водіями, що може бути незручним для тих з них, хто бажає контролювати свій робочий процес.

- Неможливість взяти попутників. Платформа не підтримує можливості брати попутників на замовлення, що обмежує варіанти економії для пасажирів і додаткового заробітку для водіїв.

- Фіксована ціна може бути не вигідною для водіїв. У деяких випадках, коли попит на поїздки низький, водії можуть отримувати нижчу оплату за свої послуги, оскільки ціни жорстко контролюються алгоритмами платформи.

2. Платформа InDrive

InDrive — це мобільний додаток, який надає більше гнучкості як для водіїв, так і для пасажирів [3]. Основна концепція InDrive полягає в тому, що пасажирів можуть самостійно пропонувати ціну за поїздку, а водії — приймати її або пропонувати власні умови.

Переваги InDrive:

- Гнучкість ціноутворення. Пасажирів можуть запропонувати свою ціну за поїздку, що дозволяє водіям вибирати найвигідніші для себе замовлення та пасажирів.

- Вибір замовлень водіями. Водії мають змогу обирати замовлення самостійно зі списку доступних пропозицій, що надає їм більше контролю над своїм графіком та умовами роботи.

- Прямі переговори. Водій і пасажир можуть домовлятися щодо вартості поїздки безпосередньо, що створює можливість гнучкішого підходу до ціноутворення.

Недоліки InDrive:

- Відсутність фільтрів для замовлень. Платформа не надає можливості водіям фільтрувати замовлення за додатковими умовами, такими як наявність багажу, тварин чи дітей, що може створювати незручності.

- Неможливість взяти попутників. Платформа не дозволяє водіям брати попутників, що обмежує можливості зниження вартості поїздки.

- Відсутність акцій та знижок. Платформа не пропонує акцій або знижок, що може знижувати її привабливість для постійних користувачів.

Висновки порівняльного аналізу

Аналіз існуючих платформ Uber та InDrive показує, що вони мають сильні та слабкі сторони, проте жодна з них не пропонує ідеального балансу між гнучкістю для водіїв і зручністю для пасажирів. Тому виникає необхідність у поєднанні найкращих властивостей цих платформ, надаючи користувачам більше контролю над процесом організації поїздок та пропонуючи можливості для персоналізації. Це може бути реалізовано за рахунок впровадження функціоналу з вибору замовлень, додатковим фільтрам та можливості брати попутників, що забезпечить новий рівень комфорту для водіїв і пасажирів, що робить його конкурентоспроможним на ринку мобільних платформ для пасажирських перевезень.

3. Розробляємий власний додаток: сервіс для пошуку водіїв та попутників

Додаток, який буде розроблятися, спрямований на усунення недоліків платформ Uber та InDrive, наведених вище, має одночасно зберігати їхні найкращі риси. Тому основною метою розробляемого сервісу є поєднання зручності автоматизації та гнучкості вибору користувачам, що дозволить їм отримати більш комфортні умови використання.

Переваги розробляемого додатку:

- Вибір замовлень водіями. Як і в платформі InDrive, водії зможуть самостійно вибирати замовлення зі списку, що дозволить їм контролювати свій робочий графік та вибирати найвигідніші пропозиції.

- Можливість домовленості про ціну. Водій і пасажир матимуть змогу домовлятися про вартість поїздки безпосередньо, що забезпечує гнучкість для обох сторін.

- Додаткові фільтри для замовлень. На відміну від платформи InDrive, мій додаток надаватиме можливість водіям і пасажиром використовувати фільтри для пошуку замовлень, що відповідають їхнім вимогам, наприклад, наявність багажу, тварин, дітей тощо.

- Можливість брати попутників. Однією з ключових функцій є можливість для водіїв брати попутників, що дозволить знизити витрати на паливо та підвищити прибутковість поїздки.

- Інтуїтивна навігація та зручний інтерфейс. Завдяки продуманому інтерфейсу користувачі легко зможуть створювати замовлення, фільтрувати їх за потрібними критеріями та знаходити попутників, що значно спростить процес організації поїздки.

Недоліки розробляемого додатку:

- Відсутність ретельної верифікації облікових записів. На відміну від Uber, додаток не включає жорсткої верифікації водіїв і пасажирів, що може вплинути на рівень безпеки.

- Відсутність акцій. На першому етапі розвитку не передбачено пропонування спеціальних акцій або знижок для користувачів, що може вплинути на його популярність серед постійних клієнтів.

Особливості розробляемого застосунку

Застосунок для пошуку водіїв та попутників, який буде розроблено, буде включати два основні режими — **режим водія** та **режим пасажирів**. Нижче наведено приклади основних функцій застосунка для ілюстрації ключових елементів. Застосунок буде побудований на платформі Android Studio для ОС Android [4].

Інтерфейс застосунка базується на інтуїтивній навігації, де головні вкладки розташовані в нижній частині екрана для зручного доступу до основних функцій. На кожному етапі користувач зможе швидко переходити між

різними вкладками, такими як профіль, історія поїздок, пошук замовлень, тощо.

Ключові вкладки для водія:

- Головна стрічка замовлень — список замовлень, відсортованих за відстанню від водія.
- Управління замовленням — перегляд деталей маршруту, можливість запропонувати ціну або прийняти пропозицію пасажирів.
- Особистий профіль — дані про водія, автомобіль, методи оплати, рейтинг, а також перемикання на пасажирський режим.

Ключові вкладки для пасажирів:

- Створення замовлення — форма для введення деталей поїздки, кількості пасажирів, маршрутів, способу оплати та додаткових умов (багаж, тварини, діти).
- Пошук водія — список доступних водіїв з їх умовами, можливістю вибрати водія або продовжити пошук.
- Історія поїздок — список попередніх поїздок, включаючи можливість перегляду водіїв та залишення відгуків.

Висновок

Застосунок для пошуку водіїв та попутників, що розробляється, спрямований на вирішення кількох важливих недоліків, які існують у сучасних платформах для пасажирських перевезень. Завдяки інтуїтивній навігації, гнучкості у виборі замовлень, можливості домовлятися про ціну та налаштувати замовлення відповідно до потреб, цей додаток надасть користувачам більше контролю та комфорту. Функція можливості взяти попутників додатково підвищує економічну вигоду для водіїв і пасажирів, що є суттєвою конкурентною перевагою на цьому ринку послуг.

Відсутність ретельної верифікації та спеціальних акцій на початковому етапі може бути певним викликом, але ці аспекти можуть бути вдосконалені в наступних версіях додатку. Розвиток таких платформ у поєднанні з сучасними технологіями дозволить користувачам ефективно організовувати поїздки, забезпечуючи кращу взаємодію та персоналізований підхід, що є необхідним у сучасному світі мобільних сервісів.

Список використаних джерел:

1. Ткаченко, О., Васьківський, О. "Вебзастосунок 'Система пошуку служби таксі' як елемент цифровізації процесів на ринку таксі." Державний університет інфраструктури та технологій, 2024. URL: <http://infotech-soccult.knukim.edu.ua/article/view/307023> (дата звернення: 07.10.2024).
2. Uber. "How Uber Works". URL: <https://www.uber.com/> (дата звернення: 07.10.2024).
3. InDrive. "InDrive: A new way to get a ride". URL: <https://indrive.com/> (дата звернення: 07.10.2024).

4. Android Developers. Офіційна документація. URL: <https://developer.android.com/docs> (дата звернення: 07.10.2024).

Ключові слова: Мобільний застосунок, служба таксі, цифровізація, Android

Keywords: Mobile application, taxi service, digitalization, Android

Науковий керівник: *к.т.н., доцент Задерейко Олександр*

АНАЛІЗ СУЧАСНИХ ЗАСОБІВ РЕБ ЯК ІНСТРУМЕНТІВ ПОРУШЕННЯ КІБЕРБЕЗПЕКИ

Биби́к Рома́н

*асистент кафедри Захисту інформації Національного університету
«Львівська Політехніка»*

У роботі розглянуто сучасні засоби радіоелектронної боротьби (РЕБ) як інструменти порушення кібербезпеки. Проаналізовано ключові типи технологій РЕБ, їхній вплив на інформаційні системи, зокрема на конфіденційність, цілісність і доступність даних. Наведено приклади використання РЕБ для атак на критичну інфраструктуру та в умовах гібридних конфліктів. Окрему увагу приділено методам захисту від таких загроз, включаючи застосування шифрування, захист радіочастотного спектра та інструментів штучного інтелекту для моніторингу й нейтралізації атак. Зроблено висновки щодо актуальних викликів та перспектив розвитку систем кіберзахисту в умовах радіоелектронного впливу.

1. Вступ

Сучасний світ характеризується стрімким розвитком інформаційних технологій, що одночасно створює нові можливості та загрози для кібербезпеки. У цьому контексті засоби радіоелектронної боротьби (РЕБ) набувають особливого значення, оскільки вони здатні не лише впливати на фізичну інфраструктуру, а й становити серйозну загрозу інформаційним системам. Технології РЕБ дозволяють перехоплювати, глушити або спотворювати сигнали, що може призводити до втрати конфіденційності, порушення цілісності даних та блокування доступу до інформації. Метою цієї роботи є аналіз сучасних засобів РЕБ, їхнього впливу на кібербезпеку, а також визначення ефективних методів протидії цим загрозам. У дослідженні висвітлюються ключові аспекти застосування РЕБ, як інструментів порушення безпеки інформаційних систем, а також можливості інтеграції новітніх технологій для забезпечення захисту.

2. Основні засоби РЕБ та їх вплив на кібербезпеку

Сучасні засоби радіоелектронної боротьби (РЕБ) активно використовуються для впливу на інформаційні системи та порушення кібербезпеки.

Вони працюють через маніпуляції радіочастотним спектром, порушуючи конфіденційність, цілісність і доступність даних.

Класифікація основних засобів РЕБ:

Тип засобів РЕБ	Принцип дії	Вплив на кібербезпеку
Глушіння сигналів	Генерація перешкод для передачі даних	Порушення зв'язку, втрати критичних систем
Перехоплення сигналів	Зчитування даних із відслабко захищених каналів	Витік конфіденційної інформації
Спотворення сигналів	Зміна або підробка даних дачі	Порушення цілісності даних, атак на управління системою
Атаки на GPS-системи	Глушіння або підробка сигналів	Порушення роуту логістики, втрати орієнтації

Засоби РЕБ створюють серйозні загрози для систем кібербезпеки, особливо у критичних інфраструктурах. Наприклад, глушіння сигналів в енергетичних або транспортних мережах може призвести до серйозних збоїв і втрат.

3. Приклади порушення кібербезпеки через засоби РЕБ

Атаки на критичну інфраструктуру

Засоби радіоелектронної боротьби (РЕБ) активно використовуються для порушення роботи критичних елементів інфраструктури, таких як енергетичні системи, транспортні мережі, телекомунікації та медичні установи. Приклади таких атак:

- **Порушення енергопостачання:** РЕБ може використовуватись для впливу на системи управління електромережами, що призводить до збоїв у подачі електроенергії. Такі атаки можуть бути реалізовані шляхом створення перешкод для сигналів зв'язку між диспетчерськими центрами та генераторами.

- **Вплив на системи громадського транспорту:** Блокування сигналів GPS або радіозв'язку може порушити роботу залізничного транспорту, авіації або морського судноплавства, створюючи загрози для безпеки пасажирів і вантажів.

- **Перешкоди в телекомунікаційних мережах:** РЕБ використовується для створення шумових сигналів, які блокують мобільний зв'язок або доступ до Інтернету, що особливо критично під час надзвичайних ситуацій.

Використання РЕБ у гібридних конфліктах

У сучасних гібридних війнах засоби РЕБ стали невід'ємною складовою атак, спрямованих на дестабілізацію ситуації в країні. Зокрема:

- **Дезінформація:** Перехоплення та модифікація сигналів зв'язку дозволяють поширювати фейкову інформацію серед військових або цивільного населення.

- **Зрив роботи військових систем:** Використання РЕБ для блокування зв'язку між підрозділами або управління безпілотними апаратами знижує ефективність військових операцій.

- **Порушення роботи інформаційних систем:** Вплив на сервери або центри обробки даних через РЕБ може призводити до втрати або викривлення важливої інформації.

Методи захисту від атак РЕБ

Для зменшення впливу засобів РЕБ на кібербезпеку розроблено низку підходів, що включають технологічні, організаційні та тактичні заходи:

Технологічні заходи:

- Використання **захищених протоколів зв'язку** з інтегрованими алгоритмами шифрування.

- Розробка **адаптивних систем зв'язку**, які здатні автоматично змінювати частоти або маршрути передачі сигналу.

- Впровадження **резервних каналів зв'язку** для забезпечення надійної комунікації навіть під час атак РЕБ.

Організаційні заходи:

- Регулярні **навчання персоналу** з протидії атакам РЕБ.

- Проведення **аудиту інфраструктури**, спрямованого на виявлення слабких місць у системах кіберзахисту.

- Створення **центрів моніторингу активності РЕБ** для оперативного реагування на загрози.

Тактичні заходи:

- Використання **географічно розподілених систем**, які складніше одночасно вивести з ладу.

- Розробка стратегій **активної протидії РЕБ**, що передбачають нейтралізацію джерел перешкод.

Приклади успішного захисту

Одним із прикладів успішного захисту від атак РЕБ є впровадження когнітивних радіомереж, які автоматично аналізують спектр частот у реальному часі та адаптують параметри передачі сигналу для мінімізації впливу перешкод. Такі технології вже використовуються в оборонних і цивільних системах зв'язку в провідних країнах світу.

Методи захисту від РЕБ залишаються важливою частиною забезпечення надійності та стійкості кіберінфраструктури, особливо в умовах зростаючих гібридних загроз.

4. Методи захисту від атак РЕБ

Шифрування та захист радіочастотного спектра

Один із ключових методів захисту від атак засобів радіоелектронної боротьби (РЕБ) — це використання сучасних технологій шифрування та ме-

ханізмів захисту радіочастотного спектра. Ці заходи дозволяють мінімізувати вплив перешкод і запобігти перехопленню або викривленню інформації.

Шифрування даних:

- Шифрування дозволяє захистити дані, що передаються через радіо-канали, від перехоплення і розшифровки. Використання сучасних алгоритмів шифрування, таких як AES-256 або квантове шифрування, гарантує високий рівень безпеки навіть за умов активного радіоелектронного впливу.

Захист спектра:

- Застосування **динамічного управління частотами** допомагає уникати перешкод, автоматично змінюючи частоту передачі у разі виявлення втручання.

- Технології **розширеного спектра сигналу** (Spread Spectrum) дозволяють рівномірно розподілити енергію сигналу по широкому діапазону частот, що ускладнює його виявлення та блокування засобами РЕБ.

- Використання **технологій ультраширококулового зв'язку (UWB)** забезпечує високу стійкість до перешкод завдяки низькій потужності сигналу і широкій смузі частот.

Використання штучного інтелекту для моніторингу загроз

Штучний інтелект (ШІ) стає невід'ємною частиною сучасних систем захисту від РЕБ. Інтеграція алгоритмів машинного навчання дозволяє значно підвищити ефективність моніторингу та нейтралізації загроз.

- **Автоматичне виявлення атак:** ШІ-системи аналізують радіочастотний спектр у реальному часі та виявляють аномалії, що можуть свідчити про атаку РЕБ. Це дозволяє оперативно ідентифікувати джерела перешкод.

- **Прогнозування загроз:** Застосування методів машинного навчання на основі великих обсягів даних дозволяє передбачати можливі дії противника та завчасно підготувати захисні заходи.

- **Оптимізація управління ресурсами:** ШІ допомагає оптимізувати використання частотного спектра та мережевих ресурсів, автоматично переналаштовуючи канали зв'язку для зниження впливу перешкод.

Інтеграція технологій у системи кібербезпеки

Ефективний захист від атак РЕБ можливий лише за умови комплексного підходу, який включає інтеграцію технологій захисту радіочастотного спектра та штучного інтелекту в системи кібербезпеки. Такі системи повинні забезпечувати:

- Постійний моніторинг радіочастотного середовища.
- Швидке виявлення та блокування джерел перешкод.
- Гнучке управління частотами та каналами зв'язку.

Перспективи розвитку захисту від атак РЕБ

Перспективні дослідження спрямовані на розробку когнітивних радіомереж, які поєднують технології ШІ та динамічного управління спектром. Це дозволить створювати системи, здатні адаптуватися до змін у реальному часі, підвищуючи їхню стійкість до впливу РЕБ.

Інноваційні рішення у сфері захисту від РЕБ сприяють зміцненню кібербезпеки як у військовій, так і в цивільній сфері, забезпечуючи стабільність критичних інфраструктур навіть в умовах радіоелектронного впливу.

5. Висновки

У результаті проведеного дослідження було встановлено, що засоби радіоелектронної боротьби (РЕБ) є серйозною загрозою для кібербезпеки сучасних інформаційних і комунікаційних систем. Основні аспекти, які були розглянуті:

- Засоби РЕБ здатні порушувати роботу критичної інфраструктури, блокувати зв'язок, дезінформувати та сприяти втраті даних.
- Використання РЕБ у гібридних конфліктах значно підвищує ризики для інформаційної безпеки, особливо в умовах складних міждержавних відносин.
- Для захисту від атак РЕБ розробляються технологічні рішення, такі як шифрування даних, адаптивні системи зв'язку та штучний інтелект, які ефективно мінімізують вплив перешкод і забезпечують стабільність комунікаційних мереж.

Розробка інноваційних методів захисту від засобів РЕБ, зокрема з використанням штучного інтелекту, дозволить забезпечити стійкість як цивільних, так і військових систем у складних умовах сучасного інформаційного середовища. Важливим є комплексний підхід, що включає не лише технологічні рішення, а й організаційні заходи для підвищення рівня кібербезпеки.

Список використаних джерел:

1. Гайдук, В. М. Радіоелектронна боротьба у військових конфліктах. Київ: НВФ "Авіа-прес", 2022.
2. Коваленко, А. І. Системи захисту інформації: технології та методи протидії. Харків: Видавництво ХНУРЕ, 2021.
3. Петриченко, Ю. Г., Сидоренко, М. П. **Штучний інтелект у системах радіоелектронної боротьби** // Науковий вісник Одеської національної академії зв'язку, 2023, №4, с. 22-28.
4. **Electronic Warfare and Cybersecurity Integration** // IEEE Communications Magazine, 2022, Vol. 60, Issue 10, pp. 45–51.
5. Zhao, Y., Wang, J., & Zhang, Q. Cognitive Radio Networks for Spectrum Management in Electronic Warfare // Journal of Defense Technology, 2023, Vol. 19, Issue 2, pp. 89–97.
6. Miller, D. P. Encryption Techniques for Secure Communication in the Face of Jamming Attacks // Cybersecurity Advances, 2021, Vol. 8, pp. 128–135.
7. Manual on the Use of Artificial Intelligence in Countering EW Threats. NATO Science and Technology Organization, 2023.

8. Шматко, І. О. Кіберзахист критичної інфраструктури в умовах гібридних загроз. Львів: Видавництво ЛНУ, 2020.
9. Gordon, R. J. Modern EW: From Jamming to Information Dominance. Cambridge: MIT Press, 2022.
10. Artificial Intelligence in EW and Cyber Defense Systems. Report by RAND Corporation, 2023.

Ключові слова: Радіoeлектронна боротьба(РЕБ), кібербезпека, штучний інтелект, захист радіочастотного спектра, шифрування даних, гібридні конфлікти, моніторинг загроз.

Keywords: Electronic warfare (REW), cybersecurity, piece intelligence, radio frequency spectrum protection, data encryption, hybrid conflicts, threat monitoring.

ЗАСТОСУВАННЯ АЛГОРИТМУ МАШИННОГО НАВЧАННЯ ISOLATION FOREST ДЛЯ ВИЯВЛЕННЯ АНОМАЛЬНИХ ДІЙ КОРИСТУВАЧІВ

Лабур Ярослав

студент 4 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Існує кілька загроз і проблем, що виникають при впровадженні генеративного штучного інтелекту в програмуванні, особливо в області аномалій і безпеки даних, особливо якщо це вимагає використання алгоритмів машинного навчання для захисту безпеки [1].

Демонстраційний код використовує метод неконтрольованого навчання під назвою Isolation Forest для виявлення аномальних дій користувача на основі його попередніх дій (або профілю). Він складається з декількох кроків: збір даних, попередня обробка даних, аналіз поточних даних та їх порівняння з профілем користувача і останній крок - визначення аномалій.

Наведемо опис коду по кроках:

1. Оскільки ми будемо використовувати різні бібліотеки, спочатку ми імпортуємо їх у наш скрипт.

```
import pandas as pd
from sklearn.ensemble import IsolationForest
from datetime import datetime
```

Pandas має працювати з таблицями DataFrame, які полегшують обробку даних.

IsolationForest з sklearn.ensemble - це алгоритм, який використовується для виявлення викидів.

- Він може бути інстанційований як datetime для створення та маніпулювання датами і часом.

2. Минулі записи у вигляді звичного профілю активності.

```
historical_data = {'user_id'
```

```

«user_id": [101, 101, 102, 102, 103],
common_ip: Loggedcandidates: [192.168.1.1, 192.168.1.1, 192.168.1.2,
192.168.1.2, 192.168.1.3],
«звичайний_часовий_зон»: [UTC + 2, UTC + 2, UTC + 2, UTC + 2, UTC +
2, UTC + 4].
sensitive_access_count: [3, 3, 2, 2, 1]
}
profile_df = pd.DataFrame(historical_data).

```

Включає ідентифікатор кожного користувача та його ID з такою інформацією, як звичайна IP-адреса; звичайний час; кількість доступів до конфіденційних даних.

«profile_df» - це DataFrame для зберігання цих історичних даних.»

3. Поточні дані журналу для аналізу

```

current_data = {
timestamp: [2024-11-07 08:12, 2024-11-07 08:15, 2024-11:30, 2024-11-07
09:00.

```

```

«user_id»: [101, 102, 101, 103],
«operation»: Вхід, доступ до файлу, видалення файлу, вхід
ip_address: [192.168.1.1, 192.168.1.2, 192.168.1.1, 192.168.1.4]
«часовий пояс»: [ UTC + 2 години, UTC + 2 години, UTC + 2 години, UTC
+ 2 години, UTC + 4 години ]
data_sensitivity: [0, 1, 1, 0]
}
df = pd.DataFrames(current_data)

```

Ці дані також включають нову активність користувача, яка ретельно перевіряється на відповідність профілю.

«df» включає час дії або операції, ідентифікатор користувача, характер операції, IP-адресу, часовий пояс, в якому він знаходиться, і вказівку на чутливість даних.

4. Обробка тимчасових даних

```

df[timestamp] = pd.to_datetime(df[timestamp])
де, df[hour] = df[timestamp].dt.hour

```

Перетворює значення «мітки часу» у формат дата-час, а потім використовує функцію hour для виведення часу активності користувача.

5. Кодування текстових даних

```

df[код_операції] = pd.Categorical(df[операція]).codes
df[ip_code] = np.factorize(df[ip_address])[0]
to[timezone_code] = pd.factorize(to[timezone])[0].

```

Переводить текстові вхідні дані (operation, ip_address, timezone) у числову форму, що полегшує їх сприйняття алгоритмами машинного навчання.

6. Злиття з профілем користувача

```
df = df.merge(profile_df, on=user_id, how=left)
```

- Зливає поточні дані з профілем користувача на основі user_id, додаючи звичну IP-адресу, часову зону та інші параметри з профілю.

7. Додавання характеристик для порівняння з профілем

```
df[unusual_ip] = (df[ip_address] != df[common_ip]).astype(int)
```

```
df[unusual_timezone] = (df[timezone] != df[usual_timezone]).astype(int)
```

```
df[high_sensitive_access] = (df[data_sensitivity] > 0).astype(int)
```

- unusual_ip показує, чи збігається IP-адреса з профілем.

- unusual_timezone перевіряє відповідність часової зони профілю.

- high_sensitive_access позначає доступ до конфіденційних даних.

8. Вибір характеристик для моделі

```
features = df[[user_id, operation_code, ip_code, timezone_code, data_sensitivity, hour, unusual_ip, unusual_timezone, high_sensitive_access]]
```

- Виділяє всі ключові характеристики, які будуть використовуватися для навчання моделі.

9. Налаштування і навчання моделі Isolation Forest

```
model = IsolationForest(contamination=0.1, random_state=42)
```

```
df[anomaly_score] = model.fit_predict(features)
```

- IsolationForest навчається на вибраних характеристиках. Аномалії (підозрілі дії) позначаються як -1.

10. Виведення потенційних загроз

```
anomalies = df[df[anomaly_score] == -1]
```

```
print(Потенційні загрози для перевірки:\n, anomalies[[timestamp, user_id, operation, ip_address, timezone, data_sensitivity, unusual_ip, unusual_timezone, high_sensitive_access]])
```

- Виводяться всі дії, які модель визначила як аномальні для подальшої перевірки (рис. 1):

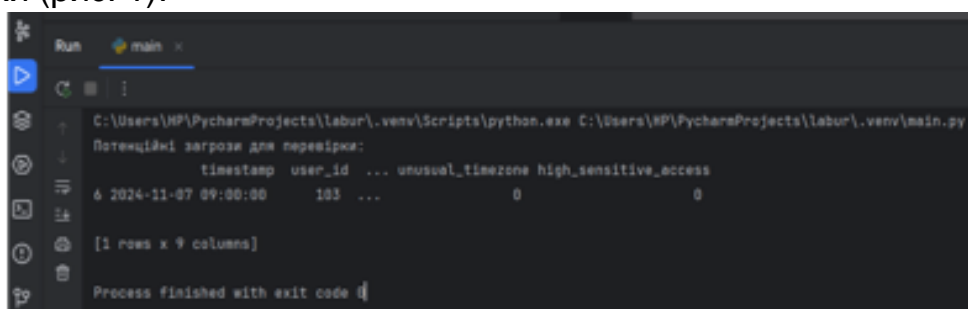


Рис. 1 Вивід результату в терміналі

Цей код порівнює нову активність користувача з типовою поведінкою користувача, а потім використовує IsolationForest для виявлення аномальної поведінки. Дії відтворюються аномально, щоб підтвердити і, зрештою, допомогти у виявленні загроз безпеці.

Список використаних джерел:

1. Бойко, В., Василенко, М., Слатвінська, В. (2023). Програмування за допомогою систем генеративного штучного інтелекту: ризики та виклики. Інформаційні технології та суспільство, 2 (8), С. 18–26. DOI: <https://doi.org/10.32689/maup.it.2023.2.2> URL: <http://journals.maup.com.ua/index.php/it/article/view/2664> (дата звернення: 09.11.2024).

Ключові слова: штучний інтелект, загрози, кібербезпека.

Keywords: artificial intelligence, threats, cybersecurity.

Науковий керівник: доктор філософії, асистент кафедри кібербезпеки
Слатвінська В.М.

ВИКОРИСТАННЯ МЕРЕЖЕВОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ ПРИХОВАНИХ ЗАКОНОМІРНОСТЕЙ У ВЕЛИКИХ ДАНИХ

Савенко Михайло

студент 1 курсу магістратури, спеціальність 124 «Системний аналіз»
Національного університету «Одеська юридична академія»

У сучасному світі обсяги даних зростають з кожним роком, що ставить нові виклики перед науковцями та аналітиками. Одним із потужних методів для вивчення складних систем, у яких важливі взаємозв'язки між окремими елементами, є мережевий аналіз даних. Мережевий аналіз дає змогу будувати моделі соціальних, біологічних, економічних та багатьох інших систем, досліджуючи зв'язки між їхніми компонентами та виявляючи приховані закономірності.

Мережевий аналіз даних базується на теорії графів, що дозволяє досліджувати зв'язки між різними об'єктами. Основними елементами будь-якої мережі є вузли (вершини) та зв'язки (ребра). Вузли представляють об'єкти, наприклад, людей, гени або компанії, тоді як зв'язки між ними показують взаємодії, такі як дружба, генетичні зв'язки або економічні відносини.

Існують різні типи мереж, залежно від характеру зв'язків. В орієнтованих мережах зв'язки мають напрямок: наприклад, у Twitter можна слідкувати за людиною, яка, у свою чергу, може не слідкувати за вами, що створює односторонній зв'язок. У неорієнтованих мережах зв'язки не мають напрямку, як у випадку з Facebook, де дружба є взаємною. Інший критерій — вага зв'язків. У вагових мережах кожен зв'язок має значимість або вагу, яка може відображати, наприклад, частоту комунікації або обсяг торгівлі. У невагових мережах зв'язки рівнозначні й не мають ваги.

Мережевий аналіз використовує різноманітні метрики для оцінки властивостей вузлів та зв'язків. Однією з найпростіших метрик є ступінь вузла, який відображає кількість зв'язків, що приєднані до цього вузла. Вузли з ви-

соким ступенем можуть вказувати на важливість або впливовість елемента у мережі. Центральність є ще одним показником значущості вузла і буває декількох видів: ступенева центральність відображає кількість зв'язків вузла, міжпосередницька центральність показує, скільки разів вузол знаходиться на найкоротшому шляху між іншими вузлами, а близькісна центральність визначає, наскільки близько вузол розташований до інших вузлів мережі.

Кластеризація або кластерний коефіцієнт показує, наскільки вузли в мережі мають схильність утворювати щільно пов'язані групи. Високий коефіцієнт кластеризації свідчить про наявність щільних спільнот або груп вузлів у мережі. Ще одним важливим параметром є середня довжина шляху, яка визначає середню відстань між будь-якими двома вузлами в мережі та допомагає оцінити швидкість поширення інформації.

Одним із завдань мережевого аналізу є виявлення спільнот або кластерів — груп вузлів, які мають більше зв'язків один з одним, ніж з іншими частинами мережі. Спільноти можуть вказувати на наявність тісніших взаємозв'язків у певних частинах мережі, наприклад, дружні групи в соціальних мережах або групи генів, що взаємодіють у біологічних процесах. Показник модульності визначає якість розбиття мережі на спільноти: висока модульність свідчить про щільні зв'язки всередині груп та рідкісні зв'язки між ними, що допомагає виявити природний розподіл мережі на підструктури.

Поняття вузлів, зв'язків та метрик допомагають формалізувати і оцінити структуру мереж, а також виявляти ключові компоненти й закономірності. Використання таких метрик є важливим для розуміння складних систем, оскільки дозволяє аналізувати їхні властивості, прогнозувати динаміку та виявляти приховані взаємозв'язки у великих обсягах даних. Це робить мережевий аналіз цінним інструментом у багатьох галузях, включаючи соціологію, біологію, кібербезпеку та економіку [1].

Методи мережевого аналізу

Мережевий аналіз даних базується на трьох основних методах: графічних, алгоритмічних та кластерному аналізі. Кожен з них дозволяє вивчати та інтерпретувати структури взаємодій у системі та виявляти приховані зв'язки між елементами.

Графічні методи

Графічні методи є важливою частиною мережевого аналізу, оскільки вони дають змогу візуалізувати зв'язки у вигляді графів. Граф є діаграмою, де вузли представляють елементи, а ребра — зв'язки між ними. Графічна модель дозволяє виявляти ключові елементи у мережі, їхні зв'язки та характер взаємодії. Візуалізація дає можливість аналізувати структуру мережі інтуїтивніше, ніж абстрактні числові показники, і є основою для подальшого аналізу.

Для візуалізації мереж використовуються графи — графічні моделі, що дають змогу представити зв'язки між вузлами у вигляді діаграми. Візуалізація допомагає аналізувати мережі інтуїтивніше, виявляючи значимі вузли, кластерні структури та інші особливості [2].

Алгоритмічні методи

Алгоритмічні методи використовуються для вирішення конкретних завдань, таких як знаходження найкоротших шляхів між вузлами або аналіз зв'язності мережі. Наприклад, алгоритм Дейкстри дозволяє обчислювати найкоротші шляхи, що корисно в транспортних або комунікаційних мережах, коли потрібно мінімізувати витрати. Інші алгоритми, такі як пошук у ширину або глибину, дозволяють визначити компоненти зв'язності у мережі — частини, що є внутрішньо зв'язаними і не мають зв'язків із зовнішніми вузлами. Ці алгоритми допомагають виявити ключові вузли або структури, що можуть бути важливими для досліджуваної системи.

Важливими алгоритмами є:

- **Алгоритм Дейкстри:** для знаходження найкоротших шляхів між вузлами [3].
- **Алгоритм Брезена (BFS/DFS):** для пошуку в ширину/глибину, що використовується для аналізу зв'язності мережі.
- **Компоненти зв'язності:** частини мережі, які є зв'язаними та не мають зв'язків із зовнішніми елементами [4].

Кластерний аналіз

Кластерний аналіз є методом, що дозволяє виявляти групи вузлів, які мають сильні зв'язки між собою порівняно з іншими вузлами у мережі. Такі групи називають кластерами або спільнотами. Кластерний аналіз є важливим інструментом у дослідженні соціальних мереж, де важливо розуміти структуру спілкування між групами людей. Також цей метод застосовується у біологічних мережах для виявлення груп генів або білків, що взаємодіють між собою у схожий спосіб.

Кластерний аналіз дозволяє виділяти групи вузлів, які мають тісніші зв'язки між собою, ніж з іншими вузлами мережі. Це корисно для аналізу соціальних груп, спільнот у біологічних мережах, а також виявлення підгруп у великих організаціях чи колективах.

Використання зазначених методів дозволяє досліджувати мережі з різних перспектив і допомагає отримати цінну інформацію про структуру та функціонування складних систем. Кожен із методів має свої переваги, і їх комбінація дає можливість комплексно підходити до мережевого аналізу [5].

Приклади використання мережевого аналізу

Соціальні мережі. Аналіз соціальних мереж дозволяє визначити ключових користувачів, які мають найбільший вплив, або дослідити розповсюдження інформації серед користувачів, виявити популярних лідерів думок.

Біологія. У біології мережевий аналіз використовується для дослідження білкових та генетичних взаємодій, що дозволяє визначати зв'язки між генами, білками та іншими біологічними компонентами.

Економіка та бізнес. Ланцюги постачання можуть бути представлені у вигляді мереж, де кожен вузол є підприємством, а зв'язки — економічними взаємодіями. Це дозволяє аналізувати взаємозалежність компаній та виявляти ключових гравців ринку.

Кібербезпека. У сфері кібербезпеки мережевий аналіз використовується для виявлення зв'язків між кіберзагрозами та ідентифікації можливих атак.

Інструменти для мережевого аналізу

Для проведення мережевого аналізу існує багато спеціалізованих інструментів, що дозволяють не лише проводити обчислення, а й візуалізувати мережеві структури та спрощують інтерпретацію результатів. Ось кілька найпопулярніших програм та бібліотек, що використовуються для роботи з мережами:

Gephi є одним із найпоширеніших інструментів для візуалізації та аналізу великих мереж. Gephi відомий своєю здатністю працювати з великими наборами даних і створювати інтуїтивні та привабливі візуалізації мереж. Інструмент пропонує широкі можливості для налаштування стилів вузлів, ребер та кольорів, що дозволяє створювати складні діаграми мереж. Завдяки своїй гнучкості, Gephi використовується у багатьох галузях, включаючи соціальні науки, біологію, та економіку, де важлива візуальна інтерпретація взаємодій між елементами.

NetworkX — це бібліотека для мови програмування Python, яка дозволяє створювати, аналізувати та візуалізувати складні мережі. NetworkX є популярним вибором для дослідників та аналітиків, які прагнуть використовувати програмування для детальнішого аналізу мережевих структур. Бібліотека підтримує роботу з різними типами графів, включаючи орієнтовані, неорієнтовані, вагові та багатoshарові графи. NetworkX надає широкий набір функцій для обчислення центральності, кластеризації, пошуку найкоротших шляхів та інших метрик мережевого аналізу. Її гнучкість та інтеграція з іншими бібліотеками Python роблять її важливим інструментом для наукових досліджень та аналітичних проектів.

Cytoscape — спеціалізована програма, яка використовується переважно для аналізу біологічних мереж. Ця програма популярна серед генетиків та молекулярних біологів, оскільки дозволяє візуалізувати складні взаємодії між

генами, білками та іншими біомолекулами. Cytoscape має розширювану архітектуру, що дозволяє користувачам додавати нові плагіни для спеціалізованих завдань, таких як аналіз геномних даних або вивчення метаболічних шляхів. Ця гнучкість робить Cytoscape ефективним інструментом для глибокого аналізу біологічних мереж, де важливим є вивчення складних зв'язків у клітинних процесах [6].

Кожен із цих інструментів має свої унікальні переваги та призначений для певних типів мережевого аналізу. Використання Gephi підходить для візуалізації та швидкого аналізу великих мереж. NetworkX є відмінним вибором для програмістів, що потребують високого рівня налаштування та інтеграції з іншими інструментами Python. Cytoscape забезпечує спеціалізовані функції для біологічних досліджень, пропонуючи багаті можливості для аналізу молекулярних взаємодій.

Мережевий аналіз даних є надзвичайно важливим інструментом для вивчення складних систем. Завдяки своїм методам він дозволяє структурувати великі обсяги даних, що виникають у різних галузях науки та практики. Перспективи його використання включають розробку нових алгоритмів, адаптованих під специфічні завдання, а також інтеграцію з іншими технологіями, такими як машинне навчання та штучний інтелект, для більш глибокого аналізу.

Список використаних джерел:

1. Аналіз метрик для інтелектуальних інформаційних систем Віктор Григорович URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2021/jun/23829/0210544infmarket-01-07-98-113.pdf> (дата звернення 6.11.2024).
2. Левченко, О. С. Кластерний аналіз та його застосування в соціальних мережах. Літературні студії, 23(4), 85-101. (2018).
3. Алгоритм Дейкстри URL: <https://disted.edu.vn.ua/media/doc/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%20%D0%94%D1%96%D0%B5%D0%BA%D1%81%D1%82%D1%80%D0%B8.pdf> (дата звернення 6.11.2024).
4. MIT - BFS/DFS: Пошук у ширину і глибину URL: <https://courses.csail.mit.edu/6.006/spring11/rec/rec12.pdf> (дата звернення 6.11.2024).
5. Кластеризація: методика та практична реалізація. Аршава Олена URL: https://www.researchgate.net/publication/370737592_KLASTERIZACIA_METODIKA_TA_PRAKTICNA_REALIZACIA (дата звернення 6.11.2024).
6. Інструменти для тестування мережевого трафіку та безпеки URL: <https://hackyourmom.com/kibervijna/instrumenty-dlya-testuvannya-merezhevogo-trafiky-ta-bezpeky/> (дата звернення 6.11.2024).

Ключові слова: мережевий аналіз, інструменти мережевого аналізу, кластерний аналіз, мережевий аналіз даних

Keywords: network analysis, network analysis tools, cluster analysis, network data analysis

Науковий керівник: К.Т.Н., доцент Задерейко Олександр

ВИКОРИСТАННЯ PYTHON ДЛЯ АНОНІМІЗАЦІЇ ВЕБ-ЗАПИТІВ

Москаленко Олексій

*студент 4 курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

Розробляючи методи анонімізації запитів до Python з кінцевою метою використання їх для дослідження шкідливого програмного забезпечення, необхідно враховувати сучасні методи виявлення шкідливого програмного забезпечення, оскільки методи анонімізації можуть бути використані як в хороших, так і в поганих цілях. С.В. Кухаренко та В.М. Слатвінська зазначають: «Сучасні техніки виявлення шкідливого коду значно вдосконалилися, що робить необхідним поглиблений аналіз функціоналу Python для зменшення вразливостей» [1]. Це особливо важливо для розуміння того, як анонімізація може забезпечити не тільки конфіденційність користувачів, а й служити інструментом для виявлення підозрілих запитів.

Демонстраційний код запропонованого методу просто надсилає анонімний HTTP-запит до веб-сайту, використовуючи бібліотеку запитів. Він змінює User-Agent (ідентифікатор браузера), що може допомогти приховати справжній браузер або пристрій, який використовується для запиту сторінки. Ось детальне пояснення:

1. Імпорт бібліотек:

запити на імпорт

з довільного вибору імпорту

- запитів: Окрема бібліотека для iOS зроблена відповідно до HTTP запиту на мові Python.

- вибір з випадкового: Функція для вибору елемента випадковим чином зі списку і використовувалася для вибору випадкового User-Agent зі створеного списку.

2. Список USER_AGENTS:

USER_AGENTS = [

Пошта: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, як Gecko) Chrome/85.0.4183.121 Safari/537.36.

Chrome 80.0.3987.149 Safari 605.1.15 на Mac OS X,

Mozilla/5.0 (Linux; Android 10; SM-G973F) AppleWebKit/537.36 (KHTML, як Gecko) Chrome/83.0.4103.106 Mobile/Safari/537.36

Додайте додаткових агентів користувача

]

Цей список включає кілька рядків User-Agent, які імітують запити, що надходять від різних браузерів і пристроїв (наприклад, Windows, Mac, Android).

User-Agent - це ідентифікатор, який використовується в HTTP-запитах і відповідях як інформація про клієнтську програму, яка може допомогти вам замаскувати особистість під час перегляду веб-сторінок.

3. Функція `get_random_user_agent()`:

```
def get_random_user_agent():  
    return choice(USER_AGENTS)
```

- Використовує `choice(USER_AGENTS)` для випадкового вибору агента користувача зі списку `USER_AGENTS`.

Це допомагає зробити кожен запит дещо відмінним, а отже, набагато складнішим для відстеження.

4. Функція `send_anonymous_request(url)`:

```
def send_anonymous_request(url):  
    headers = {}  
    User-Agent: get_random_user_agent(),  
}
```

- Це формує словник `headers`, який додає User-Agent, отриманий за допомогою `get_random_user_agent()`, для кожного запиту.

Параметр `headers` передається разом із запитом, щоб замаскувати інформацію про User-Agent за замовчуванням.

5. Виконайте запит:

```
try:  
    response = requests.get(url, headers=headers, timeout = 5)  
    response.raise_for_status()  
    return response.text  
except requests.exceptions.RequestException as e:  
    print(f 'Помилка: {e}')  
    return None
```

Виконує HTTP-запит методом GET на заданий url з випадковим U-A.

- `timeout=5` означає, що максимальний час очікування відповіді на деякий запит становить 5 секунд.

Нарешті, згідно з об'єктом `response`, якщо запит пройшов успішно, повертає текст відповіді. У випадку помилки (наприклад, сервер недоступний), обробка помилки буде виконана в блоці `except`, а повідомлення про помилку буде занесено до журналу.

6. Використання функції `send_anonymous_request`:

```
url = 'https://httpbin.org/ip' # перевірка ip-адреси  
response = make_a_request(url, anonymous=True)  
if response:  
    print('Відповідь сервера:', response)
```

- Призначає url для перевірки IP-адреси за допомогою `httpbin.org`.

Два виклики `send_anonymous_request(url)` виводять на друк результати, які представляють сприйняття сервером вашого запиту, такі як IP-адреса та User-Agent.

Цей код допомагає в тих простих випадках, коли користувач хоче замаскувати себе при виконанні веб-запитів і коли ви знаєте, що деякі сайти відстежують вас за допомогою вашого User-Agent.

Список використаних джерел:

1. Кухаренко С.В., Слатвінська В.М. Аналіз функціоналу Python keylogger: від розуміння до виявлення шкідливого коду. *Наука і техніка сьогодні*. 2024. № 11. С. 926-940. DOI: [https://doi.org/10.52058/2786-6025-2024-11\(39\)-926-940](https://doi.org/10.52058/2786-6025-2024-11(39)-926-940) URL: <http://perspectives.pp.ua/index.php/nts/article/view/15909/15981> (дата звернення: 09.11.2024).

Ключові слова: анонімність, кібербезпека, Python.

Keywords: anonymity, cybersecurity, Python.

Науковий керівник: доктор філософії, асистент кафедри кібербезпеки Слатвінська В.М.

КІБЕРБЕЗПЕКА АВТОНОМНИХ ДРОНІВ: ЗАХИСТ ВІД АТАК НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Новосельський Дмитро

студент 1 курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Інтеграція штучного інтелекту (ШІ) у автономні дрони значно підвищує їхню ефективність, роблячи їх незамінними інструментами для служб безпеки, швидкого реагування та інших критично важливих операцій. Дрони з ШІ здатні обробляти великі обсяги даних у реальному часі. Вони аналізують отриману візуальну інформацію і автоматично приймають рішення. Однак, зі збільшенням рівня автономності дронів зростають і їх вразливість для імовірних кіберзагроз, оскільки системи їх керування стають більш вразливими до кібератак. Захист автономних дронів, що базуються на ШІ, є ключовим елементом для забезпечення їхньої надійної та безпечної роботи [1].

Одним із найбільших ризиків є атаки на моделі ШІ, коли зловмисники можуть маніпулювати даними, які використовуються для навчання штатних систем ШІ, або змінювати вхідні дані, що може привести до помилкових рішень керування дроном. Такі атаки можуть спричинити збій у роботі дрона, або навіть зробити його неконтрольованим. Наприклад, зловмисники можуть змінити навігаційні дані, що змусить дрон відхилитися від заданого маршруту.

Ще однією серйозною загрозою є атаки типу відмова в обслуговуванні (DoS), коли зловмисники перенавантажують канал зв'язку з дроном, що при-

зводить до блокування його зв'язок з оператором. Це може призвести до припинення роботи дрону під час виконання критичних завдань. Окрім цього, дрони можуть бути вразливими до перехоплення сигналу або викрадення даних, що передаються якщо шифрування сигналу або захист каналу зв'язку недостатньо надійні. Це може дати зловмисникам можливість отримати доступ до передаваної інформації або взяти під контроль дрон [2].

Ще один приклад — атаки на дрони в аеропорту Гатвік (Велика Британія) у 2018 році, коли зловмисники використовували дрони для порушення роботи аеропорту, що спричинило затримку численних рейсів. Хоча це не була кібернетична атака, інцидент демонструє, як важливим є забезпечення контролю над дронами і їх захист від можливого перехоплення.

Дрони також покладаються на мережеві протоколи для обміну даними та управління, що робить їх вразливими до атак через експлойти. Недоліки у захисті цих протоколів можуть призвести до компрометації системи дрона, що створює загрозу для безпеки його операцій.

ШІ є ефективним інструментом не тільки для функціонування автономних дронів, але й для їхнього захисту від зловмисників. Одним із ключових методів є виявлення загроз у реальному часі. Алгоритми ШІ можуть постійно моніторити роботу дрона і виявляти аномальні дії, що свідчать про можливу атаку зловмисників. Це дозволяє виявляти спроби несанкціонованого втручання, такі як зміна маршруту або перехоплення сигналів. Наприклад, системи виявлення вторгнень, побудовані на ШІ, здатні швидко реагувати на підозрілу активність, передаючи попередження операторам або автоматично коригуючи дії дрона для запобігання загрозі.

Наприклад, американська армія використовує системи, що здатні виявляти і нейтралізувати спроби атак на безпілотні літальні апарати за допомогою ШІ. Такі системи можуть виявляти підозрілу активність і блокувати спроби перехоплення канали управління дронами, що дозволяє зберегти контроль над ними в умовах активного електронного впливу.

ШІ також забезпечує автономну адаптацію до загроз у реальному часі. Використовуючи алгоритми машинного навчання, дрони можуть швидко змінювати маршрути або частоти сигналів, щоб уникнути перешкод або атак. Це дозволяє їм бути гнучкими і реагувати на непередбачувані загрози. Крім того, криптографічний захист є ще одним важливим елементом у захисті дронів. ШІ може управляти процесами шифрування для забезпечення безпеки передачі даних між дроном і оператором. Це знижує ризик перехоплення даних або підробки команд, що надсилаються дрону [3].

Для захисту моделей ШІ від атак на рівні навчальних даних (adversarial attacks) використовуються механізми моніторингу та перевірки вхідних даних. Це дозволяє виявляти підозрілі або змінені дані та уникати маніпуляцій, що

можуть призвести до помилкових рішень, генеруємих ШІ дрона. Таким чином, захист на рівні моделі є важливою складовою для забезпечення надійності систем ШІ в автономних дронах.

ШІ також може допомогти в розробці контрзаходів проти зловмисників. Якщо система виявляє спробу атаки, вона може автоматично блокувати джерело атаки або використовувати інші механізми для захисту від зловмисного впливу.

Хоча автономні дрони з ШІ здатні самотійно виконувати складні завдання, роль оператора у контролі за їхньою роботою залишається важливою. Оператор повинен мати можливість втручатися в роботу дрона у разі виникнення критичних ситуацій або загроз. Це дозволяє зберігати відповідальність за прийняття рішень та забезпечувати дотримання етичних норм у роботі дронів. Особливо це стосується ситуацій, коли дрони використовуються для моніторингу або збору даних, що може порушувати приватність і конфіденційність людей.

Використання технологій ШІ, таких як розпізнавання обличчя, також вимагає дотримання правових і етичних норм, щоб уникнути вторгнення в приватне життя громадян. Це питання потребує ретельного регулювання з боку законодавства, а також прозорості в тому, як використовуються алгоритми ШІ в автономних дронах.

У перспективі використання ШІ для захисту дронів від кібератак буде лише розширюватися. Основні напрямки розвитку включають вдосконалення алгоритмів виявлення загроз та автоматизацію роботи систем їх захисту. Розвиток криптографічних систем на основі ШІ дозволить підвищити рівень захищеності передачі даних між дронами і центрами управління. Крім того, впровадження нових методів навчання з підкріпленням забезпечить адаптацію дронів до нових типів загроз, що зробить їх більш стійкими до кібератак [4].

Людський контроль за автономними дронами залишається важливим аспектом, який забезпечує безпеку їхньої роботи. Оператори повинні мати змогу контролювати дрон у будь-який момент і втручатися в його роботу за необхідності. Це допоможе зберігати баланс між автономністю дронів і контролем над їхніми діями.

Штучний інтелект є не лише основою для автоматизації роботи автономних дронів, але й потужним інструментом для їхнього захисту від кібератак. Використання алгоритмів для виявлення загроз, адаптація до нових викликів у реальному часі та криптографічний захист дозволяють забезпечити надійним зв'язок з дронами у складних умовах. Проте важливо зберігати баланс між автономністю і людським контролем, дотримуючись етичних і правових норм для забезпечення безпеки та конфіденційності даних.

Список використаних джерел:

1. Jay Stanley. Eye-in-the-Sky Policing Needs Strict Limits. American Civil Liberties Union, 2023. URL: [https:// www.aclu.org/documents/eye-in-the-sky-policingneeds-strict-limits](https://www.aclu.org/documents/eye-in-the-sky-policingneeds-strict-limits).
2. Robert DeLillo. "The Coast Guard Must Use Unmanned Aerial Systems and AI in Search and Rescue". In: Proceedings 149.7/1,445 (2023). URL: <https://www.usni.org/magazines/proceedings/2023/july/coast-guard-must-use-unmanned-aerial-systemsand-ai-search-and>.
3. ASUVI. AUVSI Partnership for Drone Competitiveness. White Paper. Association for Uncrewed Vehicle Systems International, 2022. URL: <https://www.auvsi.org/sites/default/files/AUVSI-Partnership-for-Drone-Competitiveness-White-Paper.pdf>.
4. Westheider, J.; Rueckin, J.; Popovic, M. Multi-UAV Adaptive Path Planning Using Deep Reinforcement Learning. In Proceedings of the 2023 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Detroit, MI, USA, 1–5 October 2023; pp. 649–656.

Ключові слова: кібератаки, дрони з ШІ, моделі машинного навчання, виявлення загроз, адаптивна безпека.

Keywords: cyberattacks, AI drones, machine learning models, threat detection, adaptive security.

Науковий керівник: *к.т.н., доц. Задерейко Олександр*

РОЗГЛЯД ТЕХНОЛОГІЙ BIG DATA ЯК ІНСТРУМЕНТУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОБОТИ ПІДПРИЄМСТВ РОЗДРІБНОЇ ТОРГІВЛІ

Осадчук Анастасія

*студентка 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

У сучасному конкурентному середовищі роздрібні компанії стикаються з проблемами, пов'язаними з динамічними змінами споживчих уподобань, високими очікуваннями покупців і необхідністю швидко реагувати на тенденції ринку. Використання технологій великих даних стає важливим інструментом підвищення ефективності роботи таких компаній. Збираючи, обробляючи й аналізуючи великі обсяги інформації, технології великих даних дають змогу ухвалювати стратегічні рішення, що сприяють оптимізації бізнес-процесів, зниженню витрат і підвищенню рентабельності.

Під великими даними розуміють великі обсяги структурованих і неструктурованих даних, зібраних із різних джерел, як-от дані про продажі, активність покупців в Інтернеті, соціальних мережах, мобільних додатках і програмах лояльності. Для опрацювання таких даних застосовуються спеціальні інструменти аналізу з використанням алгоритмів машинного навчання, штучного інтелекту і статистичних методів. У сфері роздрібної торгівлі великі дані

допомагають отримати цінні відомості про поведінку та вподобання споживачів, тенденції ринку та ефективність маркетингових кампаній [1].

Ключові сфери застосування великих даних у роздрібній торгівлі розглядаються у табл. 1.

Таблиця 1. Ключові сфери застосування великих даних та їхній опис

Ключові сфери застосування	Опис
Аналіз поведінки споживачів	Ритейлери активно використовують великі дані для збору інформації про своїх клієнтів, їхні покупки, відвідування магазинів, уподобання та інші параметри, щоб краще зрозуміти свою цільову аудиторію. Аналізуючи ці дані, можна сегментувати покупців і створювати персоналізовані пропозиції на основі різних характеристик, таких як вік, дохід, місце розташування.
Оптимізація асортименту та управління запасами	Аналіз великих даних може допомогти ритейлерам краще зрозуміти попит на конкретні товари, визначити популярні категорії товарів і знизити частку менш популярних продуктів. Впроваджуючи такі технології, компанії можуть поліпшити управління запасами, знизити витрати на зберігання і мінімізувати ризики.
Прогнозування продажів	За допомогою алгоритмів машинного навчання та аналітичних моделей, заснованих на історичних даних, технології великих даних дають змогу прогнозувати майбутній попит на товари та рівень продажів у різних магазинах і регіонах. Це дає змогу ритейлерам планувати ресурси, оптимізувати запаси і уникати ситуацій дефіциту та затоварення. Крім того, прогнози, засновані на великих даних, можуть допомогти в прийнятті рішень щодо цін, промоцій та інших маркетингових заходів.
Оптимізація ціноутворення	Великі дані дають змогу аналізувати різні фактори, що впливають на ціноутворення (ціни конкурентів, попит на продукцію, сезонність, промоакції та інші умови ринку). Використовуючи аналітичні алгоритми, компанії можуть встановлювати оптимальні ціни, які забезпечують максимальний прибуток при збереженні конкурентоспроможності. Динамічне ціноутворення на основі великих даних дозволяє оперативно реагувати на зміни на ринку.
Ефективність маркетингових кампаній	За допомогою великих даних компанії можуть аналізувати ефективність своїх маркетингових заходів і адаптувати їх для досягнення максимальних результатів. Наприклад, аналізуючи поведінку користувачів на веб-сайтах, у застосунках і соціальних мережах, можна створювати персоналізовані рекомендації та пропозиції.
Поліпшення обслуговування клієнтів	Аналіз даних про взаємодію клієнтів з бізнесом дає змогу поліпшити процеси обслуговування клієнтів, усуваючи найпоширеніші проблеми та запити. Наприклад, впровадження чат-ботів, заснованих на великих даних, може підвищити задоволеність клієнтів, дозволивши швидше відповідати на їхні запити.

Великі дані відіграють ключову роль у розвитку ритейлу, дозволяючи компаніям ефективніше працювати та краще взаємодіяти зі споживачами. Вони дають змогу аналізувати поведінку клієнтів, персоналізувати пропозиції, оптимізувати асортимент і управління запасами, прогнозувати попит і адаптуватися до змін на ринку [1-3]. Аналітичні алгоритми допомагають

встановлювати оптимальні ціни, підвищувати ефективність маркетингових кампаній та покращувати обслуговування клієнтів [4]. Використання великих даних підвищує конкурентоспроможність компаній, скорочує витрати і збільшує прибутковість бізнесу.

Впровадження технологій великих даних у роздрібній торгівлі приносить значні економічні та конкурентні переваги. Компанії, які активно використовують ці технології, можуть значно підвищити ефективність управління бізнес-процесами, скоротити витрати та оптимізувати асортимент продукції. Персоналізований підхід до клієнтів і більш ефективні маркетингові стратегії можуть значно підвищити лояльність покупців і задоволеність брендом [5]. Водночас впровадження великих даних вимагає значних інвестицій у технічну інфраструктуру, навчання персоналу та адаптацію бізнес-процесів. Однак довгострокова віддача від таких інвестицій у вигляді підвищення ефективності та прибутковості може значно переважити початкові витрати.

Отже, технологія великих даних – потужний інструмент для підвищення ефективності роздрібної торгівлі. Вона дає змогу оптимізувати управління асортиментом, прогнозувати продажі, створювати персоналізовані маркетингові кампанії та покращувати якість обслуговування клієнтів. Використання великих даних допомагає компаніям залишатися конкурентоспроможними та адаптуватися до швидких змін ринкового середовища, що зрештою сприяє їхньому сталому розвитку та успіху.

Список використаної літератури:

1. Вікіпедія. Великі дані. Електронний ресурс. URL: <http://surl.li/wdchkr> (дата звернення: 21.10.2024);
2. Big Data. Електронний ресурс. URL: <http://surl.li/krbfbk> (дата звернення: 21.10.2024);
3. Big Data. Що це таке? Електронний ресурс. URL: <http://surl.li/uvywth> (дата звернення: 21.10.2024);
4. Економіка та організація виробничої діяльності підприємства. Електронний посібник. URL: <http://surl.li/xricib> (дата звернення: 21.10.2024);
5. Мажулін Є. В. Дослідження шляхів підвищення ефективності діяльності підприємства. Наукова робота. URL: <http://surl.li/zaqzwd> (дата звернення: 21.10.2024);

Ключові слова: роздрібна торгівля, великі дані, конкурентоспроможність, аналіз споживчої поведінки, прогнозування продажів, персоналізація, управління запасами, оптимізація асортименту.

Keywords: retail trade, big data, competitiveness, consumer behavior analysis, sales forecasting, personalization, inventory management, assortment optimization.

Науковий керівник: к.т.н., доцент *Задерейко Олександр*

ШТУЧНИЙ ІНТЕЛЕКТ У ВИЯВЛЕННІ КІБЕРЗАГРОЗ ТА РЕАГУВАННІ НА НИХ

Струк Данило

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Штучний інтелект (ШІ) наразі стає важливим інструментом для виявлення та реагування на кіберзагрози. Через зростання складності та частоти кібератак, інструменти на основі ШІ є вкрай необхідними для посилення захисту кібербезпеки шляхом автоматизації процесів, розпізнавання закономірностей у великих масивах даних і швидкого реагування на загрози. ШІ здатен виправляти негаразди при виявленні кіберзагроз і реагуванні на них.

Однією з важливіших сфер застосування ШІ є системи виявлення вторгнень (Intrusion Detection Systems, IDS). Традиційні інструменти IDS покладаються на заздалегідь визначені інструкції та сигнатури, що обмежує їхню здатність виявляти нові, невідомі загрози. З іншого боку, IDS на основі ШІ використовують методи машинного та глибокого навчання, щоб вчитися на наборах даних і виявляти аномалії в режимі реального часу. Моделі ШІ в IDS аналізують мережевий трафік і виявляють шкідливі дії без потреби розшифровки, аналізуючи метадані зашифрованого трафіка, що дозволяє швидше і точніше виявляти загрози. Прикладом такого інструмента є IBM QRadar, який використовує ШІ для моніторингу мережевого трафіка та виявлення загроз на основі поведінкових аномалій [1].

Інструменти на основі ШІ надають змогу командам кібербезпеки передбачати потенційні атаки до того, як вони стануться, що суттєво покращує ефективність попереднього виявлення загроз. Постійний моніторинг та аналіз даних із різних джерел (мережевих журналів, каналів розвідки загроз та активності кінцевих точок) дозволяють алгоритмам ШІ виявляти закономірності та аномалії, які можуть бути сигналом про наближення кібератаки. Таке прогнозування зменшує рівень вразливості системи та посилює захист інфраструктури організації [2].

Корпорація Microsoft інтегрувала алгоритми ШІ у свої операції з безпеки за допомогою Microsoft Intelligent Security Graph, яка щодня обробляє понад 6,5 трильйонів сигналів від своїх продуктів і сервісів. Ця система використовує передову аналітику для виявлення аномалій, ідентифікації загроз і надання практичних рекомендацій командам безпеки. Завдяки впровадженню ШІ, кількість успішних кібератак на інфраструктуру Microsoft знизилася на 60%, а рівень виявлення шкідливого програмного забезпечення та фішингових атак зріс на 40% [3].

ШІ покращує не лише виявлення, а й реагування на кіберзагрози, автоматизуючи трудомісткі завдання, які раніше виконували люди. Системи, керувані ШІ, можуть автоматично ініціювати дії з реагування на інциденти, як от: ізоляція скомпрометованих систем, застосування патчів, блокування шкідливого трафіка. Така автоматизація скорочує час реагування, обмежуючи шкоду, спричинену інцидентами. Здатність ШІ працювати з високою швидкістю забезпечує нейтралізацію навіть складних кібератак можуть до того, як вони завдали шкоду. Провідна компанія в галузі екстремальних видів спорту та способу життя Boardriders зіткнулася зі значними проблемами в забезпеченні безпеки своїх глобальних операцій, оскільки команда фахівців із кібербезпеки, що її підтримувала, була замала для захисту великої інфраструктури компанії. Boardriders впровадили самонавчальний ШІ та автономне реагування Darktrace, щоб покращити видимість та захист у своїх мережових та хмарних середовищах. ШІ почав з вивчення звичайних «моделей життя» для кожного користувача і пристрою, що дозволило йому виявляти незначні відхилення, які вказують на потенційні загрози. За кілька тижнів Boardriders перевели Darktrace у повністю автономний режим, що дозволило ШІ системі самостійно вживати заходів для стримування постійних кібератак. Так у 2021 році Darktrace першим відреагував на спробу атаки на Boardriders з вимогою викупу [3].

ШІ трансформує розвідку загроз, просіюючи величезні обсяги даних для вилучення корисної інформації. Платформи розвідки загроз на основі ШІ можуть аналізувати інформацію з неструктурованих джерел, таких як новинні канали, соціальні мережі та форуми в даркнеті, щоб виявляти нові загрози і прогнозувати їх розвиток. Такий проактивний підхід до аналізу загроз дозволяє організаціям випереджати зловмисників, оскільки ШІ постійно оновлює своє розуміння ландшафту загроз [4, 5].

Однак ефективність ШІ у виявленні кіберзагроз і реагуванні на них не безмежна. Такі виклики, як ворожі атаки, коли зловмисники намагаються обдурити системи штучного інтелекту, подаючи їм маніпульовані дані, можуть підірвати надійність інструментів на основі ШІ. Крім того, якість даних залишається критично важливим фактором успіху систем ШІ. Неякісні або упереджені дані можуть призвести до неточних прогнозів і більшої кількості помилкових спрацьовувань або негативних результатів, що знижує довіру до рішень зі ШІ.

Попри це роль ШІ у виявленні кіберзагроз та реагуванні на них є важливою, оскільки він дозволяє підвищити швидкість, точність та ефективність операцій з кібербезпеки. Його здатність автоматизувати виявлення, прогнозування загроз і швидке реагування на інциденти гарантує, що організації

можуть краще захищати свою цифрову інфраструктуру в умовах дедалі складнішого кіберландшафту.

Використання алгоритмів ШІ та складних методів аналізу даних дозволяє системам безпеки автономно виявляти, аналізувати та реагувати на нові загрози в режимі реального часу. Крім того, алгоритми ШІ мають здатність адаптуватися та вчитися на нових шаблонах даних, постійно вдосконалюючи свої можливості виявлення і випередження кіберзагроз, перш ніж вони переростуть у повноцінні порушення.

Список використаних джерел:

1. AI and automation for cybersecurity. How leaders succeed by uniting technology and talent. IBM. URL: <https://www.ibm.com/ai-cybersecurity>
2. Artificial Intelligence in Cybersecurity. How AI can help mitigate false negatives and usher in a new era of razor-sharp cybersecurity solutions. LTIMindtree. URL: <https://www.ltimindtree.com/wp-content/uploads/2021/08/Artificial-Intelligence-in-Cybersecurity-PoV.pdf?pdf=download>
3. AI in Cybersecurity: Key Case Studies and Breakthroughs. URL: <https://eastgate-software.com/ai-in-cybersecurity-key-case-studies-and-breakthroughs/>
4. AI for Cybersecurity A Handbook of use cases. Peng Liu, Tao Liu, Nanqing Luo, Zitong Shang, Haizhou Wang, Zhilong Wang, Lan Zhang and Qingtian Zou. Penn State Cyber Security Lab. URL: <https://github.com/PSUCyberSecurityLab/PSUCyberSecurity-Lab.github.io>
5. AI Cybersecurity challenges. Threat Landscape For Artificial Intelligence. December 2020. ENISA. URL: <https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges>

Ключові слова: штучний інтелект, кібербезпека, системний аналіз, системи виявлення вторгнень, виявлення кіберзагроз.

Keywords: artificial intelligence, cybersecurity, system analysis, intrusion detection systems, cyber threat detection.

Науковий керівник: к.т.н., доцент Трофименко О.Г.

ЕФЕКТИВНІСТЬ ВИКОРИСТАННЯ TYPESCRIPT У ВЕЛИКИХ ПРОЄКТАХ

Шагалін Кіріл

студент 3 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

TypeScript стає все більш популярним у середовищі розробників, зокрема для створення великих та масштабованих проєктів. Як надбудова над JavaScript, TypeScript додає статичну типізацію, яка значно полегшує процес розробки, зменшує кількість помилок на ранніх етапах і покращує зчитуваність та підтримку коду. Розглянемо, як використання TypeScript впливає

на ефективність роботи з великими проєктами, та якими є переваги і недоліки його застосування.

Актуальність - з розвитком технологій проєкти стають дедалі складнішими. Без чіткого визначення типів та структур, робота з масштабними базами коду втрачає стабільність, і обслуговування проєктів стає складним завданням. У контексті великих команд розробників підтримка чистого коду є ключем до успіху проєкту, що і пояснює високу актуальність TypeScript. Інтеграція TypeScript допомагає стандартизувати підхід до типізації, що значно спрощує комунікацію між членами команди, підвищує безпеку коду та дозволяє легко підтримувати існуючий функціонал.

Проблематика

1. Масштабування коду: Чим більше коду в проєкті, тим важче підтримувати його чистоту та зрозумілість. Без типізації JavaScript-код часто містить логічні помилки, які важко виявити на етапі розробки.

2. Командна робота: Робота в команді вимагає ясності у визначенні об'єктів, функцій та методів. Відсутність чіткої типізації ускладнює комунікацію та створює ризик виникнення несумісних елементів коду.

3. Стабільність великих проєктів: Відсутність статичної типізації у великих проєктах може призводити до критичних помилок, які виникають під час виконання, що суттєво впливає на надійність та стабільність програми.

4. Складність у підтримці: Виявлення та виправлення помилок у великому JavaScript-коді часто потребує значних ресурсів і часу. Це може уповільнити процес розробки нових функцій і збільшити витрати на підтримку проєкту.

Переваги TypeScript у великих проєктах

1. Скорочення кількості помилок: Завдяки статичній типізації, TypeScript дозволяє виявляти помилки під час компіляції, що допомагає уникнути багатьох проблем на етапі виконання.

2. Покращена читабельність коду: Статична типізація робить код зрозумілішим для розробників, оскільки кожна змінна має чітко визначений тип. Це полегшує підтримку та розвиток проєкту.

3. Зручна робота в командах: TypeScript полегшує колективну роботу над проєктом. Кожен член команди може бачити очікувані типи аргументів функцій, що значно зменшує кількість комунікаційних помилок.

4. Інтеграція з IDE: TypeScript підтримує автодоповнення, навігацію по коду та рефакторинг, що сприяє швидкій розробці та підтримці програмного забезпечення.

5. Модульність: TypeScript дозволяє розробникам розділяти код на модулі, що робить його структуру більш організованою, що особливо важливо у великих проєктах.

Недоліки використання TypeScript

1. Збільшення часу на налаштування: Інтеграція TypeScript потребує додаткового налаштування та адаптації вже існуючого JavaScript-коду.

2. Збільшення обсягу коду: Додаткова типізація може зробити код дещо громіздким, особливо якщо проєкт містить багато складних об'єктів.

3. Вимоги до кваліфікації розробників: Робота з TypeScript вимагає певних знань і досвіду, що може стати викликом для розробників, які не мають відповідного досвіду.

Критерій	TypeScript	JavaScript
Типізація	Статична типізація допомагає виявляти помилки на етапі компіляції	Динамічна типізація, помилки типів виникають під час виконання
Інструменти розробника	Покращене автодоповнення, рефакторинг та навігація завдяки підтримці в IDE	Базове автодоповнення, обмежені можливості навігації та рефакторингу
Безпека коду	Більш захищений код завдяки типізації, менше критичних помилок у великих проєктах	Вищий ризик помилок типів, які можуть спричинити нестабільність на етапі виконання
Читабельність	Чіткі типи роблять код зрозумілішим для інших розробників	Код може бути менш зрозумілим без визначених типів, що ускладнює підтримку
Командна робота	Легше передавати інформацію між розробниками завдяки стандартизації типів	Вимагає більше документування та комунікації для розуміння структури даних
Сумісність з JavaScript	Можна використовувати існуючий JavaScript-код, поступово додаючи типи	Підтримується повна гнучкість написання коду, але без типізації
Підтримка модularity	Легше структуровано розподіляти код завдяки інтерфейсам та класам	Доступна підтримка модульності, але без статичної типізації це складніше для великих проєктів
Продуктивність розробки	Більша продуктивність на довгих проєктах, менше часу на пошук помилок типізації	Вища швидкість розробки на початкових етапах, але більше витрат на підтримку та тестування
Налаштування	Потребує налаштування компілятора, конфігурації tsconfig.json	Не потребує спеціальної компіляції, достатньо браузера або Node.js
Гнучкість	Менша гнучкість, оскільки потрібно визначати типи, що обмежує використання динаміки	Вища гнучкість, оскільки дозволяє змінювати типи динамічно

Статична типізація

TypeScript дозволяє вказувати типи для змінних, параметрів функцій та повернутих значень. Це дозволяє виявляти помилки ще на етапі компіляції, що значно знижує ризик помилок під час виконання.

`let age: number = 25; // age = "twenty-five";` // Помилка: 'string' не можна присвоїти 'number'

Інтерфейси та типи

TypeScript дозволяє визначати інтерфейси та складні типи, що робить код структурованим і більш зрозумілим.

Інтерфейси допомагають описувати форму об'єктів, що полегшує роботу в командах і дозволяє зменшити кількість помилок при передачі даних між функціями.

```
interface User {  
    name: string;  
    age: number;  
}  
const user: User = { name: "Alice", age: 30 };
```

Суворий режим типів

TypeScript має спеціальний режим `strict`, який включає кілька додаткових перевірок, наприклад, `strictNullChecks` (запобігає присвоєнню значення `null` типу, що його не підтримує) та `strictFunctionTypes` (перевіряє відповідність параметрів функцій).

Це робить код безпечнішим і допомагає уникати неочікуваних помилок.

Універсальні типи (Generics)

TypeScript підтримує універсальні типи, які дозволяють створювати багаторазові компоненти та функції, зберігаючи точність типізації. Універсальні типи забезпечують гнучкість коду і використовуються для створення адаптивних функцій або класів.

Розширені можливості роботи з класами

TypeScript додає підтримку абстрактних класів, модифікаторів доступу (`public`, `private`, `protected`) і членів класів, що допомагає контролювати доступ до методів та змінних.

Це особливо корисно для організації великих проєктів, дозволяючи розробникам створювати інкапсульовані компоненти.

Перевантаження функцій (Function Overloading)

TypeScript дозволяє оголошувати функції з різними сигнатурами для одного і того ж імені, що робить код більш гнучким і зручним для використання.

Модулі та простори імен

TypeScript підтримує організацію коду за допомогою модулів та просторів імен. Це спрощує керування залежностями в проєктах та робить код структурованим і легким для підтримки.

```
export class Car {  
    constructor(public make: string) {}  
}
```

Покращене автодоповнення та інтеграція з IDE

Завдяки статичній типізації, TypeScript пропонує покращене автодоповнення в редакторах коду, що робить розробку швидшою та знижує кількість помилок.

Це полегшує навігацію по великим проєктам і допомагає розробникам швидше орієнтуватися в чужому коді.

Компіляція в JavaScript

TypeScript компілюється в JavaScript, що дозволяє використовувати його можливості у будь-якому середовищі, де підтримується JavaScript (браузери, Node.js). Результат роботи — стандартний JavaScript-код, сумісний з усіма сучасними платформами.

Аналіз типів та рефакторинг

TypeScript аналізує типи, що дозволяє легко виконувати рефакторинг коду без побоювання змінити поведінку програми. Наприклад, перейменування змінних, методів, класів виконується безпечно завдяки знанню типів і взаємозв'язків.

Підтримка конструкцій нового стандарту JavaScript

TypeScript підтримує всі останні версії ECMAScript, включаючи такі можливості, як асинхронні функції (async/await), генератори, деструктуризація, тощо, що дозволяє використовувати новітні функції JavaScript в проєкті.

Висновок

TypeScript забезпечує суттєві переваги у масштабних проєктах, допомагаючи команді зменшити кількість помилок, спрощуючи підтримку та розвиток коду, та роблячи проєкт стабільнішим та легшим для розуміння. Хоча впровадження TypeScript може потребувати певних ресурсів на налаштування та навчання, його довгострокові переваги у великих проєктах є вагомими.

Список використаних джерел:

1. Сельська Н. П. Дослідження перспектив розробки SPA з використанням TypeScript на прикладі сайту для занять фітнесом з авторизацією користувачів : кваліфікаційна робота на здобуття освітнього ступеня бакалавр за спеціальністю „121 — інженерія програмного забезпечення“ / Наталія Петрівна Сельська . — Тернопіль: ТНТУ, 2023. — 63 с. - <https://elartu.tntu.edu.ua/handle/lib/42429>
2. БЕЗВЕРХИЙ, О., & КУЦЕНКО, О. (2022). ЕФЕКТИВНІСТЬ ЗАСТОСУВАННЯ БІБЛІОТЕКИ REACT. *Інформаційні технології та суспільство*, (2 (4), 13-19. <https://doi.org/10.32689/maup.it.2022.2.2>
3. Василенко Е.С. Вебзастосунок для системи управління проєктами з використанням фреймворку Angular. - Дипломна робота на здобуття ступеня бакалавра спеціальності «Комп'ютерні науки», «Інформаційні технології проектування». - Національний авіаційний університет. - Київ, 2024. — 55 с. - <https://dspace.nau.edu.ua/handle/NAU/65505>

Ключові слова: TypeScript, JavaScript, статична типізація, масштабовані проєкти, командна робота, підтримка коду, інтеграція з IDE, автодоповнення, модулі, універсальні типи (Generics), інтерфейси, рефакторинг, продуктивність, компіляція, ECMAScript.

Keywords: TypeScript, JavaScript, static typing, scalable projects, team collaboration, code maintenance, IDE integration, autocompletion, modules, generics, interfaces, refactoring, productivity, compilation, ECMAScript.

Науковий керівник: доцент Задерейко Олександр

ЕЛЕКТРОННІ СИСТЕМИ ВВЕДЕННЯ ЗАПИСІВ (ELD) РОБОЧОГО ДНЯ ВОДІЯ ВАНТАЖНОГО ТРАНСПОРТУ

Питомець Ярослав

аспірант 1-го курсу факультету факультету кібербезпеки та інформаційних технологій Національний університет "Одеська юридична академія"

Електронні системи ведення записів робочого дня водія, або ELD, використовуються водіями комерційного транспорту для автоматичного запису годин роботи (HOS) та часу водіння. Ці пристрої синхронізуються з двигуном автомобіля, фіксуючи необхідну інформацію, зокрема активність водіння, місцезнаходження, пройдені милі, стан запалювання та години роботи двигуна.

ELD найбільше поширені в США, і їхнє впровадження зумовлено кількома ключовими факторами:

Введення електронних систем ведення записів робочого дня водія (ELD) зумовлене кількома ключовими факторами. По-перше, існує нагальна потреба підвищити безпеку на дорогах через зростаючу кількість ДТП за участю водіїв вантажного транспорту, що часто викликані перевтомою. Це призводить до високого рівня травм і смертності, особливо через порушення норм робочого часу. По-друге, традиційні методи обліку, такі як паперові журнали, часто містять неточності та ускладнюють процес перевірок, а також можуть бути піддані маніпуляціям через людський фактор [1].

Технологічний прогрес також відіграє важливу роль у впровадженні ELD, адже з'явилися надійні електронні пристрої та програмне забезпечення для збору даних, а також нові мобільні технології, які дозволяють інтегрувати ці системи у транспортні процеси. Економічні чинники, такі як зменшення витрат на штрафи і покращення управління ресурсами, а також бажання компаній підвищити ефективність і знизити ризики, пов'язані з людським фактором, також стимулюють впровадження ELD. Таким чином, ці передумови створюють міцну основу для переходу на електронні системи ведення записів.

Призначення та особливості ELD. ELD забезпечують зручний спосіб відстеження та обміну даними про робочий статус водія в режимі реального часу. Це дозволяє диспетчерам і водіям мати доступ до інформації про кількість вільних годин та знижує ризик порушення вимог щодо годин роботи. Пристрій передає дані на сервер, де створюються та оновлюються журнали статусу чергування [2].

Основні функції ELD: Електронні системи ведення записів робочого дня водія (ELD) виконують кілька основних функцій, які сприяють ефективному управлінню робочим часом водіїв. Серед них: запис часу, розташування,

дати, пройдених автомобільних миль, годин роботи двигуна, а також ідентифікація водія і аутентифікація користувача. Крім того, ELD дозволяють здійснювати зміни статусу чергування, що забезпечує зручний контроль за робочими змінами.

Переваги ELD. Серед основних переваг використання ELD можна виділити спрощення документації: автоматизований запис даних зменшує потребу в паперових документах. Вбудовані пристрої відстеження забезпечують дані про місцезнаходження в реальному часі, що покращує управління маршрутами. Також ELD спрощують технічне обслуговування, оскільки підключення до порту OBD дозволяє швидко діагностувати проблеми з автомобілем. Система геозонування підвищує безпеку, дозволяючи відстежувати переміщення транспортного засобу, а точні звіти, що генеруються ELD, допомагають виявити можливості для зниження витрат [3].

Недоліки ELD. Однак, попри численні переваги, впровадження ELD має й певні недоліки. По-перше, витрати на обладнання та навчання персоналу можуть бути значними. По-друге, водії можуть відчувати занепокоєння щодо конфіденційності, оскільки їхня геолокація постійно моніториться. Крім того, постійний моніторинг може викликати стрес і дискомфорт у водіїв. Тому, хоча ELD надають багато переваг у забезпеченні безпеки та ефективності, їх реалізація вимагає врахування потенційних викликів.

Висновок

Впровадження ELD є важливим кроком у модернізації транспортної галузі США. Це призвело до підвищення безпеки, покращення ефективності та відповідності нормам. Проте реалізація ELD вимагає врахування потенційних викликів та витрат, що можуть виникнути під час переходу на нові технології.

Список використаних джерел:

1. Ask The Right Questions: ELDs Are Designed To Ensure Compliance With HOS, Not For Use As Life-Saving Devices URL: <https://cdlresources.org/uncategorized/ask-the-right-questions-elds-are-designed-to-ensure-compliance-with-hos-not-for-use-as-life-saving-devices/> (дата звернення 08.10.2024).
2. Noah M. :10 Must-Know Facts About ELD Compliance: Stay Ahead Of The Game 22.08.2023 URL: <https://cybermatters.info/compliance/what-is-eld-compliance/> (дата звернення 08.10.2024).
3. Gerlée K.: Electronic Logging Devices: The Future of Trucking Industry 21.07.2023 URL: <https://freeway.com/electronic-logging-devices-the-future-of-trucking-industry/> (дата звернення 08.10.2024).

Ключові слова: електронна система введення записів, години роботи, ведення записів, автоматизація, моніторинг

Keywords: electronic logic device, hours of service, record keeping, automation, monitoring

Науковий керівник: к.т.н., доцент **Задерейко Олександр**

TACKLING SHADOW IT AND RISK ANALYSIS IN PUBLIC CLOUD INFRASTRUCTURE

Марценюк Євгеній

*асистент кафедри Захисту інформації Національного університету
«Львівська Політехніка»*

Introduction

Shadow IT, defined as the use of information technology systems, solutions, and services without explicit organizational approval, has become an increasingly critical issue with the advent and widespread adoption of cloud computing. Recent studies have extensively examined the multifaceted risks and challenges associated with Shadow IT, particularly within public cloud environments.

For example, Edwards et al. (2019) [1] highlighted that Shadow IT introduces significant security vulnerabilities due to the lack of oversight and proper security measures. Their study illustrated how unauthorized cloud services could lead to severe data breaches and unauthorized access to sensitive information, posing substantial risks to organizational data integrity and security. Similarly, Akello (2021) [2] explored the volitional non-malicious insider threats associated with Shadow IT, especially in the context of work-from-home (WFH) arrangements during the COVID-19 pandemic. This research emphasized the heightened risk of data exposure and security breaches due to the uncontrolled use of cloud-based applications by employees working remotely.

The aim of this work is to explore the complex nature of Shadow IT within public cloud environments, focusing on the risks it poses, the impacts it incurs, and the strategies that can be employed for its effective management. By synthesizing recent literature and proposing comprehensive risk mitigation strategies, this study seeks to provide a robust framework for organizations to manage Shadow IT more effectively, ensuring data protection, security, and compliance in cloud computing.

Methodology

Understanding the scope and impact of shadow IT within an organization, particularly in the context of public cloud environments, is crucial for developing effective management strategies. The ease of access and widespread adoption of public cloud services have significantly increased the prevalence of shadow IT, as departments and individuals can readily procure cloud services without IT department approval. Both technology solutions and proactive engagement are essential in gaining insights into these unauthorized IT activities. [3] By focusing on public cloud environments, organizations can tailor their management strategies to address the unique challenges and risks associated with the unauthorized use of cloud services, ensuring a comprehensive approach to maintaining security, compliance, and operational efficiency. In addressing the risks associated with

shadow IT, especially within public cloud environments, it's crucial to identify and prioritize key risk areas. By focusing on these domains, organizations can develop a more effective strategy for mitigating the potential threats shadow IT poses. [4]

Scientific Contribution

1. Risk Profiling in Public Cloud Environments:

The study synthesizes recent findings to create a detailed framework for understanding the security vulnerabilities and operational risks caused by Shadow IT in public cloud settings. It highlights how unauthorized cloud services can compromise data integrity, security, and compliance.

2. Focus on Volitional Insider Threats:

It emphasizes the role of well-intentioned but unauthorized actions by employees, particularly during remote work situations such as those seen during the COVID-19 pandemic. This perspective provides a deeper understanding of how employee-driven Shadow IT increases security risks. [5]

3. Development of Mitigation Strategies:

The research proposes practical strategies for managing Shadow IT, combining technological solutions with proactive organizational practices. These strategies are specifically designed to address the unique challenges posed by public cloud environments.

4. Framework for Organizational Management:

The study presents a framework for assessing and mitigating Shadow IT risks. This framework helps organizations prioritize key risk areas while ensuring security, operational efficiency, and compliance in cloud computing. [6]

Results

This case study highlights a strategic approach to managing a multi-cloud infrastructure (AWS, Azure, GCP) from late 2020 to 2023, achieving significant milestones:

- **End of 2020:** Baseline set with 230 known accounts.
- **2021:**
 1. Initiated audits and monitoring for full visibility.
 2. Improved compliance to NIST 800-53 rev.4 standards.
 3. Discovered and managed 120 unknown accounts.
 4. Closed 30 obsolete accounts to reduce risks.
- **2022-2023:** Expanded to 447 accounts with enhanced security, compliance, and risk management capabilities.

End of 2023 Key Results:

1. Total resources managed: 35,493.
2. Vulnerability status: 0 critical/high; 954 medium; 1,870 low; 3,667 informal.
3. Compliance improvement: From 67% to 82%.

4. Enhanced security: Zero critical/high vulnerabilities achieved.

5. Governance: Proactive management of known and shadow accounts strengthened control and visibility.

This structured effort resulted in a robust, secure, and compliant cloud environment.

Conclusions

This case study highlights the value of a structured and proactive approach to managing cloud infrastructure. By implementing regular audits, continuous monitoring, and prioritizing compliance and security, the organization significantly enhanced its operational security while aligning cloud resources with its strategic objectives. The identification and removal of redundant or unnecessary accounts were key steps in improving cost efficiency and optimizing resource use. This process serves as a model for effective cloud governance, providing a benchmark for other enterprises seeking to secure and streamline their cloud environments.

References

- [1] Edwards, Kasper. (2004). Expected and Realized Costs and Benefits when Implementing Product Configuration Systems. Mass Customization for Personalized Communication Environments: Integrating Human Factors. 10.4018/978-1-60566-260-2.ch012.
- [2] Akello, P. (2021). Volitional Non-Malicious Insider Threats: At The Intersection of COVID-19, WFH and Cloud-Facilitated Shadow-Apps. 27th Annual Americas Conference on Information Systems, AMCIS 2021.
- [3] (2019). Shadow IT Management Concept for Public Sector. 65-73. 10.1007/978-3-030-37632-1_6.
- [4] Walterbusch, Marc & Fietz, Adrian & Teuteberg, Frank. (2017). Missing Cloud Security Awareness: Investigating Risk Exposure in Shadow IT. Journal of Enterprise Information Management. 30. 10.1108/JEIM-07-2015-0066.
- [5] Yaseen, Fenik. (2024). Chapter 2 2. Literature review 2.1. Information Security Policy availability and compliance literature.
- [6] Walterbusch, Marc & Fietz, Adrian & Teuteberg, Frank. (2017). Missing Cloud Security Awareness: Investigating Risk Exposure in Shadow IT. Journal of Enterprise Information Management. 30. 10.1108/JEIM-07-2015-0066.

Keywords Public clouds, AWS, Cyber security risks, compliance, automation, risk analysis, cloud infrastructure

Ключові слова: Публічна хмара, ризики кібербезпеки, відповідність, автоматизація, аналіз ризиків, хмарна інфраструктура

МЕТОДИ ОПТИМІЗАЦІЇ ПРОДУКТИВНОСТІ ДЕЦЕНТРАЛІЗОВАНИХ БАЗ ДАНИХ НА ОСНОВІ БЛОКЧЕЙН-ТЕХНОЛОГІЇ

Петрів Петро

аспірант Національного університету «Львівська політехніка»

Актуальність. Сучасний розвиток інформаційних технологій характеризується стрімким зростанням об'ємів даних та потребою в їх надійному та ефективному зберіганні. Блокчейн-технології, що спочатку розроблялися для криптовалют [1], знаходять все ширше застосування у різних сферах, зокрема в області децентралізованих баз даних [2]. Однак, існуючі реалізації стикаються з серйозними викликами щодо продуктивності та масштабованості.

Актуальність дослідження зумовлена зростаючою потребою у високопродуктивних децентралізованих системах зберігання даних. Традиційні методи оптимізації баз даних виявляються неефективними в контексті блокчейн-архітектури [3], що створює потребу в розробці спеціалізованих підходів до оптимізації. Особливої уваги потребують питання балансу між продуктивністю та збереженням ключових властивостей блокчейну – децентралізації та безпеки [4].

Метою дослідження є розробка комплексу методів оптимізації продуктивності децентралізованих баз даних на основі блокчейн-технології, що забезпечують підвищення швидкодії системи при збереженні її основних характеристик. Це включає оптимізацію механізмів консенсусу, вдосконалення структур даних та впровадження ефективних методів шардингу [5].

Основні положення. В рамках дослідження розроблено модифікований алгоритм досягнення консенсусу, який базується на удосконаленому механізмі Proof-of-Stake. Запропонований підхід включає оптимізований процес валідації транзакцій та систему попередньої перевірки, що дозволяє значно зменшити час підтвердження операцій. Експериментальні дослідження показують покращення швидкодії на 30-40% порівняно з традиційними реалізаціями [2].

Важливим компонентом розробленої методології є впровадження методу smart-sharding, який забезпечує оптимальний розподіл даних між вузлами мережі. На відміну від існуючих підходів [3], запропонований метод враховує не лише обсяг даних, але й паттерни доступу до них, що дозволяє мінімізувати кількість крос-шардових транзакцій та забезпечити більш ефективну синхронізацію між вузлами.

Для підвищення ефективності операцій читання розроблено систему багаторівневої індексації, спеціально адаптовану під особливості блокчейн-структур. Система використовує модифіковані Merkle Patricia Tries та спеціалізовані індекси для найбільш частих паттернів запитів [4], що дозволяє

суттєво прискорити пошук та зчитування даних при збереженні криптографічної верифікованості структури даних.

Науковий внесок. Наукова новизна дослідження полягає в комплексному підході до вирішення проблеми оптимізації продуктивності децентралізованих баз даних на основі блокчейн-технології. Вперше запропоновано інтегрований метод оптимізації, який поєднує модифіковані алгоритми консенсусу з адаптивним шардингом та спеціалізованою системою індексації [1]. На відміну від існуючих рішень [3], розроблений підхід забезпечує не лише підвищення продуктивності, але й зберігає основні властивості блокчейн-систем: децентралізацію, безпеку та незмінність даних.

Розроблено та теоретично обґрунтовано новий метод динамічної оптимізації розподілу даних, який, на відміну від існуючих підходів [2], враховує як структурні особливості блокчейну, так і специфіку запитів до бази даних. Це дозволило досягти більш ефективного використання ресурсів системи та підвищити її загальну продуктивність.

Висновки. Проведене дослідження демонструє ефективність запропонованих методів оптимізації продуктивності децентралізованих баз даних на основі блокчейн-технології. Експериментальні результати підтверджують можливість значного підвищення швидкодії системи при збереженні її основних характеристик [5]. Зокрема, досягнуто зменшення часу відгуку на 30-40%, підвищення пропускну здатності системи на 25% та оптимізацію використання ресурсів зберігання. Практична цінність отриманих результатів полягає в можливості їх безпосереднього застосування для оптимізації існуючих блокчейн-систем та розробки нових децентралізованих додатків. Подальші дослідження можуть бути спрямовані на розробку адаптивних механізмів оптимізації та вдосконалення методів масштабування системи.

Список літератури

- [1] Wang, W., Hoang, D. T., Xiong, Z. (2022). A survey on consensus mechanisms and mining management in blockchain networks. *IEEE Access*, 7, 22328-22370.
- [2] Gorenflo, C., Lee, S., Golab, L. (2020). FastFabric: Scaling hyperledger fabric to 20,000 transactions per second. *International Journal of Network Management*, 30(5), e2099.
- [3] Yang, R., Yu, F. R., Si, P. (2019). Integrated blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Communications Surveys & Tutorials*, 21(2), 1508-1532.
- [4] Park, J., & Park, J. (2021). Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry*, 13(1), 164.
- [5] Hassan, M. U., Rehmani, M. H. (2020). Differential privacy techniques for cyber physical systems: A survey. *IEEE Communications Surveys & Tutorials*, 22(1), 746-789.

Keywords: blockchain, decentralized databases, performance optimization, scalability, distributed systems.

Ключові слова: блокчейн, децентралізовані бази даних, оптимізація продуктивності, масштабованість, розподілені системи.

Секція 3. УПРАВЛІНСЬКІ, СОЦІАЛЬНІ ТА ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ

ОПТИМІЗАЦІЯ ПІДХОДІВ ДО ЦІНОУТВОРЕННЯ НА ПОСЛУГИ КІБЕРБЕЗПЕКИ

Горбаченко Станіслав

*завідуючий кафедри кібербезпеки Національного університету «Одеська
юридична академія», д.е.н. професор*

Разінкін Нікіта

*асистент кафедри кібербезпеки Національного університету «Одеська юри-
дична академія»*

В останні роки підприємства стикаються зі зростанням кількості та якості кібератак і, відповідно, намагаються відреагувати на це збільшенням витрат на захист інформаційної інфраструктури. При цьому від підбору адекватної цінової стратегії залежить не лише конкурентоспроможність безпосередньо постачальників послуг кібербезпеки, а й здатність їхніх клієнтів ефективно захищати власні активи. А отже формування цін на послуги передбачає врахування не лише собівартості і ринкових цін, але й таких чинників, як ризики, специфічні потреби клієнта та потенційні фінансові втрати від кібератак [1].

На сучасному ринку існують різноманітні моделі підходи до ціноутворення на послуги кібербезпеки, деякі з них є класичними для усіх ІТ-послуг, а деякі - спрямовано саме на безпековий сегмент ІТ-ринку. Серед найбільш поширених – фіксована плата, ціноутворення на основі ризику, модель «плата за використання» та інтелектуальні системи ціноутворення, що використовують штучний інтелект.

Модель фіксованої ціни можна вважати традиційною для сфери кібербезпеки. Зазвичай, вона передбачає встановлення чіткої ціни на пакет послуг, який охоплює визначений обсяг робіт. Наприклад, McAfee, один з лідерів в сегменті антивірусних програм, пропонує підписки на свої продукти кібербезпеки для малого та середнього бізнесу за фіксованою ціною. Такі пакети можуть включати стандартний набір послуг, наприклад, захист від вірусів, фішингових атак та шкідливого програмного забезпечення. Це дозволяє клієнтам прогнозувати витрати та обирати певний рівень захисту без необхідності сплачувати за додаткові послуги, що можуть бути їм непотрібними. Модель є зручною для невеликих підприємств, яким потрібно забезпечити базовий рівень захисту за фіксовану плату [2].

Проте, вказана модель має й певні обмеження. Великі організації, що стикаються з більш складними загрозами, можуть потребувати гнучкого підходу, що враховує високий рівень ризику. В цьому випадку модель фіксованої ціни не завжди здатна охопити всі потреби клієнта, оскільки зростаючий обсяг робіт з кібербезпеки призводить до зниження рентабельності для компанії-постачальника послуг.

Модель «плата за використання» дозволяє клієнтам сплачувати тільки за ті послуги, які їм дійсно потрібні, в обсязі, який вони використовують. Таку модель застосовує, зокрема, AWS (Amazon Web Services) у своєму рішенні AWS Security Hub. AWS Security Hub – це централізована платформа, що збирає та аналізує інформацію про безпеку з усіх сервісів, які використовує клієнт. Тут клієнти можуть платити за кожен використаний сервіс, наприклад, моніторинг даних, аналітику ризиків або інші послуги, що допомагають ідентифікувати загрози. Зазначена модель є комерційно вигідною для підприємств, яким потрібен мінімальний набір послуг і які прагнуть контролювати свої витрати. Водночас, модель «плата за використання» може мати суттєві недоліки, адже витрати клієнта різко зростатимуть у випадку інтенсивного використання ресурсів у періоди підвищених кіберзагроз [3].

Ціноутворення на основі ризику є інноваційним підходом, який враховує рівень ризиків, з якими стикається кожен окремий клієнт. Цей підхід підходить для підприємств, що працюють в галузях з високим рівнем кіберзагроз, наприклад, у фінансовому, медичному, телекомунікаційному секторах. Як приклад, CrowdStrike, один з провідних постачальників рішень з кібербезпеки, використовує підхід, що враховує обсяг та специфіку даних, які захищає клієнт, а також рівень ризику, пов'язаний з галуззю, в якій він працює. Такий підхід дозволяє врахувати не лише тип захисту, а й реальні ризики, які можуть бути унікальними для конкретного підприємства чи організації і передбачає формування індивідуальних цінових пропозицій.

Інноваційні підходи до ціноутворення включають використання штучного інтелекту (ШІ) та машинного навчання, що дозволяє аналізувати дані у реальному часі та прогнозувати ризики. Підприємство Darktrace розробила інструменти на основі ШІ, які здатні автоматично виявляти аномальні дії в мережах клієнтів та попереджати про можливі загрози. Модель ціноутворення в таких компаніях враховує як обсяг даних, які аналізуються, так і складність алгоритмів ШІ, що використовуються для аналізу. ШІ допомагає оптимізувати ціноутворення, враховуючи різні фактори, зокрема, дані про попередні атаки, поведінкові моделі користувачів та загальну активність у мережі.

Інтеграція ШІ дозволяє компаніям формувати прогнозовану вартість послуг на основі ймовірності майбутніх атак. У разі значного зростання ризику кібератак, що можуть виявити алгоритми ШІ, клієнту може бути запропо-

новано підвищений рівень захисту за додаткову плату. Такий підхід також дозволяє забезпечити високу адаптивність до ринку і водночас обґрунтованість ціноутворення.

З огляду на зростання кібератак у світі та підвищені регуляторні вимоги, ціноутворення на послуги кібербезпеки стає все складним завданням. Законодавчі ініціативи, такі як Загальний регламент захисту даних (GDPR) у Європейському Союзі, що зобов'язує посилювати заходи безпеки для захисту особистих даних, спонукають суб'єктів підприємництва до збільшення витрат на кібербезпеку. У результаті моделі та підходи до ціноутворення повинні враховувати ще й глобальні виклики, такі як відповідність вимогам різних країн та адаптація до нових загроз, що виникають внаслідок посилення глобальної цифровізації.

Оптимізація ціноутворення на послуги кібербезпеки передбачає також активне використання технологій ШІ, що дозволяють не тільки прогнозувати загрози, а й краще зрозуміти унікальні потреби кожного конкретного клієнта та здійснювати коригування ціни у відповідності з їх змінами. Це допоможе постачальникам послуг та їхнім клієнтам знаходити оптимальні рішення для захисту даних, забезпечуючи високий рівень захисту за обґрунтовану ціну.

Список використаних джерел:

1. Конопленко А., Ковальов Б., Боруха А. Аналіз моделей ціноутворення та регіональних особливостей на ринку іт аутсорсингу. *Економіка та суспільство*. 2024. № 63. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/4166>
2. Вдовіна О. О. Кібербезпека України: до постановки питання. *Інформація, комунікація та управління знаннями в глобалізованому світі*: зб. матеріалів IV між-нар. наук. конф., м. Київ, 20–22 травня 2021 р. / упоряд. М. М. Цілина. Київ: Видавництво Ліра-К, 2021. С. 187–189.
3. Шостак Л., Федонюк А., Помазун О. Кібербезпека в системі формування бізнес-моделі підприємства в умовах цифрової економіки. *Економіка та суспільство*, 2024. № 64. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/4240>

Ключові слова: ціноутворення, кібербезпека, моделі, ризики, штучний інтелект.

Keywords: pricing, cybersecurity, models, risks, artificial intelligence.

УПРАВЛІНСЬКІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ

В'юник Ольга

*професор кафедри економіки, менеджменту та комерційної діяльності
Центральноукраїнського національного технічного університету,
кандидат економічних наук, професор*

Сучасний етап розвитку економіки і суспільства характеризується посиленням використання цифрових технологій та інструментів в діяльності підприємницьких структур, що суттєво трансформує умови їх господарювання. Розвиток новітніх цифрових технологій створив широкі додаткові можливості для бізнесу, але поряд з тим, спричинив підвищення впливу низки загроз у сфері кібербезпеки. Забезпечення кібербезпеки на сьогодні виступає одним із нагальних завдань для підприємств, установ, організацій, держави загалом. Отже, будь-яка система менеджменту має бути орієнтованою на ідентифікацію, оцінювання, мінімізацію та ефективне керування ризиками, що лежать в площині інформаційної безпеки, генерувати раціональні управлінські рішення, спрямовані на захист власних інформаційних ресурсів та забезпечення кібербезпеки.

Кібербезпека, у загальному розумінні, може бути охарактеризована як «захист підключених до Інтернету систем, таких як обладнання, програмне забезпечення та дані від кіберзагроз» [3].

Розрізняють такі складові елементи інформаційної безпеки бізнес-структур: технічний, програмний, інформаційний, кадровий, організаційний [2].

Значного поширення набули такі види кібератак, як фішинг (спонукання користувача завантажити певну шкідливу програму на власний пристрій), витік даних (отримання сторонніми особами доступу до конфіденційної інформації). Низка проблем у сфері кібербезпеки, з якими найчастіше стикаються господарюючі суб'єкти, пов'язані із незахищеністю мережі, серверів і пристроїв, інформації та наявних баз даних, каналів передання інформації, сайтів фірм, програм і додатків, відсутністю якісного захисту від вірусів [1]. Кібератаки можуть мати вкрай негативні наслідки для діяльності суб'єкта господарювання, включаючи погіршення його іміджу та репутації, зниження конкурентних позицій на ринку, отримання суттєвих фінансових збитків або ж недоодержання прибутку.

Прикладами новітніх підходів до забезпечення кібербезпеки в умовах глобального цифрового простору можуть слугувати: «розвідка загроз, машинне навчання, поведінкова аналітика, архітектура нульової довіри, управління ризиками» [3]; систематичне оновлення засобів захисту, ідентифікація

нетипової активності в мережі шляхом постійного моніторингу, створення резервних копій даних, чітке дотримання протоколів інформаційної безпеки, проведення тестувань та аналіз рівня захищеності [5]; покращення організаційних аспектів управління кібербезпекою, формування та розвиток цифрової культури персоналу компанії [1]; проведення оцінювання вразливостей інформаційної системи, за рахунок чого отримується своєчасна інформація щодо наявних ризиків та формуються шляхи щодо їх усунення [4].

Загальний алгоритм дій в процесі забезпечення інформаційної безпеки суб'єкта господарювання містить сукупність взаємопов'язаних етапів:

- 1) визначення ключових загроз;
- 2) ідентифікація ризиків та специфіки керування ними;
- 3) формування власної моделі управління інформаційними ризиками;
- 4) розробка комплексу заходів, націлених на протидію ризикам і загрозам;
- 5) формування організаційних регламентів, що поширюються на захист інформаційних ресурсів компанії;
- 6) забезпечення своєчасного контролю та оцінка ефективності [2].

Розробляючи систему заходів щодо забезпечення кібербезпеки на рівні підприємства, установи, організації, варто брати до уваги, що результативність цієї системи залежить не лише від дій технічних фахівців, але й від усвідомлення адміністративно-управлінським персоналом важливості даної ланки діяльності та впровадження ними виважених управлінських рішень на стратегічному і тактичному рівнях.

Отже, до найважливіших управлінських аспектів забезпечення кібербезпеки в умовах цифровізації вважаємо за доцільне віднести, по-перше, врахування питань захисту інформації і додержання правил кібербезпеки під час розроблення чи оновлення загальної стратегії функціонування та розвитку суб'єкта господарювання. По-друге, сучасні умови провадження господарської діяльності вимагають від бізнес-структур бути гнучкими та адаптивними, впроваджувати системи раннього попередження та реагування, оскільки чим раніше певний ризик чи загроза у сфері кібербезпеки будуть виявлені, тим більшими є шанси на їх успішне усунення або мінімізацію негативних наслідків. По-третє, важливим є проведення аналітичних, оціночних і моніторингових процедур на систематичній основі, із використанням альтернативних джерел інформації. По-четверте, належний рівень кібербезпеки потребує відповідного фінансового, технічного і програмного забезпечення, а також сприяння підтриманню загальної цифрової культури і цифрової грамотності усіх працівників, які мають доступ і працюють з інформацією, на належному рівні та ін.

Список використаних джерел:

1. Бондар-Підгурська О.В., Хоменко І.І. Науково-методичні засади оцінки ефективності процесу управління інформаційною безпекою підприємств малого та середнього бізнесу: кібербезпека та інтелектуальна власність. *Проблеми економіки*. 2022. №2. С. 108-116.
2. Василюшин С. Удосконалення важелів управління діджиталізаційними ризиками економічної безпеки та формування кібербезпеки облікової системи. *Вісник економіки*. 2021. Вип. 1. С. 97-110.
3. Вовк А. Сучасні проблеми публічного управління забезпеченням кібербезпеки в Україні. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. Вип. 8. С. 28-35.
4. Галузін І.С. Управління вразливостями і оцінювання вразливостей як засоби забезпечення кібербезпеки. *Сучасний захист інформації*. 2020. №3. С. 29-33.
5. Галушко О.І., Селівьорстова Т.В. Кібербезпека в управлінні ланцюгами постачань (SCM). *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. №2. С. 537-542.

Ключові слова: кібербезпека, інформаційна безпека, управління, ризик, загроза.

Keywords: cyber security, information security, management, risk, threat.

АНАЛІЗ НАСТРОЇВ ЯК ОДИН ІЗ АСПЕКТІВ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ

Синенко Марина

доцент Національного університету «Чернігівська політехніка»,

к.ф.-м.н., доцент

Зотєєв Станіслав

аспірант Національного університету «Чернігівська політехніка»

Роль соціальних мереж у сучасному світі є досить вагомою. Насьогодні соціальні мережі стали ключовим джерелом інформації та платформою для обміну думками, ідеями, а також настроями та емоціями між користувачами. Їхній стрімкий розвиток зумовлює необхідність ефективного аналізу контенту для виявлення трендів, дослідження настроїв у суспільстві, боротьби з дезінформацією та прийняття обґрунтованих рішень. Таким чином, аналіз контенту соціальних мереж є ключовим інструментом у сучасних дослідженнях комунікацій.

Згідно з [1] інтелектуальний аналіз даних (ІАД) – науковий і технологічний напрямок, пов'язаний з обробкою інформації та виявленням в ній закономірностей і тенденцій, які можуть застосовуватися при підтримці прийняття рішень. Технологія ІАД є міждисциплінарною областю дослідження, яка

синтезує методи ряду дисциплін, зокрема, таких як теорія інформації, системи штучного інтелекту, теорія ймовірностей, математична статистика, машинне навчання, тощо.

На нашу думку, аналізуючи контент у соціальних мережах варто висвітлити наступні питання:

- Класифікація контенту у соціальних мережах;
- Аналіз настроїв у соціальних мережах (Sentiment Analysis);
- Виявлення трендів і популярного контенту;
- Боротьба з дезінформацією і фейками

Аналіз настроїв (Sentiment Analysis також відомий як Opining Mining) – це процес автоматизованого визначення емоційного забарвлення тексту. Мета цього аналізу – визначити чи є текст позитивним, негативним або нейтральним. У деяких випадках також варто враховувати специфічні емоції такі як радість, страх, гнів чи здивування. Аналіз настроїв як метод ґрунтується на обробці природної мови (Natural Language Processing, NLP), статистичних алгоритмах та машинному навчанні. При реалізації методу виділяють наступні кроки.

- Збір даних. Дані варто збирати з різних джерел: соціальних мереж, оглядів товарів і послуг, коментарів користувачів, новинних статей, тощо.

- Попередня обробка тексту. Текст очищується від зайвих елементів, таких як стоп-слова (часто уживані, але несуттєві слова, наприклад, «і», «але», «або», тощо), емодзі, спеціальні символи. Цей етап також може включати нормалізацію тексту, тобто лематизацію або стемінг. Слід зазначити, що стемінг, на відміну від лематизації, як правило, легше реалізувати. Однак стемінг зменшує точність.

- Токенізація та векторизація. Текст розбивається на окремі слова або фрази (токени). Далі, щоб можна було аналізувати текст за допомогою певних алгоритмів, він представляється у числовій формі. Серед використовуваних для аналізу методів слід зазначити Bag of Words, TF-IDF або векторизацію за допомогою Word Embeddings.

- Аналіз тексту. При аналізі тексту можна застосовувати лексичний підхід, тобто використання словників емоційних слів, які оцінюються на основі їх емоційного значення, машинне навчання (алгоритми такі як Support Vector Machines, Random Forest або нейронні мережі), гібридний підхід, який поєднує лексичний аналіз з методами машинного навчання.

- Класифікація та інтерпретація. Модель класифікує текст за категоріями (позитивний, негативний, нейтральний), або за шкалою, наприклад, -1, 0, 1.

Аналіз настроїв має широкий спектр застосування у бізнесі та маркетингу, у політиці та суспільних дослідженнях, електронній комерції, медицині

та психології. Так, наприклад, у бізнесі компанії можуть аналізувати відгуки клієнтів на платформах з метою покращення якості своїх товарів чи послуг. Аналіз настроїв також допомагає адаптувати рекламні кампанії залежно від реакції аудиторії. У політиці на основі аналізу громадської думки можна досліджувати ставлення суспільства до політичних ініціатив, законів чи кандидатів під час виборів, прогнозувати результати виборів – аналіз настроїв у соціальних мережах, як правило, корелює з реальними результатами голосування. Так, наприклад, відомо, що у США аналіз настроїв у Twitter широко використовувався для прогнозування електоральних настроїв, аналізу популярності кандидатів і тем, що хвилюють виборців. Метод аналізу настроїв дозволяє проводити моніторинг психічного стану – аналіз настроїв постів у соціальних мережах може допомогти визначити емоційний стан користувачів. Наприклад, Facebook використовує аналіз настроїв у поєднанні з алгоритмами класифікації для виявлення та видалення контенту з мовою ненависті. Аналіз коментарів дозволяє зрозуміти вплив медичних або наукових публікацій на аудиторію.

Разом з тим аналіз настроїв як метод має ряд викликів та обмежень.

- Складність інтерпретації тексту. Сарказм, іронія та багатозначність мови ускладнюють точний аналіз. Наприклад, вислів «Це просто чудово, усе знову зламалось.» може бути іронічним, але модель сприйматиме його як позитивний.

- Мовна та культурна специфіка. Слова, які є позитивними в одній культурі, можуть не бути такими у іншій.

- Динамічність мови. Постійна поява нових сленгових виразів, хештегів або мемів може знижувати точність моделі.

Висновок. Аналіз настроїв – це потужний інструмент, який дозволяє розуміти емоції думки та настрої людей на базі текстових даних. Його застосування охоплює безліч сфер. Попри виклики пов'язані зі складністю текстових даних, розвиток NLP та машинного навчання удосконалювати ефективність цього підходу.

Список використаних джерел

1. Ланде Д.В., Субач І.Ю., Бояринова Ю.Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник. — К.: ІСЗІ КПІ ім. Ігоря Сікорського», 2018. — 300 с.
2. Чирун Л.Б., Кучковський В.В., Висоцька В.А. Особливості методів контент-аналізу у межах регіону// Національний університет "Львівська політехніка"- 2015. С. 296-320.
3. Sai Zhao Research on Social Network Analysis Method in Cooperative Innovation Performance//Advances in Economics, Business and Management Research, volume 146.- 2019. P.79-84.

4. Ланде Д.В. Елементи комп'ютерної лінгвістики в правовій інформатиці. – К.: НДІП НАПрН України, 2014. – 168 с.
5. Кифяк О.В., Урда В.Д. Маркетинг у соціальних медіа (SMM) як інструмент просування товарів та послуг. Міжнародний науковий журнал «Інтернаука». 2017. No 14 (36). С. 123-130.
6. Герасимчук Т.А. Управління маркетингом підприємств торгівлі в соціальних мережах. Реклама: інтеграція теорії та практик: тези доповідей XI міжнародної наук.-практ. конф. Київ, 2017. С. 22 -24.

Ключові слова: соціальні мережі, аналіз контенту, аналіз настроїв, обробка природної мови, машинне навчання.

Keywords: social networks, content analysis, sentiment analysis, natural language processing, machine learning.

ОФІСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ ВІЗУАЛІЗАЦІЇ МАРКЕТИНГОВИХ ДАНИХ

Лобода Юлія

*доцент кафедри інформаційних технологій Національного університету
«Одеська юридична академія», кандидат педагогічних наук, доцент*

Сучасний ринок вимагає від бізнесу швидкого та обґрунтованого прийняття рішень, що базуються на точних даних про клієнтів, продажі та ефективність маркетингових кампаній. Проте обробка великих обсягів даних стає значною складністю, адже розуміння та інтерпретація сирих даних обмежені та часто неінтуїтивні. У цьому контексті візуалізація даних стає важливим інструментом, який дозволяє зробити дані доступнішими та кориснішими для аналізу, спрощуючи процес прийняття рішень [1].

Використання спеціалізованих аналітичних платформ, таких як Tableau чи Power BI, не завжди є доступним для малих і середніх компаній через їхню вартість, складність та ресурсомісткість. Виникає потреба у використанні офісних інформаційних технологій для візуалізації маркетингових даних, які дозволяють побудувати зрозумілі та інтерактивні звіти в умовах обмежених ресурсів.

Маркетингові дані охоплюють широкий спектр інформації, зокрема дані про поведінку споживачів, аналітику продажів, статистику взаємодії в соціальних мережах, показники ефективності кампаній (KPI) тощо [2].

Візуалізація даних є критично важливою для маркетологів, оскільки вона дозволяє спрощено представити складну інформацію, сприяє легшому розумінню тенденцій та аномалій, а також пришвидшує процес прийняття рішень.

Робота з великими обсягами даних має свої складнощі:

- великий обсяг даних може утруднювати розуміння основних трендів;
- без належної візуалізації дані можуть залишитися малозрозумілими для осіб, які не мають спеціальної підготовки в аналізі;
- складність інтеграції даних із різних джерел, як-от CRM-систем, інтернет-магазинів та інших ресурсів, що часто призводить до фрагментації інформації [3].

Офісні інформаційні технології є зручними та доступними інструментами, які можуть допомогти у вирішенні проблем візуалізації маркетингових даних, особливо для малого та середнього бізнесу. Розглянемо найбільш популярні з них:

1. Microsoft Excel – інструмент для обробки даних та створення графіків і діаграм. Зведені таблиці та функція Power Query дозволяють об'єднувати дані з різних джерел, що є важливим для створення узагальнених звітів.

2. Google Sheets – інструмент для обробки даних у хмарному середовищі, який забезпечує доступ до даних із будь-якого пристрою та дозволяє спільну роботу над проектами. Google Sheets має інструменти інтеграції з Google Analytics та іншими джерелами, що дозволяє автоматизувати завантаження маркетингових даних для подальшої візуалізації.

3. Google Data Studio – безкоштовний сервіс від Google для створення інтерактивних дашбордів та звітів. Data Studio інтегрується з багатьма популярними маркетинговими платформами, що дає можливість створювати актуальні та динамічні звіти.

4. Хмарні CRM-системи – офісні технології також дозволяють автоматично отримувати дані з CRM-систем для подальшої візуалізації, що дозволяє швидко аналізувати клієнтські взаємодії та визначати тенденції.

Переваги використання офісних технологій для візуалізації:

- доступність, більшість офісних технологій доступні для широкого загалу, а Google Sheets та Google Data Studio – безкоштовні.
- інтеграція з іншими сервісами, здатність інтегрувати дані з CRM, Google Analytics та інших джерел підвищує ефективність аналізу [4].
- простота використання, офісні інструменти мають інтуїтивно зрозумілі інтерфейси, тому їх можна використовувати навіть без спеціальної підготовки.

Виклики використання офісних технологій для візуалізації даних:

- обмеження масштабованості, офісні технології не завжди здатні ефективно обробляти великі обсяги даних, як це роблять спеціалізовані аналітичні платформи.

– обмежені можливості для налаштування, більшість офісних інструментів має базові функції для візуалізації, але не може забезпечити ті ж функціональні можливості, що спеціалізовані програми.

Офісні інформаційні технології є корисними та доступними інструментами для візуалізації маркетингових даних, особливо для малого та середнього бізнесу. Використання таких інструментів, як Microsoft Excel, Google Sheets та Google Data Studio, дозволяє ефективно інтегрувати та аналізувати дані, зберігаючи ресурси та час. Незважаючи на обмеження в обробці великих обсягів даних та налаштування візуалізацій, ці інструменти можуть слугувати ефективним рішенням для візуалізації даних, необхідної для прийняття рішень у маркетингу.

Список використаних джерел:

1. Jeanne Moore. Data Visualization in Support of Executive Decision Making. *Interdisciplinary Journal of Information, Knowledge, and Management*. Volume 12, 2017, pp. 125-138. <https://doi.org/10.28945/3687>
2. Durmuş Şenyapar, H. N. The Future of Marketing: The Transformative Power of Artificial Intelligence. *International Journal of Management and Administration*, 8(15), 2024, p. 1-19. <https://doi.org/10.29064/ijma.1412272>
3. Google. (n.d.). *Google Data Studio*: Product Overview. Available at: <https://datastudio.google.com/>.
4. Payne, A., & Frow, P. (2013). *Strategic Customer Management: Integrating Relationship Marketing and CRM*. Cambridge University Press. 2013. <https://doi.org/10.1017/CBO9781139057417>

Ключові слова: офісні інформаційні технології, маркетингові дані, візуалізація.

Keywords: office information technologies, marketing data, visualization.

СУЧАСНІ ВИКЛИКИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ІТ-КОМПАНІЯХ

Немченко Тетяна

*доцент кафедри економіки, менеджменту та комерційної діяльності
Центральноукраїнського національного технічного університету, кандидат
економічних наук, доцент*

Рудь Ростислав

*студент гр. МІТ-24 ОПП «Менеджмент ІТ у глобальному бізнес-середовищі»
Центральноукраїнського національного технічного університету*

На сьогодні ІТ-індустрія виступає одним із ключових джерел конкурентоспроможності економіки України. Зокрема, в 2023 році саме ІТ-галузь зайняла друге місце за обсягом експорту (питома вага становить 42%), а загаль-

ний приріст суми сплачених податків виріс у порівнянні із 2022 р. на 11,5% [1]. Власне, в умовах воєнного стану саме дана сфера, попри невизначеність зовнішнього середовища, демонструє стійкість та тенденцію до зростання, забезпечуючи економічну стабільність України. В цей же час зростає ризик нарощення її привабливості для кіберзлочинців.

В умовах повномасштабного військового вторгнення на територію України, питання кібербезпеки набуло особливого значення, оскільки кіберпростір став повноцінним полем бою, де постійно відбуваються спроби де-стабілізувати роботу українських організацій та установ. Маємо зауважити, що актуальність питань забезпечення кібербезпеки нарощується внаслідок зростання популярності дистанційної роботи, що зумовлює додаткові ризики вразливості корпоративних мереж. Значно зросла кількість атак, спрямованих на викрадення конфіденційних даних та інтелектуальної власності українських компаній. Окрім цього, особливістю діяльності ІТ-компанії є співпраця з іноземними клієнтами, тож, маючи доступ до комерційної таємниці міжнародних організацій зростає і відповідальність щодо забезпечення належного рівня кібербезпеки та необхідність відповідати міжнародним стандартам захисту інформації.

Сучасні реалії вимагають від компаній безперервного вдосконалення систем захисту з огляду на зростання кількості та складності кібератак, використання новітніх технологій для зламу систем безпеки. Зокрема, як свідчать дані, опубліковані у Статистичному звіті за результатами роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році Державним центром кіберзахисту у 2023 році зафіксовано на 62,5% кіберінцидентів більше, ніж за результатами 2022 року [2]. Особливо помітним стало збільшення випадків фішингу та DDoS-атак. Цілями стають не лише великі корпорації, але й середній та малий бізнес, успішні кібератаки на який призводять не лише до фінансових збитків компаній, але й сприяють погіршенню репутації, зменшенню клієнтів та втраті ринкових позицій. У окремих випадках наслідки можуть бути катастрофічними, особливо для малого та середнього бізнесу, що не має достатньо ресурсів для подальшого відновлення у разі масштабної атаки.

Все вище сказане обумовлює актуальність удосконалення системи забезпечення кібербезпеки в українських ІТ-компаніях, що виступає стратегічною перспективою їх розвитку та визначальним елементом їх конкурентоспроможності на національному та глобальному ринку.

Загалом, як визначає українське законодавство кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середо-

вища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [3].

Серед ключових видів загроз для кібербезпеки вчені виокремлюють malware (шкідливе ПЗ), фішинг, програми-вимагачі, DDoS-атаки, insider threats, хмарні експлойти, атаки ботнетів, тощо [4].

На переконання М. Сироватченка позитивна динаміка розвитку інформаційних технологій, забезпечуючи розвиток економіки, формує сприятливі умови для зростання кібератак. Основними проблемами кібербезпеки автор називає збільшення кількості вакансій, що важко заповнити наявними працівниками в ІТ-сфері. В той же час формування стратегій захисту стимулює розвиток аналітики, штучного інтелекту та автоматизованих систем реагування на кіберзагрози [5].

Українські ІТ-компанії стикаються з низкою специфічних проблем у сфері забезпечення кібербезпеки, серед яких варто виділити наступні:

- обмежений бюджет на кібербезпеку, що досить гостро постає для малих та середніх підприємств, оскільки на сьогодні, в умовах кризи та невизначеності багато організацій вимушені скорочувати витрати, нерідко і в сфері кіберзахисту. Молоді компанії, які тільки починають свою діяльність часто не можуть дозволити собі придбання передових технологічних рішень для захисту від кіберзагроз, що робить їх більш вразливими до атак;

- дефіцит кваліфікованих фахівців з кібербезпеки, що наразі виступає критичною проблемою для українського ІТ-сектору. На сьогодні спостерігається відтік спеціалістів через мобілізацію, від'їзд за кордон (особливо жінок). Окрім цього, зважаючи на можливості дистанційної зайнятості, ІТ-фахівці часто обирають роботу в іноземних компаніях з вищим рівнем оплати. Маємо зауважити, що швидкі зміни видового різноманіття кіберзагроз вимагає постійного навчання та підвищення кваліфікації існуючих спеціалістів, що також потребує значних ресурсів;

- загострення безпекових факторів вимагає формування не лише потужної системи технологічних рішень в сфері кіберзагроз, а й забезпечення фізичної безпеки, що пов'язане часто їх потребою переміщення обладнання та персоналу, що в свою чергу формує додаткові ризики з огляду на необхідність забезпечення безпечних каналів зв'язку, захисту обладнання під час транспортування.

Тож, формування системи кіберзахисту, враховуючи розгалужену мережу видів атак вимагає комплексного підходу, що ставить перед компаніями вимогу щодо постійного вдосконалення технічних засобів захисту, застосування низки превентивних заходів (проведенню аудиту, тестування), проведення регулярних тренінгів для персоналу, культивування корпоративної культури кібербезпеки, тощо. Важливим в даному ключі виступає налагод-

ження співпраці з державними органами та міжнародними партнерами щодо обміну інформацією, що дасть змогу отримати інформацію щодо нових загроз та визначити актуальні методи протидії. Застосування означеного комплексу захисту дасть створити ефективну систему захисту, здатну успішно протистояти сучасним кіберзагрозам в ІТ-сфері.

Список використаних джерел:

1. Цифровий тигр: сила українського ІТ—2023. *ITUkraine*. URL: <https://itukraine.org.ua/en/digital-tiger-the-power-of-ukrainian-it-2023/> (дата звернення: 08.11.2024 р.)
2. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році. *Державний центр кіберзахисту*. URL: <https://scpc.gov.ua/uk/articles/334> (дата звернення: 08.11.2024 р.)
3. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 р зі змінами та доповненнями. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 08.11.2024 р.)
4. What is cybersecurity? *IBM*. URL: <https://www.ibm.com/topics/cybersecurity> (дата звернення: 08.11.2024 р.)
2. Сироватченко М. (2024) Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник Національного університету «Львівська політехніка»*. Серія: "Юридичні науки". Том 11, № 1(41), С. 314-320.

Ключові слова: кіберзахист, ІТ-сектор, кібератаки

Keywords: cyber defense, IT sector, cyber attacks

АКТУАЛЬНІ ІНСТРУМЕНТИ ДЛЯ ІННОВАЦІЙНОГО РОЗВИТКУ

Пунченко Наталія

доцент кафедри інформаційних технологій Одеського державного аграрного університету, кандидат технічних наук, доцент

Сьогодні актуальними інструментами для інноваційного розвитку багатьох галузей та соціальної сфери є методи та засоби управління великими обсягами інформації. Їх оптимізація в процесі цифровізації різних видів діяльності дозволяє суттєво покращити аналітичні процеси прийняття рішень. Тому одним з ключових пріоритетів цифрової трансформації в кожній галузі стає впровадження систем штучного інтелекту.

Штучний інтелект представляє собою здатність машин виконувати когнітивні функції, аналогічні людським, такі як сприйняття, навчання, міркування та вирішення задач. Еталоном для штучного інтелекту є рівень людського мислення в контексті міркувань, мови та сприйняття.

На сьогоднішній день штучний інтелект застосовується практично в усіх секторах, надаючи технологічну перевагу компаніям, які активно інтегрують його в свої процеси. За даними McKinsey, штучний інтелект має потенціал створення вартості в 600 мільярдів доларів у роздрібній торгівлі та здатний збільшити прибуток банківського сектора на 50% порівняно з традиційними методами аналітики. У транспортній та логістичній сферах очікується зростання доходів на 89% [1].

Наприклад, використання штучного інтелекту в маркетингових командах дозволяє автоматизувати рутинні завдання, надаючи працівникам можливість зосередитися на побудові стосунків з клієнтами та залученні нових потенційних клієнтів[2]. Компанія Gong, наприклад, аналізує розмови торгових представників, записуючи, розшифровуючи та аналізуючи їх. Віце-президент може використовувати рекомендації ІІ для розробки ефективних стратегій.

Таким чином, штучний інтелект пропонує сучасні технології для роботи зі складними даними, які важко обробити людині. Автоматизація повторюваних завдань дозволяє працівникам зосередитися на більш важливих аспектах роботи, які додають цінність. Масштабне впровадження штучного інтелекту сприяє зниженню витрат і збільшенню доходів.

Системи штучного інтелекту також забезпечують контроль і коригування прийнятих рішень шляхом аналізу результатів їх реалізації та прогнозування майбутніх змін на основі аналізу даних.

Розробка та впровадження систем підтримки прийняття рішень із використанням штучного інтелекту вимагає нових навичок як від спеціалістів, що працюють з цими технологіями, так і від осіб, які приймають рішення. До функцій таких систем належать:

- Підтримка осіб, які приймають рішення, у генерації рекомендацій.
- Моделювання прогнозних трендів і оцінка альтернативних рішень.

Процес створення систем штучного інтелекту включає адаптацію методів семіотики та аналізу великих даних, концептуальні моделі знань та експертні моделі. Класичний підхід до розробки включає:

1. Формулювання технічних вимог.
2. Аналіз предметної області.
3. Концептуалізація області у вигляді базисних множин і логічних відносин.
4. Розробка програмного забезпечення.
5. Тестування та експлуатація систем.

Системи підтримки прийняття рішень інтегрують бази даних та інтелектуальні модулі. До їх функціональних елементів належать:

- Модуль навчання — пошук інформації та адаптація системи.

- Модуль отримання та зберігання інформації — наповнюється експертами для подальшого аналізу.
- Користувацькі інтерфейси, що залежать від ролей користувачів.
- Зовнішні інтерфейси для взаємодії з іншими програмами.
- Модуль прогнозування — моделює різні сценарії на основі рішень.
- Модуль аналізу — надає дані для прийняття рішень.
- Модуль рішень — пропонує оптимальні моделі рішень.
- Модуль консультування — пояснює рішення та їх обґрунтування.
- Колекція моделей — надає альтернативні механізми прийняття рішень.

Актуальні завдання розробки систем штучного інтелекту в організаціях включають створення нового програмного та апаратного забезпечення для ефективного моделювання процесів і вироблення рішень. Як засоби розробки можуть використовуватися мови програмування та спеціальні програмні продукти з готовими шаблонами для створення систем штучного інтелекту.

Крім того, важливим аспектом є забезпечення кібербезпеки систем судноводіння. Захист даних та запобігання кібератакам стають критично важливими в умовах зростаючої залежності від цифрових технологій[3].

Урахування методичних особливостей розробки та впровадження технологій підвищить ефективність аналітичної роботи і процесів прийняття рішень, а також покращить лояльність співробітників до змін у рамках цифрової трансформації. Як підкреслює Сидоренко, "системи підтримки прийняття рішень можуть суттєво полегшити навантаження на управлінський апарат і підвищити якість рішень"[4].

Список використаних джерел:

1. Бондаренко, О. "Штучний інтелект: концепції, технології та перспективи". Київ, 2020.
2. Лисенко, А. "Цифрова трансформація бізнесу: виклики та можливості". Львів, 2021.
3. Петренко, І. "Кібербезпека в умовах цифровізації". Харків, 2019.
4. Сидоренко, В. "Системи підтримки прийняття рішень на основі штучного інтелекту". Одеса, 2022.

Ключові слова: штучний інтелект, системи підтримки прийняття рішень, модуль.

Keywords: artificial intelligence, decision support systems, module.

МЕТОДИ АНАЛІЗУ ТА ЗАХИСТУ ВІД КІБЕРАТАК. МЕТОДИ АНАЛІЗУ ПОВЕДІНКИ КІБЕРЗЛОЧИНЦЯ

Бойко Віктор

*доцент кафедри кібербезпеки Національного університету
«Одеська юридична академія», кандидат технічних наук*

Ніякий Олександр

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Розвиток технологій призвів до того, що злочинці стали використовувати дедалі складніші та витонченіші методи злому, обходячи традиційні системи безпеки. Кібератаки не тільки можуть призвести до витоку конфіденційних даних, а й завдати серйозної шкоди інфраструктурі.

Традиційні методи захисту, такі як фаєрволи та системи виявлення вторгнень (IDS), відіграють важливу роль у забезпеченні безпеки, але часто вони виявляються недостатніми. Нові, раніше невідомі загрози й атаки можуть залишатися непоміченими, що створює небезпечні вразливості. У таких випадках, для захисту від кібератак треба розуміти як вони реалізуються, проаналізувати дії кіберзлочинців.

Часто використовувані методи захисту від кібератак:

Брандмауер — це мережеве програмне забезпечення, яке захищає внутрішню мережу від ненадійних зовнішніх джерел, таких як Інтернет. Його основна функція полягає у контролі та фільтрації вхідного й вихідного трафіку, відповідно до заздалегідь налаштованих правил безпеки. Брандмауери грають ключову роль у запобіганні несанкціонованому доступу, захищають від шкідливих атак і потенційних загроз. Крім того, вони допомагають блокувати або обмежувати доступ до певних мережевих портів, що дозволяє мінімізувати ризик використання цих портів для атак або проникнення в систему [1].

Система виявлення вторгнень (IDS) — це мережевий інструмент безпеки, який призначений для моніторингу трафіку та активності пристроїв з метою виявлення відомих шкідливих дій, підозрілої поведінки або порушень правил безпеки. IDS виявляє потенційні загрози та попереджає адміністраторів про інциденти, але не має можливості самостійно блокувати або запобігати атакам. Для більшої ефективності IDS часто працюють у поєднанні з системами запобігання вторгненням (IPS) [3], які можуть не тільки виявляти загрози, але й активно блокувати шкідливі дії в режимі реального часу [2].

Класичний захист Firewall / IDS / IPS – у реальній реалізації захисту, використовуються об'єднання активних методів захисту, це дає можливість за-

безпечити багаторівневу оборону, підвищуючи ефективність виявлення та блокування загроз на різних етапах атаки.

До цього ми розглядали активні методи аналізу та захисту. Метод honeypot значно відрізняється від інших. Це пасивний метод концепція якого полягає в тому, щоб створити спокусливу ціль, яка виглядає як законний і цінний ресурс, спонукаючи потенційних зловмисників взаємодіяти з нею, як залучення бджіл медом. Однак приманка не містить справжньої інформації, і вона ізольована від ваших фактичних виробничих систем, щоб гарантувати, що будь-яка діяльність ретельно відстежується та не становить реальної загрози для ваших критичних активів [4].

Метою кіберприманки є залучення зловмисників для збору даних про їхні методи, тактики та прийоми. Спостерігаючи за їхньою поведінкою в контрольованому середовищі та аналізуючи отриману інформацію, можна краще зрозуміти способи дій атакуючих і використовувати ці знання для посилення захисту від реальних загроз. Такий підхід фахівці з кібербезпеки називають розвідкою загроз.

Існує багато видів приманок, але найчастіше їх поділяють на приманки з низьким та високим рівнем взаємодії:

Приманка з низьким рівнем взаємодії — це та, яка, будучи виявленою зловмисником, не дає йому можливості отримати цінні дані або проникнути глибше в систему. У деяких випадках хакеру пропонується форма входу, пройти яку він не може. Honeypot фіксує та зберігає всі спроби злому, включаючи введені ім'я користувача, паролі та IP-адресу зловмисника, яка іноді може допомогти визначити його місцезнаходження.

Приманка з високим рівнем взаємодії — дозволяє зловмиснику зайти далі, щоб зібрати більше даних про його наміри та методи. Вона заохочує зловмисника до спроб входу за допомогою заздалегідь визначених імен користувачів і паролів, а також реєструє всі команди та дії, які атакуючий намагається виконати. Приманки з високим рівнем взаємодії є більш потужними інструментами для збору детальної інформації, але й вимагають більших ресурсів для підтримки та аналізу.

Honeypots виступають пастками для кіберзловмисників, збираючи інформацію про їхні методи, інструменти та мотиви. Основні кроки для їх ефективного використання включають [5]:

1. Розгортання: Honeypots створюються так, щоб виглядати привабливими для атак. Вони можуть бути автономними системами або віртуальними машинами, що імітують реальні служби й програми.

2. Імітація вразливостей: Приманки налаштовані з навмисними слабкостями, такими як застаріле ПЗ або слабкі паролі, щоб здаватися легкою мішенню.

3. Ізоляція: Honeypots ізольовані від ключових систем, щоб запобігти реальній шкоді. Вони розташовуються в окремих сегментах мережі.

4. Моніторинг і ведення журналів: Приманки уважно стежать за всіма діями зловмисника, реєструючи спроби входу, команди та інший трафік для аналізу.

5. Сповіщення та відповіді: При виявленні несанкціонованого доступу, honeypot сповіщає адміністраторів для аналізу та реакції.

6. Обман і затримка: Honeypots можуть навмисно затримувати дії зловмисників, щоб надати більше часу для збору даних і аналізу.

7. Збір і аналіз даних: Дані з honeypots допомагають зрозуміти тактики атакуючих і вдосконалювати заходи безпеки.

Використання Honeypot є стратегічним кроком, який дозволяє не лише запобігати атакам, але й краще розуміти природу загроз у кіберпросторі. Завдяки цьому інструменту організації отримують можливість не просто реагувати на інциденти, а прогнозувати та попереджати їх на основі реальних даних про дії та поведінку кіберзлочинців.

Список використаних джерел

1. What is Firewall?. Cisco. [Електронний ресурс]. URL: <http://surl.li/fuaias>
2. IBM. What is an Intrusion Detection System (IDS)? | IBM. *IBM - United States*. URL: <https://www.ibm.com/topics/intrusion-detection-system>
3. What is an Intrusion Prevention System (IPS)? | Fortinet. *Fortinet*. URL: <https://www.fortinet.com/resources/cyberglossary/what-is-an-ips>
4. GeeksforGeeks. What is Honeypot? - GeeksforGeeks. *GeeksforGeeks*. URL: <https://www.geeksforgeeks.org/what-is-honeypot/>
5. Honeypots Explained | How Does a Honeypot Work?. *SOPHOS*. URL: <https://www.sophos.com/en-us/cybersecurity-explained/honeypots>

Ключові слова: аналіз кібератак, пасивний аналіз, honeypot

Keywords: cyberattack analysis, passive analysis, honeypot

Науковий керівник: *Бойко Віктор Дмитрович*

КІБЕРЗАХИСТ ЯК ІНСТРУМЕНТ СУЧАСНОГО РИЗИК-МЕНЕДЖМЕНТУ

Кірович Андрій

*аспірант кафедри кібербезпеки Національного університету
«Одеська юридична академія»*

Сучасна управлінська наука ідентифікує ризик як вірогідну подію, в результаті настання якої можуть відбутися позитивні, нейтральні або негативні

наслідки. В останні роки як бізнес-структури, так і державні установи дедалі частіше стикаються з ризиками, які спричиняють швидкий розвиток цифрових технологій, глобальної взаємодії та зростання залежності від інформаційних систем.

Кіберризики стають найбільш вагомими у структурі загроз для бізнесу (особливо для тих суб'єктів підприємництва, які працюють в мережі Інтернет), а їхні масштаби та рівень потенційних втрат постійно збільшуються. При цьому кібератаки здатні призвести не тільки до прямих фінансових втрат, але й до серйозного порушення бізнес-процесів, компрометації конфіденційної інформації, пошкодження репутації та навіть повного зупинення діяльності суб'єкта підприємництва. Тому цифрові трансформації вимагають інтеграції інструментів, пов'язаних із кіберзахистом в загальну систему ризик-менеджменту, що дозволяє зменшити ймовірність реалізації кіберзагроз і мінімізувати наслідки можливих інцидентів.

Актуальні кіберзагрози включають хакерські атаки, зловмисне програмне забезпечення (таке як віруси, трояни та програми-шантажисти), фішингові атаки, крадіжку даних, атаки соціальної інженерії, а також поширення неправдивої інформації для дезорієнтації користувачів. Всі ці загрози мають суттєві відмінності в механізмах реалізації, але їх спільна мета полягає у порушенні цілісності, конфіденційності або доступності інформаційних ресурсів. Відтак ефективний ризик-менеджмент має включати систему ідентифікації та вимірювання кіберзагроз, систему моніторингу та контролю і, на решті систему управління кіберзахистом.

В процесі застосування ризик-менеджменту суб'єкти підприємництва намагаються вирішити такі завдання як профілактика виникнення ризиків; мінімізація шкоди, заподіяної ризиками; максимізація додаткового прибутку, одержуваного в результаті управління ризиками.

В контексті профілактики виникнення ризиків основна мета кіберзахисту полягає в створенні та підтримці безпечного інформаційного середовища, що забезпечує захист інформаційних активів організації на всіх рівнях. Комплексний підхід до кіберзахисту включає низку методів і заходів, спрямованих на запобігання можливим кіберінцидентам, швидке реагування на них та ефективне відновлення функціональності інформаційних систем. У рамках ризик-менеджменту кіберзахист не лише запобігає зловмисним діям, але й допомагає мінімізувати наслідки атак і запобігати повторенню інцидентів.

Важливим аспектом ефективного кіберзахисту є розробка й впровадження чітко визначених політик безпеки, які регулюють доступ до інформаційних систем, правила використання мережевих ресурсів та обробки даних. Такі політики мають бути адаптовані до специфіки діяльності організації та враховувати всі можливі кіберзагрози, пов'язані з її операційним середови-

щем. Вони охоплюють широкий спектр питань: від контролю доступу до мережі та шифрування даних до інструкцій з реагування на інциденти та процедур відновлення. Наявність цих політик дозволяє систематизувати процеси захисту, знижує ймовірність виникнення помилок і дозволяє співробітникам діяти в умовах загрози швидко та ефективно.

Звдля мінімізація шкоди, заподіяної ризиками кіберзахист має бути багаторівневим, що дозволяє застосовувати різноманітні інструменти та технології для захисту інформаційних активів на різних етапах їх обробки та передачі. До таких інструментів належать шифрування даних, яке забезпечує їх конфіденційність; багатофакторна аутентифікація, яка ускладнює несанкціонований доступ до систем; регулярне оновлення програмного забезпечення для усунення вразливостей, а також використання технологій моніторингу й аналізу мережевої активності для виявлення потенційних загроз. Моніторинг дозволяє виявляти аномальні дії, що можуть свідчити про намагання проникнути до системи або порушити її роботу.

В контексті максимізації додаткового прибутку, одержуваного в результаті управління ризиками ключовим є використання технологій штучного інтелекту та машинного навчання, які значно розширюють можливості виявлення та реагування на кіберзагрози. Завдяки цим технологіям суб'єкти підприємництва можуть автоматизувати процеси аналізу великих обсягів даних, що дозволяє швидко та точно ідентифікувати потенційні загрози. Системи на базі штучного інтелекту здатні виявляти поведінкові аномалії в мережевій активності, аналізувати патерни, які можуть свідчити про нетипову активність, і навіть передбачати потенційні загрози до їх реалізації. Це дає змогу не лише швидко реагувати на інциденти, але й проактивно запобігати можливим атакам.

Кіберзахист також охоплює комплекс заходів для управління інцидентами, які дозволяють забезпечити швидке та ефективне реагування на виявлені загрози, а також відновлення нормальної роботи інформаційних систем. Управління інцидентами передбачає наявність чітко регламентованих процедур, які визначають дії співробітників під час кіберінциденту, а також розробку планів відновлення, що мінімізують наслідки кібератак. Чіткий план дій у випадку кіберінциденту допомагає знизити фінансові втрати, уникнути втрати довіри з боку клієнтів і партнерів, а також забезпечує захист репутації. Окрім цього, розробка таких планів підвищує готовність суб'єкта підприємництва до нових атак і покращує координацію дій між різними відділами.

Ефективний кіберзахист також передбачає навчання персоналу, адже більшість кіберзагроз виникають через людський фактор. Навчальні програми з кібербезпеки дозволяють підвищити обізнаність співробітників щодо актуальних кіберзагроз, навчити їх розпізнавати ознаки фішингу, соціальної ін-

женерії та інших методів зловмисників. Освічений персонал здатний самостійно ідентифікувати ризики на ранніх стадіях і вживати відповідних заходів для їхньої нейтралізації. Це підвищує загальний рівень безпеки та мінімізує можливість людської помилки, яка може стати причиною серйозного кіберінциденту.

Таким чином побудова та запровадження ризик-менеджменту допомагає суб'єктам підприємництва у визначенні стратегії, досягненні цілей та прийнятті обґрунтованих рішень, а також в цілому сприяє вдосконаленню системи управління. Мінливість кіберсередовища обумовлює важливість інтеграції кібербезпеки у загальну стратегію ризик-менеджменту. Тобто, управління кіберризиками повинно бути частиною стратегічного планування, а також процесів оцінки та аналізу ризиків. Для цього використовуються, зокрема, аналіз ризиків (дозволяє оцінити рівень загрози) та матриці впливу (визначають ймовірність реалізації конкретного ризику і його потенційний вплив на діяльність суб'єкта підприємництва). Інтеграція кіберзахисту у стратегічне управління дозволяє забезпечити максимальний рівень безпеки, оптимізувати витрати на захист інформаційних ресурсів і спрямувати зусилля на мінімізацію найбільш критичних ризиків.

Список використаних джерел:

1. Вірченко В. В. Сучасний інструментарій ризик-менеджменту інноваційно-підприємницької діяльності в умовах формування віртуальної економіки. Ефективна економіка, 2021. №9. URL: <http://surl.li/holsqx> (дата звернення: 10.10.2024).
2. Климчук М. М., Ачкасов І. А., Климчук С. А. Вплив ризик-менеджменту на формування стратегії управління бізнес-процесами підприємства в умовах цифрової економіки: міжнародний досвід. *Бізнес Інформ*, 2021. № 1, С. 272-278.
3. Рамський А., Арабаджи К. Кіберстрахування в банківському секторі: ідентифікація ризиків та інструменти підтримки безпеки. Науковий вісник Міжнародної асоціації науковців. Серія: економіка, управління, безпека, технології, 2023. № 2 (2). URL: <https://man.org.ua/nv/index.php/about/article/view/49> (дата звернення: 10.10.2024).

Ключові слова: кіберзахист, ризик-менеджмент, кіберзагрози, інформаційна безпека.

Keywords: cyber defense, risk management, cyber threats, information security.

ВПЛИВ КІБЕРЗАГРОЗ НА ЕФЕКТИВНІСТЬ ЛОГІСТИЧНОЇ ДІЯЛЬНОСТІ

Фомичев Дмитро

*аспірант кафедри економічної кібернетики та інформаційних технологій
Одеського національного економічного університету*

Як сфера підприємництва логістична діяльність охоплює процеси планування, організації, управління та контролю за переміщенням товарів, послуг, інформації і ресурсів від постачальника до кінцевого споживача. Вона виступає як комплексний процес і включає етапи закупівлі, складування, транспортування, обробки замовлень, управління запасами та обслуговування клієнтів. Відповідно, мета зазначеного процесу полягає у забезпеченні ефективного та економічного руху продукції для своєчасного задоволення потреб споживачів, з оптимізацією витрат і зменшенням ризиків, пов'язаних з поставками.

З огляду на поставлену мету ефективна логістична діяльність потребує найвищого рівня безпеки. А з розвитком цифрових технологій питання безпеки все частіше переходять у площину кіберсередовища, адже саме кіберзагрози є тим критичним фактором, що впливає на стабільність усіх бізнес-процесів в логістиці.

Посилена цифровізація, розвиток Інтернету речей (IoT), автоматизованих систем управління ланцюгами поставок, а також зростання обсягів інформації, яка обробляється в межах логістичних операцій - все це призводить до того, що логістичні компанії стикаються з новими викликами саме у сфері забезпечення кібербезпеки. При цьому наслідки кіберзагроз охоплюють різні аспекти логістичної діяльності – від операційної ефективності й економічних втрат до репутаційних ризиків та можливих порушень законодавства [1].

У таблиці 1 представлено основні кіберзагрози, що генерують найбільшу небезпеку для стабільної роботи логістичних компаній. Одним із найпоширеніших типів кіберзагроз для логістичних компаній є атаки на мережеві та операційні системи, які можуть призвести до повної паралізації діяльності компанії. У випадку, коли внаслідок атаки виходять з ладу ключові операційні системи, логістичні процеси повністю припиняються, що негативно впливає на своєчасність доставки товарів, спричиняє затримки, втрату прибутку та зниження рівня довіри клієнтів до компанії. Погіршення операційної ефективності через кіберінциденти може мати довгострокові наслідки, включаючи фінансові санкції за порушення договірних зобов'язань.

Таблиця 1
Основні види кіберзагроз

№	Вид	Опис
1	Атаки на мережу	Несанкціонований доступ до логістичних систем, порушення з'єднань між учасниками ланцюгів поставок, перехоплення даних
2	Віруси та шкідливе програмне забезпечення	Зараження серверів і пристроїв для збору, зберігання та обробки логістичної інформації
3	Фішинг	Метод соціальної інженерії, спрямований на обман співробітників для отримання конфіденційної інформації
4	Атаки на Інтернет речей (IoT)	Втручання у роботу пристроїв, таких як складські роботи, сенсори для відстеження вантажів, транспортні засоби
5	DDoS-атаки (розподілені атаки на відмову в обслуговуванні)	Створення навантаження на сервери, що порушує функціонування операційних систем компанії
6	Витік даних	Викрадення чи розголошення інформації про замовлення, маршрути, клієнтів та партнерів
7	Злом облікових записів	Отримання несанкціонованого доступу до облікових записів співробітників, що може призвести до маніпуляції логістичними процесами
8	Фальсифікація даних	Маніпуляція даними щодо місця перебування вантажу, часу доставки або стану товарів

З урахуванням важливості даних у логістичних процесах, викрадення, фальсифікація чи несанкціоноване використання інформації також може суттєво знизити ефективність діяльності компанії. Мова йде, зокрема, щодо даних про замовлення, маршрути, графіки та статус вантажів, які є необхідними для координації та оперативного реагування в межах ланцюгів поста-

чання. Якщо такі дані будуть скомпрометовані, логістичні компанії можуть втратити точність планування, що призведе до зростання витрат на виконання замовлень, порушення графіків та погіршення якості обслуговування. Інформаційні витоки, викликані кіберзагрозами, також здатні знизити конкурентоспроможність компанії, оскільки її комерційні секрети можуть стати доступними конкурентам, надаючи їм суттєву перевагу на ринку [2].

Інший значущий аспект впливу кіберзагроз на логістичну сферу пов'язаний із ризиками, що виникають із впровадженням Інтернету речей (IoT) та автоматизації бізнес-процесів (наприклад, за допомогою CRM систем). Майже усі логістичні компанії, які хочуть отримати конкурентні переваги, активно використовують інтелектуальні пристрої та автоматизовані системи. Водночас кожен із таких пристроїв може стати потенційною точкою входу для кіберзловмисників, оскільки забезпечує віддалений доступ до систем управління логістичними процесами. Несанкціонований доступ до IoT-пристроїв здатен не лише порушити роботу конкретного компонента логістичної мережі, але й призвести до ланцюгових збоїв, які можуть паралізувати весь ланцюг поставок. Це стосується, зокрема, вантажних автомобілів, роботизованих складських комплексів і безпілотних літальних апаратів, які виконують критично важливі завдання у логістичних ланцюгах. Збої у функціонуванні таких пристроїв унаслідок кібератак призводять до суттєвих витрат на відновлення, зупинок операцій та необхідності посилення кібербезпеки шляхом перегляду стандартів і політик захисту даних.

Також, кіберзагрози впливають на здатність логістичних компаній дотримуватися нормативно-правових вимог у сфері захисту даних. У багатьох країнах встановлені суворі правила щодо зберігання та обробки персональних даних клієнтів. Логістичні компанії працюють із великим обсягом конфіденційної інформації, що включає адреси доставки, контактні дані й фінансову інформацію клієнтів. У разі кіберзлому з можливим витоком цих даних компанії зазнають не лише фінансових збитків, а й можуть зіткнутися з адміністративними штрафами та судовими позовами, що значно зменшує їхній прибуток і завдає шкоди репутації. Отже, забезпечення відповідності кібербезпеці стає необхідним елементом стратегії зниження ризиків для логістичних компаній, які прагнуть уникнути як фінансових втрат, так і потенційних репутаційних збитків [3].

Таким чином кіберзагрози впливають не тільки на поточну діяльність окремих логістичних компаній, але й порушують стабільність глобальних ланцюгів постачання. Адже, враховуючи високий рівень інтегрованості та взаємозалежності логістичних процесів на глобальному рівні, кібератака на одну компанію може спричинити ланцюгову реакцію, яка вплине на діяльність численних партнерів і контрагентів. У зв'язку з цим логістичні компанії та їхні

об'єднання активно співпрацюють з метою створення колективних заходів кібербезпеки та налагодження систем обміну інформацією щодо загроз, щоб знизити вразливість логістичних ланцюгів перед потенційними кіберінцидентами.

Список використаних джерел:

1. Кривов'язюк І., Сидорчук І. Підвищення ефективності цифрових трансформацій в сфері управління логістикою промислових підприємств. Хельсінки, Фінляндія. *SCIENTIA*, 2022. С. 26–29.
2. Горбаченко С. Кібербезпека як складова економічної безпеки України.. Галицький економічний вісник. Тернопіль : ТНТУ, 2020. Том 66. № 5. С. 180–186.
3. Бойко В., Василенко. Н. Кібербезпека розумних міст: Соціальні аспекти, ризики деанонізації та доксингу. Комунальне господарство міст, 2020. Том 6. №. 159. С. 186-195.

Ключові слова: кіберзагрози, безпека, логістика, автоматизація.

Keywords: cyber threats, security, logistics, automation.

ІННОВАЦІЙНІ ПІДХОДИ ДО КОНТРОЛЮ ДОСТУПУ ДО ІНФОРМАЦІЇ ДЛЯ ПЕРСОНАЛУ З ВИКОРИСТАННЯМ БЛОКЧЕЙН-ТЕХНОЛОГІЙ

Ямнич Андрій

*аспірант кафедри безпеки інформаційних технологій
Національного університету «Львівська політехніка»*

У дослідженні пропонується інноваційний підхід до контролю доступу персоналу до інформаційних ресурсів підприємства шляхом інтеграції ролеорієнтованої моделі (RBAC) з блокчейн-технологією. Метою роботи є забезпечення безпечного, прозорого та надійного механізму управління доступом, який відповідає динамічним потребам сучасних виробничих середовищ. Методи дослідження включають розробку смарт-контрактів для управління ролями та правами доступу персоналу, а також аналіз ефективності запропонованого підходу у вигляді моделювання на основі блокчейн-платформи. Результати показують, що використання блокчейну запобігає несанкціонованому доступу та підвищує прозорість записів доступу завдяки незмінності даних. Застосування цього підходу забезпечує гнучкість і масштабованість, необхідні для сучасних кіберфізичних систем. Висновки демонструють потенціал використання блокчейн-технологій для підвищення безпеки доступу та управління інформаційними ресурсами підприємств.

Проблема управління доступом до інформаційних ресурсів підприємств стає все більш актуальною в умовах сучасних кіберзагроз. У науковій літера-

турі розглядаються різні підходи до вирішення цього питання, зокрема використання інноваційних технологій для підвищення ефективності управління доступом і забезпечення високого рівня безпеки. Одним із підходів, розроблених у контексті дистанційного доступу до ресурсів, є запропонована Могильним система віддаленого доступу до інформаційних ресурсів комп'ютерних лабораторій на основі технології VPN, що дозволяє налаштовувати безпечне середовище для роботи в умовах віддаленого доступу [1].

Ключові виклики кібербезпеки, зокрема для хмарних обчислювальних середовищ, розглянуті в дослідженні Опірського, який акцентує увагу на загрозах у хмарній інфраструктурі та шляхах їх мінімізації. Його робота демонструє важливість адаптивних механізмів захисту для забезпечення безпеки даних у таких умовах [2]. Крім того, робота з оцінки ризиків інформаційної безпеки для персоналу підкреслює потребу у створенні багатовимірних моделей класифікації інформації для полегшення управління ризиками та забезпечення належного рівня захисту [3].

Дослідники також звертають увагу на можливість інтеграції технології блокчейн із ролеорієнтованою моделлю доступу (RBAC), що забезпечує гнучке управління доступом та значно підвищує захист інформаційних ресурсів [4]. Впровадження блокчейну дозволяє забезпечити високу прозорість і незмінність записів про доступ, зберігаючи дії користувачів як транзакції, що робить систему стійкою до зовнішніх загроз [5].

Однією з ключових моделей для управління доступом є ролеорієнтована модель (RBAC), яка визначає права доступу користувачів на основі їхніх ролей в організації. Цей підхід дозволяє чітко розмежувати рівні доступу до інформаційних ресурсів, що особливо важливо для великих підприємств із складною структурою. Проте класичний підхід до RBAC має певні обмеження, зокрема, труднощі з адаптацією до швидких змін у ролях користувачів та потребах бізнесу.

Інтеграція блокчейн-технології в модель RBAC розширює можливості управління доступом, дозволяючи автоматизувати контроль за діями користувачів і підвищити надійність системи безпеки. Блокчейн надає можливість зберігати всі записи про доступ у вигляді транзакцій, що зберігаються у незмінній формі. Це забезпечує прозорість усього процесу доступу та дозволяє проводити аудит у разі необхідності [4]. Крім того, використання смарт-контрактів у поєднанні з RBAC дозволяє автоматично налаштовувати права доступу, що робить модель гнучкішою та здатною реагувати на зміни в реальному часі [5].

Таким чином, поєднання блокчейн-технології з моделлю RBAC формує надійну й масштабовану систему управління доступом, яка враховує потреби

підприємств у гнучкому та захищеному контролі за інформаційними ресурсами.

Для забезпечення ефективного управління доступом і підвищення рівня захисту інформаційних ресурсів інтеграція блокчейн-технологій із моделлю RBAC стає стратегічним кроком. Впровадження блокчейну дозволяє використовувати смарт-контракти для зберігання правил доступу та записів усіх операцій, пов'язаних із доступом до ресурсів. Такий підхід забезпечує децентралізований контроль над доступом та унеможливорює зміну або видалення записів, створюючи незмінну історію транзакцій.

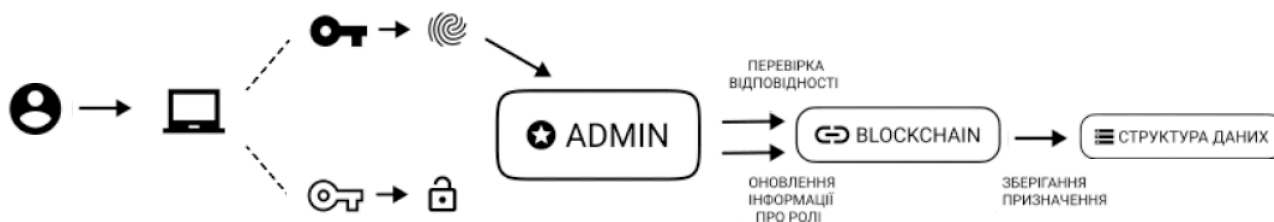


Рисунок 1 – Діаграма комбінованої моделі *RBAC*-блокчейн

Рисунок 1 демонструє, як відбувається процес управління доступом через смарт-контракти, де кожен доступний ресурс зберігається у вигляді блоків із записом про відповідний рівень доступу користувача. Це значно знижує ризик несанкціонованого доступу, оскільки будь-яка спроба зміни або втручання в систему потребує внесення змін у блокчейн, що є практично неможливим завдяки його криптографічному захисту.

Крім того, блокчейн надає можливість реалізувати функції аудиту та моніторингу доступу в режимі реального часу, що забезпечує додатковий рівень безпеки. При цьому сам процес управління доступом стає більш прозорим, оскільки всі дії користувачів фіксуються та можуть бути відстежені відповідно до вимог корпоративної політики безпеки.

Запропонована комбінована модель *RBAC*-блокчейн не тільки підвищує безпеку інформаційних ресурсів, але й забезпечує гнучкість у налаштуванні доступу. Завдяки використанню смарт-контрактів рольові права доступу можуть автоматично змінюватися відповідно до змін у структурі підприємства або з урахуванням специфіки конкретних завдань. Наприклад, коли користувач отримує тимчасову роль або виконує нові функції, смарт-контракт автоматично змінює рівень його доступу на основі попередньо визначених параметрів.

Ключовим аспектом цієї моделі є можливість масштабованості, що особливо важливо для великих організацій, де кількість користувачів та інформаційних ресурсів постійно змінюється. Система автоматично адаптується

ся до нових користувачів та ролей, забезпечуючи точний розподіл прав доступу відповідно до встановлених критеріїв. Це дозволяє значно зменшити адміністративне навантаження, яке зазвичай виникає при ручному налаштуванні доступу для кожного користувача.

Крім того, блокчейн забезпечує додатковий захист від загроз кібербезпеці завдяки своїй стійкості до змін та зовнішніх втручань. Кожна дія, що стосується доступу до інформаційних ресурсів, зберігається як транзакція в блокчейні, створюючи незмінний ланцюг записів. Таким чином, будь-яка спроба стороннього втручання миттєво виявляється і блокується, що робить систему надзвичайно надійною для організацій із високими вимогами до безпеки.

Інтеграція блокчейн-технологій у ролеорієнтовану модель RBAC відкриває широкі можливості для підвищення ефективності управління доступом до інформаційних ресурсів. Однією з головних переваг цього підходу є прозорість і надійність усіх процесів, пов'язаних із доступом, що дозволяє не лише забезпечити безпеку, але й оптимізувати управління інформаційними ресурсами. Усі дії з доступом зберігаються як незмінні записи в блокчейні, що надає можливість швидкого аудиту в разі підозри на несанкціоновані дії.

Модель також підтримує автоматичне оновлення прав доступу завдяки смарт-контрактам, що дозволяє оперативно адаптувати систему до нових потреб підприємства. Це забезпечує більшу гнучкість у використанні ресурсів та швидкість у реагуванні на зміни в організаційній структурі або умовах роботи. Крім того, така система здатна забезпечити безперервний моніторинг користувацьких дій, що підвищує рівень безпеки та дає можливість оперативно реагувати на потенційні загрози.

Підхід із застосуванням блокчейну робить модель стійкою до зовнішніх втручань і зломів, що є важливою перевагою в умовах постійно зростаючого рівня кіберзагроз. Комбінована модель RBAC-блокчейн створює інтегровану систему захисту, яка не лише контролює доступ, але й забезпечує динамічне керування правами доступу відповідно до потреб і умов використання інформаційних ресурсів.

Запропонована комбінована модель управління доступом, яка поєднує модель RBAC із блокчейн-технологією, показала свою ефективність у підвищенні безпеки інформаційних ресурсів підприємств. Використання блокчейну для зберігання записів про доступ та смарт-контрактів для автоматичного контролю прав доступу забезпечує високу надійність, прозорість і гнучкість системи. Стійкість до втручань та незмінність записів блокчейну надають можливість захисту від кіберзагроз і забезпечують можливість для швидкого аудиту та моніторингу дій користувачів. Крім того, автоматизоване оновлення прав доступу відповідно до потреб організації знижує адміністративні вит-

рати, підвищуючи продуктивність управління інформаційною безпекою. Таким чином, запропонований підхід є перспективним рішенням для сучасних підприємств, що працюють у динамічному середовищі, та може бути основою для подальших досліджень у сфері кібербезпеки.

Список використаних джерел:

1. Могильний Г. Впровадження системи віддаленого доступу до інформаційних ресурсів комп'ютерних лабораторій. 2024.
2. Опірський, І. Дослідження та аналіз проблем та викликів, що виникають у забезпеченні кібербезпеки в хмарних обчисленнях. *Ukrainian Information Security Research Journal*, 26(1), 76–88. 2023.
3. Коробейнікова, Т. І., Ямнич, А. Б. Огляд питання оцінки ризиків інформаційної безпеки для персоналу. *International scientific integration 2023: Міжнародна наукова конференція*, 11 липня 2023 р.: тези доповідей, Сіетл, США: ProConference, 18–25. <https://doi.org/10.30888/2709-2267.2023-19-01-008>.
4. Rashid, A., Masood, A., & Khan, A. U. R. ACS-IoT: Smart contract and blockchain assisted framework for access control systems in IoT enterprise environment. *Wireless Personal Communications*, 2024, 1–22. <https://doi.org/10.1007/s11277-024-11266-1>.
5. Коробейнікова Т. І. Багатовимірна матриця класифікації інформації для оцінки ризиків інформаційної безпеки / Т. І. Коробейнікова, А. Б. Ямнич // Інформаційні технології та комп'ютерна інженерія – 2024. – №2. – С. 91–106. – ISSN 1999–9941

Ключові слова: блокчейн, контроль доступу, інформаційні ресурси, RBAC, кібербезпека.

Keywords: blockchain, access control, information resources, RBAC, cybersecurity.

ПОСИЛЕННЯ ЗАХОДІВ БЕЗПЕКИ ПРОТИ ЦИФРОВИХ ЗАГРОЗ У ТРАНСКОРДОННИХ ФІНАНСОВИХ СИСТЕМАХ

Гуренко Марк

студент 1 курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

В сучасному світі транскордонні фінансові системи швидко еволюціонують завдяки досягненням у технологіях та зростаючій інтеграції. Прогнозується, що ринок міжнародних платежів досягне 350 мільярдів доларів США протягом найближчих десяти років, що ставить фінансові установи перед безпрецедентними викликами в забезпеченні захисту транзакцій від численних цифрових загроз [1].

I. Передумови

Транскордонні платежі є критично важливими для глобальної економіки, оскільки вони спрощують операції між підприємствами та споживачами по всьому світу. Успішна інтеграція цифрових і фінансових ринків значною мірою залежить від надійних та ефективних платіжних систем, які підтримують комерцію, електронну торгівлю та фінансові послуги [2].

Країни з перехідною економікою та країни, що розвиваються, зазнають специфічних труднощів в оптимізації процесів транскордонних платежів, головним чином через складність залучення до процесу різних фінансових установ, а також численних комісій, коливань обмінних курсів та регуляторних вимог [3]. Глобальна взаємозалежність ринків вимагає від підприємств адаптації до нових ризиків, зокрема до підвищеної волатильності, геополітичних чинників та складнощів, пов'язаних з валютними операціями та дотриманням нормативних вимог [4].

II. Цифрові загрози

Кіберзагрози залишаються однією з найбільш актуальних цифрових загроз, з якими стикаються фінансові системи. Кіберзлочинці постійно вдосконалюють свою тактику, намагаючись впливати на організації, об'єкти критичної інфраструктури та уряди за допомогою складних атак, таких як програми-вимагачі, витоки інформації та фішингові схеми [5]. Зростання цих атак підкреслює вразливість банківського сектору, що вимагає стабільного управління ризиками і безпечних мережевих регламентів.

Зловживання цифровими активами несе з собою серйозні ризики фінансування незаконної діяльності, яка включає відмивання грошей, кіберзлочинність та тероризм [6]. Ці дії загрожують не лише окремим фінансовим установам, але й цілісності світової фінансової системи. Ефективні регуляторні рамки є необхідними для уникнення цих загроз і дотримання стандартів протидії відмиванню коштів та фінансуванню тероризму.

Кіберінциденти, що порушують безпеку даних, можуть призвести до значних фінансових втрат і репутаційних проблем. Конфіденційність фінансових даних викликає серйозні занепокоєння, особливо у випадках міжнародного обміну інформацією [3].

Взаємозв'язок фінансових установ призводить до зростання операційних ризиків. Кібератака на одну організацію може мати далекосяжні наслідки для всього сектору [7]. Ця взаємопов'язаність підкреслює нагальну необхідність комплексного підходу до управління цифровими ризиками, що включає в себе планування на випадок надзвичайних ситуацій та міжвідомчу співпрацю.

III. Заходи безпеки

Інтеграція заходів кібербезпеки з новими технологіями є критично важливою для підтримки високих стандартів безпеки у фінансових організаціях. Більш тісна інтеграція існуючих концепцій, таких як ISO та Національного інституту стандартів і технологій (NIST) Cybersecurity Framework (CSF), може суттєво спростити застосування нових технологій [8]. Нормативно-правова база повинна бути узгоджена для підвищення стійкості до кіберзагроз,

які постійно розвиваються, у відповідь на вдосконалення тактик зловмисників та технологічний прогрес [9].

Забезпечення стабільності платіжних систем має вирішальне значення. Процеси автентифікації та авторизації є критично важливими і потребують використання криптографічних методів для підтвердження транзакцій і захисту від атак, які компрометують облікові дані користувачів [10].

IV. Заходи безпеки

Регуляторне середовище навколо цифрових фінансових механізмів характеризується розвитком стандартів, що формуються під впливом геополітичних чинників з боку Європейського Союзу, Сполучених Штатів та Китаю. Ці нормативні впровадження намагаються вирішити ключові проблеми, пов'язані із цифровими валютами центральних банків (CBDC) і значно ширшим криптовалютним сегментом [11]. Наприклад, Китай запровадив комплексний державний моніторинг, що відображає більш централізований підхід порівняно з регуляторними рамками, які розробляються західними країнами.

Велика Двадцятка визначила своїм пріоритетом вдосконалення транскордонних платіжних систем, прагнучи зробити послуги швидшими, дешевшими, прозорішими та інклюзивнішими. Дорожня карта вдосконалення транскордонних платежів, запущена в 2020 році, окреслює багаторічну стратегію для досягнення цих цілей, підкреслюючи необхідність регуляторної узгодженості та співпраці між міжнародними фінансовими організаціями [2, 12]. Співпраця між міжнародними організаціями, такими як Група з розробки фінансових заходів боротьби з відмиванням грошей (FATF), призвела до створення концепцій боротьби з відмиванням грошей та фінансуванням тероризму, що має вирішальне значення для дотримання вимог у транскордонних транзакціях [13].

Удосконалення заходів безпеки у контексті цифрових загроз у транскордонних фінансових системах вимагає комплексного підходу, що охоплює технологічні, регуляторні та операційні виклики. Оскільки фінансовий сектор продовжує розвиватися, стає все більш критично важливим, треба мати надійні системи безпеки і сприяти міжнародній співпраці та адаптувати регуляторні стандарти до нових умов. Визначаючи пріоритети в цих зусиллях, фінансові установи зможуть краще протистояти множинним загрозам цифрового середовища, підтримуючи стабільність і цілісність глобальної фінансової системи.

Список використаних джерел:

1. Suvarna, Radha. Unlocking cross-border payments: Trends financial institutions should address // Banking Dive. URL: <https://www.bankingdive.com/spons/unlocking-cross-border-payments-trends-financial-institutions-should-address/718848/> (дата звернення: 13.10.2024).

2. IMF and World Bank Approach to Cross-Border Payments Technical Assistance // International Monetary Fund. Monetary and Capital Markets Department and World Bank. 2022. 45 с.
3. Adelmann, Frank, Jennifer A. Elliott, Ibrahim Ergen, Tamas Gaidosch, Nigel Jenkinson. Cyber Risk and Financial Stability: It's a Small World After All // International Monetary Fund. 2023. 75 с.
4. How Innovation and Digitization are Transforming Cross-Border Payments // Bank of America. URL: <https://business.bofa.com/en-us/content/cross-border-payments.html> (дата звернення: 13.10.2024).
5. Ferreira, Ricardo. The Evolution of Cybersecurity in Banking // Fortinet Blog. URL: <https://www.fortinet.com/blog/industry-trends/cybersecurity-in-banking> (дата звернення: 14.10.2024).
6. Executive Order on Ensuring Responsible Development of Digital Assets // White House. 2022. 9 березня. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/> (дата звернення: 13.10.2024).
7. Cipollone, Piero. One step ahead: protecting the cyber resilience of financial infrastructures // European Central Bank. URL: <https://www.ecb.europa.eu/press/key/date/2024/html/ecb.sp240117~3e839b396f.en.html> (дата звернення: 14.10.2024).
8. Atkins, Lamont, Soumya Banerjee, Martin Boer, Lauren Craig, Justin Greis, Grace Hao, Melanie Idler. The cyber clock is ticking: Derisking emerging technologies in financial services // McKinsey & Company. URL: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cyber-clock-is-ticking-derisking-emerging-technologies-in-financial-services> (дата звернення: 14.10.2024).
9. Healey, Jason, Patricia Mosser, Katheryn Rosen, Adriana Tache. The future of financial stability and cyber risk // Brookings. URL: <https://www.brookings.edu/articles/the-future-of-financial-stability-and-cyber-risk/> (дата звернення: 13.10.2024).
10. Fanti, Giulia, Kari Kostianen, William Howlett, Josh Lipsky, Ole Moehr, John Paul Schnapper-Casteras, Josephine Wolff. Missing Key: The challenge of cybersecurity and central bank digital currency // Atlantic Council. URL: <https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/> (дата звернення: 15.10.2024).
11. Tran, Hung, Barbara C. Matthews. CBDCs will further fragment the global economy—and could threaten the dollar // Atlantic Council. URL: <https://www.atlanticcouncil.org/blogs/econographics/cbdcs-will-further-fragment-the-global-economy-and-could-threaten-the-dollar/> (дата звернення: 16.10.2024).
12. Adrian, Tobias. A Cross-Border Payments, Exchange, and Contracting Platform for the 21st Century // Twelfth Annual BIS Consultative Council for the Americas Research Conference. Mexico City, IMF. 2022. URL: <https://www.imf.org/en/News/Articles/2022/11/18/sp-cross-border-payments-exchange-contracting-platform-21st-century> (дата звернення: 16.10.2024).
13. Securing the Global Financial System: AML Challenges in Cross-Border Transactions // Financial Crime Academy. URL: <https://financialcrimeacademy.org/aml-challenges-in-cross-border-transactions/> (дата звернення: 16.10.2024).

Ключові слова: транскордонні фінансові системи, цифрові ризики, кібербезпека, транскордонні платежі, кіберзагрози, відмивання грошей, криптографія, міжнародна співпраця, фінансові регуляції, цифрові активи.

Keywords: cross-border financial systems, digital risks, cybersecurity, cross-border payments, cyber threats, money laundering, cryptography, international cooperation, financial regulations, digital assets.

Науковий керівник: к.т.н., доцент *Задерейко Олександр*

ВИКОРИСТАННЯ CRM ДЛЯ ЗБІЛЬШЕННЯ ОБСЯГІВ ПРОДАЖІВ

Дем'янова Тетяна

*студентка 4 курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

CRM (Customer Relationship Management) - система управління відносинами з клієнтами, її використання є ефективним інструментом для збільшення обсягів продажів. Вона допомагає компаніям організовувати, автоматизувати та оптимізувати процеси взаємодії з клієнтами на різних етапах продажів.

Такі системи, дозволяють зберігати всі дані про клієнтів в одному місці, включаючи історію комунікацій, контакти, уподобання та покупки, що дозволяє продавцям легше і швидше знаходити потрібну інформацію для ефективної комунікації з клієнтами, це скорочує час на підготовку і дозволяє приділяти більше часу безпосередньо продажам. З їх допомогою стає зручно сегментувати базу клієнтів на основі різних критеріїв, наприклад: поведінки, історії покупок, регіону тощо. Це дозволяє краще розуміти потреби різних груп клієнтів і пропонувати їм персоналізовані пропозиції, що підвищує ймовірність конверсії.

Завдяки використанню CRM-систем стає можливим автоматизувати рутинні завдання, такі як надсилання нагадувань, оновлення статусу лідів або відправка електронних листів. Це дозволяє продавцям зосередитися на основних процесах взаємодії з клієнтами, що збільшує продуктивність та ефективність продажів.

Одна з не менш важливих функцій, покращення прогнозування продажів, дозволяє більш точно аналізувати дані про попередні продажі, поведінку клієнтів і тенденції, яка дозволяє будувати більш точні прогнози щодо майбутніх продажів. Таким чином, бізнесу зручно планувати свої дії і ресурсні потреби відповідно до очікуваних обсягів продажів. А також, така структура допомагає тримати під контролем всі аспекти відносин з клієнтами, включаючи їхнє задоволення після покупки. Завдяки автоматизованим сповіщенням

та нагадуванням компанія може підтримувати клієнтів, пропонувати їм нові продукти або послуги, які підвищують рівень утримання клієнтів і повторних продажів, що призводить до підвищення рентабельності бізнесу та виходу на нові можливості.

Збільшення ефективності маркетингу за допомогою інтеграції CRM з маркетинговими кампаніями дозволяє автоматично відстежувати ефективність кожної і адаптувати їх на основі поведінки клієнтів. З таким прогресом гарантовано налаштовувати більш релевантні і персоналізовані пропозиції, які підвищують конверсію та збільшують обсяги продажів, а також залучення ще більше нової аудиторії.

Система управління відносинами з клієнтами створює єдину платформу для співпраці різних відділів компанії (продажі, маркетинг, служба підтримки), що дозволяє підвищувати взаємодії між відділами, краще координувати дії і зростання ефективності обслуговування клієнтів. Також, вона допомагає не лише відстежувати існуючих клієнтів, але й ефективно управляти лідами, і так само дає змогу фільтрувати, розподіляти їх між менеджерами та автоматично пріоритезувати за ступенем готовності до покупки. Так само й можна за допомогою CRM керувати зустрічами з клієнтами, автоматично створювати нагадування про важливі дзвінки, зустрічі або інші події, пов'язані з продажами, що дозволяє менеджерам з продажів завжди залишатися на зв'язку і вчасно виконувати завдання. Ще система дозволяє легко відстежувати прогрес угоди на різних етапах продажів — від першого контакту з клієнтом, до завершення угоди та післяпродажного обслуговування. Завдяки цьому менеджери можуть оперативно реагувати на проблеми або можливості на кожному етапі і вчасно коригувати свою стратегію.

Деякі системи дозволяють керувати не лише відносинами з клієнтами, але й з постачальниками або іншими партнерами. Це може бути корисно для компаній, які працюють з великою кількістю постачальників товарів чи послуг, оскільки допомагає оптимізувати процеси закупівлі та забезпечення.

Сучасні CRM-системи часто мають мобільні версії, що дозволяє продавцям мати доступ до інформації про клієнтів, вчасно відповідати на запити, швидко приймати замовлення та готувати до відправки в будь-який час і з будь-якого місця. Також зручна фішка, що можна підтримувати різні канали комунікації, наприклад через: телефон, електронну пошту, соціальні мережі, чат-боти, месенджери, за допомогою яких набагато зручніше об'єднувати всю інформацію з різних каналів в одну систему і дає можливість компанії швидко обробляти інформацію стосовно лідів і не втрачати потенційні можливості для продажів.

Використання ботів у CRM-системах стало однією з найбільш ефективних інновацій для покращення взаємодії з клієнтами та автоматизації про-

цесів. Чат-боти та голосові боти в CRM-системах допомагають компаніям швидко обробляти запити клієнтів, виконувати рутинні завдання та забезпечувати клієнтам безперебійний досвід обслуговування. Вони можуть працювати з потенційними клієнтами, ставлячи їм запитання і визначаючи, чи підходять вони для подальшого контакту менеджера з продажів, наприклад, може запитати, якими продуктами цікавиться клієнт, який у нього бюджет або до якої галузі він належить, і на основі відповідей передати інформацію кваліфікованому менеджеру для завершення угоди. Також боти можуть автоматично надсилати нагадування про зустрічі, нагадувати менеджерам про важливі події чи дії, пов'язані з клієнтами, або відправляти повідомлення безпосередньо клієнтам з нагадуванням, що їх замовлення вже в дорозі чи вже на пошті і чекає на отримання, або подяка за користування магазином та теплі слова, наприклад «раді вас бачити знов», і виконувати зворотний зв'язок від клієнтів після завершення взаємодії, надсилаючи короткі опитування або запитуючи оцінки задоволеності.

Боти працюють цілодобово, тому клієнти можуть отримувати відповіді на свої запити навіть поза робочим часом компанії. Це покращує рівень обслуговування і допомагає утримувати клієнтів, які очікують миттєвих відповідей.

Висновок

CRM-системи є потужним інструментом для організації та покращення процесу продажів. Вони допомагають збільшити ефективність роботи команди, краще зрозуміти потреби клієнтів, автоматизувати процеси і, як результат, збільшити обсяги продажів.

Список використаної літератури:

1. Що таке CRM? URL: <https://keepincrm.com/what-is-crm-system> (дата звернення: 30.10.2024);
2. "CRM at the Speed of Light" – Паул Грінберг.
3. Козичко Вероніка. Як збільшити продажі за допомогою CRM-системи? URL: <https://apix-drive.com/ua/blog/useful/jak-zbilshiti-prodazhi-za-dopomogoj-crm-sistemi> (дата звернення: 30.10.2024);
4. Як CRM-система допомагає збільшити кількість продажів. URL: https://sitniks.ua/blog_post/yak-srm-systema-dopomagaye-zbilshyty-kilkist-prodazhiv/ (дата звернення: 30.10.2024);
5. Анна Позняк. Навіщо впроваджувати CRM-систему: основні функції та переваги. URL: <https://nethunt.ua/blog/navishcho-vprovadzhuvati-crm-sistemu-osnovni-funktsiyi-ta-perieievaghi/> (дата звернення: 30.10.2024)/

Ключові слова: CRM-системи, клієнти, ліди, компанія, команда, продаж, ефективність, допомога, підвищення, зручність.

Keywords: CRM systems, customers, leads, company, team, sales, efficiency, help, promotion, convenience

Науковій керівник: *к.т.н., доц. Задерейко Олександр*

ІНФОРМАЦІЙНИЙ ПРОСТІР УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Дробишевська Вікторія

здобувачка другого (магістерського) рівня вищої освіти Інституту права і безпеки Одеського державного університету внутрішніх справ

На сьогодні Україна опинилася в центрі глобальних геополітичних подій, що викликає необхідність глибокого аналізу інформаційної безпеки в умовах військової агресії. Введення воєнного стану в державі згідно із Законом України «Про правовий режим воєнного стану» передбачає активізацію спеціальних механізмів захисту національних інтересів, надання повноважень державним органам для забезпечення безпеки та відсічі зовнішньої агресії [1]. У таких умовах питання національної інформаційної безпеки стає невід'ємною складовою загального стратегічного захисту країни. Адже інформаційні атаки можуть зруйнувати громадську довіру, дестабілізувати суспільство та створити умови для маніпулювання суспільною думкою.

Постійна військова та економічна загроза від країни-агресора активізувала увагу української держави та суспільства на питаннях інформаційної стійкості. Український інформаційний простір перебуває під постійним тиском з боку іноземних сил, які прагнуть не лише знизити бойовий дух населення, а й посіяти розбрат та недовіру до офіційних джерел інформації. Зовнішній інформаційний тиск виявляється як у традиційних засобах масової інформації, так і в цифрових медіа, що охоплюють величезну аудиторію в соціальних мережах. Саме через ці канали агресор намагається поширити вигідну для себе дезінформацію, підриваючи основи української державності.

Значення інформаційної безпеки підвищилося також через специфіку гібридної війни, яка є характерною для 21 століття.

Гібридна війна – це вид війни, в якому поєднуються різноманітні засоби ведення бойових дій та впливу на противника, зокрема військові, інформаційні, кібернетичні, економічні та політичні [2].

Гібридна війна, що ведеться проти України, включає традиційні військові дії, інформаційну та кібернетичну складову, економічні санкції, а також дипломатичний тиск. Поєднання цих факторів створює особливу складність для державної політики безпеки, оскільки кожен компонент війни спрямований на досягнення максимальної ефективності через різноманітні канали впливу. Так, поряд із бойовими діями, інформаційна війна стає потужним інструментом агресора, який поширює дезінформацію та маніпулює інформаційним середовищем заради власних політичних інтересів.

Філіп Брідлав, колишній головнокомандувач Об'єднаних збройних сил НАТО в Європі, охарактеризував інформаційні операції росії як "найбільш масштабний інформаційний бліцкриг у сучасній історії" [3]. Завдяки потужним

ресурсам та використанню соціальних мереж, РФ вибудувала систему дезінформаційних кампаній, що формують викривлену картину подій для широкого кола аудиторії. Така інформаційна війна використовує методи перекручення фактів, створення фейкових новин та маніпуляції контекстом, що суттєво ускладнює процеси прийняття рішень і підриває довіру до українських та міжнародних джерел.

В умовах протистояння інформаційній агресії українська держава розробила низку заходів для зміцнення власного інформаційного простору. Відповіддю на потік дезінформації стало створення телемарафону «Єдині новини», який цілодобово забезпечує громадян перевіреною інформацією. Однак, агресор здійснює спроби блокування українських телеканалів на окупованих територіях, намагаючись обмежити доступ до правдивої інформації. Окупаційна влада вдається до дій, що мають на меті дезорієнтацію населення, зокрема шляхом відключення електроенергії та блокування українських телеканалів.

Крім того, інформація стала невід'ємною частиною сучасної міжнародної політики, і маніпулювання нею може посилити міждержавні конфлікти. В умовах, коли кордони між країнами більше не є бар'єром для інформаційного впливу, важливим є підвищення інформаційної грамотності населення. Створення стратегії медіаграмотності дозволяє громадянам критично сприймати інформацію та протистояти дезінформації, що надходить з різних джерел. Розвиток цифрових медіа робить суспільства відкритішими, проте й водночас вразливішими до зовнішнього впливу, що вимагає обережного підходу до захисту національного інформаційного простору.

Ефективний захист інформаційного простору передбачає, окрім протидії дезінформації, активне формування позитивного міжнародного іміджу України. Залучення міжнародних партнерів для обміну інформацією, технологіями захисту та кращими практиками протидії інформаційним загрозам стає необхідним елементом сучасної стратегії інформаційної безпеки. Таким чином, державні структури мають не лише захищати інформаційний простір, але й працювати над іміджевими аспектами, що формують сприйняття України на глобальній арені.

Окрему роль у сучасній інформаційній війні відіграють соціальні мережі, зокрема телеграм-канали. Вони стали ефективним інструментом для швидкого поширення інформації серед військових і цивільного населення. Однак, такі канали є водночас вразливими до атак із боку ворога, який намагається їх використати для розповсюдження дезінформації та психологічного впливу. Задля захисту цих платформ варто впроваджувати такі заходи:

1. Процедури верифікації для адміністраторів каналів, включно з перевіркою особистих документів та контактних даних.

2. Увімкнення двофакторної автентифікації для всіх облікових записів для захисту від несанкціонованого доступу.

3. Застосування технологій шифрування для захисту від втручань.

4. Впровадження чітких політик модерації контенту із залученням кваліфікованих модераторів, які слідкують за достовірністю та актуальністю опублікованих матеріалів.

5. Контроль за доступом до конфіденційної інформації з розподілом прав користувачів.

6. Використання сучасних засобів кіберзахисту: фаєрволів і антивірусів, що захищають від шкідливих атак.

Ці заходи забезпечують контроль над інформацією, яка поширюється через канали, а також захищають користувачів від впливу деструктивної інформації. Вони дозволяють запобігти викривленню даних, а також виявляти осіб, які співпрацюють із агресором. Одним із методів може бути створення фейкових телеграм-каналів, які імітують проросійські платформи, але насправді використовуються для виявлення симпатиків агресора та збору інформації про їхню діяльність.

Інформаційний простір в умовах гібридної війни стає критичним елементом національної безпеки. Сьогодні Україна має враховувати всі аспекти захисту інформації – від протидії кібератакам до формування позитивного іміджу країни в світі [4]. Лише системна та скоординована політика інформаційної безпеки здатна забезпечити стійкість перед зовнішніми загрозами та захистити суспільство від маніпуляцій і деструктивного впливу.

Список використаних джерел:

1. Закон України «Про правовий режим воєнного стану» (Відомості Верховної Ради (ВВР), 2015, № 28, ст. 250). URL: <https://zakon.rada.gov.ua/laws/show/389-19#Text> (дата звернення 31.10.2024).
2. Велика українська енциклопедія. URL: https://vue.gov.ua/Гібридна_війна.
3. SACEUR: Allies must prepare for Russia 'hybrid war'. URL: <https://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464>.
4. Козьмініх А.В. Кібербезпека та кібератаки в умовах гібридної війни. Національний університет «Одеська юридична академія». URL: <http://surl.li/nedgp>.

Ключові слова: гібридна війна, інформаційна безпека дезінформація медіаграмотність кіберзахист

Keywords: hybrid warfare, information security, disinformation, media literacy, cybersecurity

Науковий керівник: *Моргунова Тетяна Іванівна, к.т.н., доц., кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ*

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В БАНКІВСЬКІЙ СФЕРІ

Закірко Юрій

студент 1 курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасна банківська система є однією з найбільш вразливих галузей щодо кіберзлочинності. З розвитком цифрових технологій, обробка величезних обсягів фінансової інформації вимагає впровадження ефективних засобів захисту. Враховуючи значну кількість приватної, конфіденційної та фінансової інформації, що циркулює в банківських мережах, особливої уваги потребує питання інформаційної безпеки.

Кіберзлочинність є однією з найбільших загроз для банків. Хакери використовують різні техніки для отримання доступу до банківських систем і викрадення даних клієнтів. Серед найбільш поширених атак можна виокремити [1]:

1. Фішинг – метод, за допомогою якого зломисники намагаються отримати конфіденційні дані користувачів через підроблені електронні листи або вебсайти.

2. Шкідливе програмне забезпечення (Malware) – спеціальні програми, які використовуються для проникнення в комп'ютерні системи і викрадення даних.

3. Атаки на банкомати (АТМ) – використання шкідливих програм або фізичних пристроїв для отримання доступу до грошових коштів та персональних даних клієнтів.

Окрім зовнішніх загроз, важливим аспектом є внутрішні ризики. Вони можуть бути спричинені працівниками банку, які мають доступ до конфіденційної інформації. Недостатньо кваліфіковані або недобросовісні працівники можуть випадково або навмисно викрити або пошкодити дані.

Безпечне використання систем дистанційного банківського обслуговування, складається з [2]:

- проведення аналізу програмного забезпечення, встановленого на веб-серверах систем «Клієнт-Інтернет-Банк», а також клієнтських частин систем дистанційного банківського обслуговування, встановлених у клієнтів;

- вжиття заходів щодо оновлення застарілих версій програмного забезпечення і встановлення актуальних оновлень безпеки та щодо усунення вразливостей програмного забезпечення банківського обслуговування, операційних систем;

- застосовування захищених носіїв ключової інформації для накладання електронного цифрового підпису та методи багатфакторної автентифікації;

- розробка порядку дій працівників і клієнтів банку у випадках виявлення несанкціонованого доступу (чи підозри у спробі доступу) до рахунку;
- визначити уповноважених осіб банку, які відповідатимуть за взаємодію з правоохоронними органами, та порядок такої взаємодії у разі виявлення несанкціонованих операцій, здійснених із використанням систем дистанційного банківського обслуговування; постійне проведення роз'яснювальної роботи серед клієнтів.

Одним з найбільш ефективних способів захисту даних є їх шифрування. Шифрування забезпечує перетворення інформації в закритий формат, який може бути прочитаний лише за наявності ключа дешифрування. Для банків особливо актуальним є використання асиметричних методів шифрування, які забезпечують надійність обміну ключами.

Сучасні банківські системи впроваджують багатфакторну аутентифікацію (MFA), яка вимагає підтвердження особи через кілька незалежних джерел (паролі, SMS-коди, біометричні дані тощо). Це значно підвищує рівень безпеки і знижує ризик несанкціонованого доступу.

Захист периметру банківських мереж за допомогою міжмережевих екранів (файрволів) і систем виявлення вторгнень є важливим кроком у забезпеченні інформаційної безпеки. Ці системи дозволяють виявляти та блокувати підозрілу активність у реальному часі [3].

Системи управління інформаційною безпекою (SIEM) забезпечують збір, аналіз та кореляцію даних з різних джерел з метою виявлення аномалій або підозрілої активності. Використання таких систем допомагає швидко реагувати на інциденти та мінімізувати шкоду.

У більшості країн існують чіткі вимоги до захисту інформації в банківській сфері. Наприклад, Закон України "Про захист персональних даних" вимагає забезпечення конфіденційності та безпеки особистої інформації клієнтів банків. Банківські установи також мають відповідати міжнародним стандартам інформаційної безпеки, таким як ISO/IEC 27001 [4].

Захист інформації у банківській сфері є важливим завданням для забезпечення стабільності та надійності фінансових інститутів. Впровадження сучасних технологій шифрування, аутентифікації, управління інцидентами та захисту мереж, а також відповідність законодавчим вимогам є ключовими складовими для забезпечення інформаційної безпеки. Однак, постійний розвиток технологій вимагає регулярного оновлення та вдосконалення заходів захисту для протидії новим загрозам.

Список використаних джерел

1. Бугера Д. М. Робота банківської системи в умовах воєнного стану. Реалії сьогодення у банківській діяльності України : матеріали наукового семінару. м.Ірпінь, 18 жовтня 2022 року. Ірпінь. 2022. С. 76.

2. Довгань О., Ткачук Т. Система інформаційної безпеки України: онтологічні ви-
міри. Інформація і право. 2018. № 1(24) С. 89–103.
3. Заросило В. О. Загрози фінансовій безпеці та їх класифікація. Міжрегіональна
Академія управління персоналом. Київ, 2017. No 52(1). С. 17–22.
4. Захист прав споживачів фінансових послуг на деокупованих територіях України :
практичний посібник клініциста / Шолкова Т. О., Кармаліта М. В., Мацелик Т. О.
Субіна Т. В. Київ : Алерта, 2020. 270 с.

Ключові слова: системи управління, атаки на банкомати, банківські системи, захист ін-
формації у банківській сфері

Keywords: management systems, attacks on ATMs, banking systems, information protection in
the banking sector

Науковий керівник: к.т.н., доцент *Задерейко Олександр*

КІБЕРБЕЗПЕКА, ЯК НЕОБХІДНА СКЛАДОВА МАРКЕТИНГОВИХ ІНСТРУМЕНТІВ

Кошева Катерина

*студентка 2-го курсу магістратури факультету кібербезпеки та інформацій-
них технологій Національного університету «Одеська юридична академія»*

У сучасному світі цифрові технології стали невід'ємною частиною бізне-
су, а маркетингові стратегії все більше залежать від електронних платформ.
Використання персональних даних клієнтів, аналітика поведінки користува-
чів та автоматизація маркетингових процесів вимагають надійних інструмен-
тів для забезпечення безпеки. Кібербезпека стає ключовим фактором, який
не лише забезпечує захист даних, але й зміцнює довіру клієнтів до компанії,
що підвищує ефективність маркетингових кампаній.

Цифрові технології повністю трансформували бізнес: більше 70% ком-
паній на глобальному рівні використовують електронні платформи для про-
сування своїх товарів і послуг. Це вимагає комплексного збору даних та їх
надійного захисту. У зв'язку з цим кібербезпека стає обов'язковим елемен-
том ефективної маркетингової стратегії. За даними IBM, середня вартість
витоку даних у 2021 році склала 4,24 мільйона доларів США, що підобхідність
якісного захисту даних для мінімізації фінансових ризиків та зміцнення довіри
клієнтів. [2]

З розвитком цифрових технологій маркетинг також зазнав значних
змін. Сучасні маркетингові стратегії базуються на аналітиці великих даних.
Тепер маркетологи мають доступ до великої кількості персональних даних
користувачів, що дозволяє створювати точніші та ефективніші кампанії. На-

приклад, компанії використовують CRM-системи та платформи для електронної пошти для персоналізації пропозицій, що може збільшити їх ефективність на 25–30% . Однак збільшення персональних даних підвищує ризик витоку. У 2022 році було зафіксовано понад 4 тисячі великих витоків даних у всьому світі, що призвело до втрати мільйонів записів про користувачів .

Персональні дані клієнтів, такі як електронні пошти, номери телефонів, банківські реквізити або вподобання, повинні бути надійно захищені. Безпека таких даних, як дані, вподобання та банківська інформація, є важливим фактором довіри до бренду. Як приклад можна навести інцидент із Marriott, коли в результаті витоку було скомпрометовано дані 500 млн клієнтів, що призвело до значних фінансових втрат та втрати репутації компанії. [3]

Які ж є основні загрози для маркетингових платформ? Маркетингові інструменти, такі як CRM-системи, платформи для електронної пошти, веб-аналітика та рекламні системи, можуть бути вразливими до різних кіберзагроз. Серед найпоширеніших можна виділити:

Фішингові атаки: хакери можуть використовувати соціальну інженерію, щоб обманним шляхом отримати доступ до корпоративних систем. Близько 90% усіх кібератак починаються з фішингу. У 2021 році атаки на основі фішингу завдали збитків на суму близько 14 мільярдів доларів .

Зловживання рекламними мережами: За даними Statista, у 2021 році збитки від фальшивих кліків та маніпуляцій у рекламних кампаніях перевищили 35 млрд доларів США [1].

Витоки даних через вразливості вебсайтів: багато маркетингових кампаній покладаються на вебсайти, які можуть бути вразливими до атак типу SQL Injection або XSS.

DDoS атаки: можуть заблокувати доступ до важливих маркетингових платформ, що впливає на проведення кампаній у реальному часі.

З цього можна прийти до логічного висновку, що компанії, які інтегрують кібербезпеку в свої маркетингові стратегії, отримують значну перевагу на ринку. Це стосується не лише захисту даних, але й створення довірчих відносин з клієнтами. У сучасному бізнесі репутація бренду залежить не лише від якості продуктів чи послуг, але й від того, як компанія ставиться до безпеки персональних даних своїх клієнтів.

Більше 50% європейських користувачів готові платити більше за послуги компаній, які демонструють прихильність до захисту їхніх даних . Сертифікати безпеки, такі як ISO/IEC 27001, також сприяють зовіри, що допомагає залучати й утримувати клієнтів. Дослідження Cisco показало, що близько 32% користувачів більш схильні довіряти брендам із високим рівнем захисту даних . [4]

Розглядаючи тему більш предметно, а саме з точки зору технічного аспекту кібербезпеки, для забезпечення захисту даних компанії можуть використовувати такі методи, як: шифрування даних, близько 70% компаній використовують шифрування для захисту даних клієнтів, багатофакторну автентифікацію, за даними Google, використання багатофакттифікації знижує ризик несанкціонованого доступу на 99,9% та моніторинг загроз у реальному часі, через впровадження систем моніторингу компанії мають змогу виявляти загрози на ранніх стадіях, що знижує потенційний збиток на 80%. [5,6]

Хоча переваги захисту даних очевидні, згідно з дослідженням PwC, компанії, що активно інвестують у кібербезпеку, отримують на 15–20% більше довіри з боку клієнтів та на 10–15% більше доходів, реалізація стандартів кібербезпеки потребує значних інвестицій, які можуть складати до 7% річного бюджету компанії. [7]

Таким чином, кібербезпека — це не лише засіб захисту даних, але й важливий аспект маркетингової стратегії на підвищення довіри та лояльності клієнтів. За даними Gartner, компанії, що інвестують у захист даних, можуть скоротити збитки від витоків на 35–40%, що також позитивно впливає на їх репутацію та конкурентоспроможність. [8]

Список використаних джерел:

1. Statista. Digital Marketing Usage Statistics. 2021. URL: [https://www.statista.com/statistics/273018/usage-of-digital-marketing/].
2. IBM Security. Cost of a Data Breach Report. 2021. URL: [https://www.ibm.com/security/data-breach].
3. Marriott Incident Report. 2019. URL: [https://www.theguardian.com/business/2018/nov/30/marriott-hotels-data-breach-guest-reservation-system].
4. Cisco. Annual Cybersecurity Report. 2021. URL: [https://www.cisco.com/c/en/us/products/security/security-reports.html].
5. Google Security Blog. Impact of Multi-Factor Authentication. 2021. URL: [https://security.googleblog.com/2021/05/using-mfa-helps-prevent-account-theft.html].
6. Symantec. Real-Time Threat Monitoring Report. 2021. URL: [https://www.broadcom.com/company/newsroom/press-releases/2021/symantec-thought-leadership-report].
7. PwC. Trust in Cybersecurity Report. 2020. URL: [https://www.pwc.com/gx/en/services/consulting/cybersecurity.html].
8. Gartner. The Business Impact of Data Security. 2021. URL: [https://www.gartner.com/en/insights/data-security].

Науковий керівник: доктор економічних наук, професор, завідувач кафедри кібербезпеки Національного університету «Одеська юридична академія», Горбаченко С. А.

THE IMPACT OF HYBRID THREATS ON THE CYBER SECURITY OF CRITICAL INFRASTRUCTURE IN THE CONTEXT OF MODERN GLOBAL CHALLENGES

Page Nikita

National University «Odesa Law Academy»,
4th year student of the Faculty of Cyber Security and Information Technologies

Hybrid threats combine cyberattacks with other destabilizing methods, such as disinformation, economic pressure, and physical sabotage. These threats are highly complex and can have significant consequences for critical infrastructure. Critical infrastructure, such as energy systems, transportation, and water supply, is vital for a nation's survival. It is vulnerable to cyberattacks due to its complexity and interconnectivity with various systems [1]. The increasing digitalization and globalization intensify the risk of hybrid threats. Modern conflicts often include cyber components, making the defences of national infrastructure more complicated.

Importance of international cooperation, the implementation of cybersecurity standards, enhanced monitoring, and rapid incident response. Aligning cybersecurity technologies with global norms and developing advanced threat detection systems are crucial steps. Hybrid warfare, while not entirely new, has evolved with the integration of modern cyber tools, energy security manipulations, and disinformation campaigns.

Cyberattacks have emerged as a key component in modern hybrid warfare, targeting not only military infrastructure but also essential civilian systems. The security of critical infrastructure, such as energy and communication networks, is paramount, as cyber operations can amplify the effects of traditional warfare. A key takeaway from the Ukrainian experience is the need for increased international cooperation to counteract hybrid threats. NATO and EU collaborations play a crucial role in sharing intelligence and creating resilient defence mechanisms against both conventional and cyber components of hybrid warfare.

A significant aspect of countering hybrid threats is integrating data governance with business process management to protect critical infrastructure. Proactive governance strategies can help in securing digital assets, ensuring accountability, and preventing cascading failures during attacks, particularly in sectors like aviation [2, 4992-4993].

Effective cyber threat intelligence (CTI) is crucial for improving the resilience of critical infrastructures. CTI-driven models can identify and manage vulnerabilities by incorporating human factors, decision-making processes, and proactive measures, which enhance defences against hybrid attacks. Integrating cyber-physical and socio-technical models offers a comprehensive approach to protecting critical infrastructures. By combining these models, threats to physical systems

(e.g., railways) can be mitigated, strengthening security postures against both physical and cyber intrusions [3]. Governments must play a key role in ensuring the cybersecurity resilience of critical infrastructure through legal frameworks and support to private companies that manage this infrastructure [1].

With critical infrastructures increasingly migrating to the cloud, securing cloud environments becomes a crucial topic. This thesis could focus on cloud migration security frameworks, continuous monitoring, and access control models. By evaluating threats in hybrid IT environments and applying zero-trust architectures, organizations can ensure secure data handling in interconnected systems, especially against hybrid threats that exploit cloud vulnerabilities.

Social engineering and human error play a significant role in cyber threats to critical infrastructures. By integrating training programs and psychological manipulation defences, organizations can reduce insider threats. The study could focus on how attackers exploit human vulnerabilities, such as obedience to authority and naivety, and propose frameworks for increasing security awareness and behavioural defences among employees [4].

Multi-Domain Hybrid Threat Models would explore hybrid threats by modelling the interactions between cyber, physical, and human domains, particularly within environments like smart grids and transport systems. The focus would be on predicting and defending against multi-vector attacks by understanding the dependencies between these domains. For example, critical infrastructures like water and energy systems can be modelled for interdependencies, using machine learning and network theory to forecast vulnerabilities and create robust defence mechanisms.

List of used sources:

1. Cheh, C. *Protecting Critical Infrastructure Systems Using Cyber, Physical, and Socio-Technical Models*. — PhD Dissertation, University of Illinois at Urbana-Champaign, 2019. URL: <https://www.ideals.illinois.edu/items/112804>
2. Ghafir I., Saleem J., Hammoudeh M., Faour H., Prenosil V., Jaf S., Jabbar S., & Baker, T. *Security Threats to Critical Infrastructure: The Human Factor*. — *Computers, Materials, & Continua*, 2018, Vol. 74, pp. 4986–5002.
3. Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (Eds.). *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*.-Springer. URL: <https://link.springer.com/book/10.1007/978-3-030-00024-0>
4. Shan, A., & Myeong, S. *Proactive Threat Hunting in Critical Infrastructure Protection through Hybrid Machine Learning Algorithm Application*. — Centre of Security Convergence & e Governance, Inha University, Incheon, Republic of Korea. URL: <https://www.mdpi.com/1424-8220/24/15/4888>

Keywords: hybrid threats, critical infrastructure, cybersecurity, infrastructure protection

Науковій керівник: к.т.н., доц. Задерейко Олександр

ВПЛИВ DIGITAL-СТРАТЕГІЇ НА ПОБУДОВУ ЛОЯЛЬНОСТІ ДО БРЕНДУ

Нігуренко Аміна

студентка 4 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасних умовах швидкого розвитку цифрових технологій і зростаючої конкуренції формування лояльності до бренду є ключовим завданням для компаній. Споживачі постійно оточені великою кількістю інформації, що ускладнює утримання їхньої уваги. Ефективні digital-стратегії стають необхідними для підтримки тривалих відносин зі споживачами, адже вони забезпечують присутність бренду в інтернет-просторі. Однак швидкі зміни в digital-середовищі вимагають адаптації стратегій для створення стійкої лояльності. Це дослідження підкреслює важливість інновацій у цифрових комунікаціях для залучення нових клієнтів і підтримки їхньої довіри в довгостроковій перспективі.

Таким чином, діджитал-маркетинг став незамінним інструментом в арсеналі сучасного просування брендів, насамперед завдяки глибоким змінам у поведінці споживачів та технологічним досягненням у сфері комунікацій [1]. Основна мета діджитал-маркетингу – пов'язати бізнес із його цільовою аудиторією там, де вони проводять значну частину свого часу: в Інтернеті [2].

Наукова спільнота відзначає важливість цифрової трансформації суб'єктів ведення бізнесу в сучасних діджитал-умовах. Цей процес передбачає перехід до цифрового бізнесу, що включає комплексне перетворення діяльності компанії, її процесів, компетенцій та бізнес-моделі. Метою такої трансформації є повне використання можливостей цифрових технологій, що стає основою для успішної адаптації до динамічного ринкового середовища та зростання конкуренції [4].

Діджитал-маркетинг за своєю суттю спрямований на досягнення цілеспрямованої взаємодії з потенційними клієнтами через використання інтерактивних технологій. Однією з основних його переваг є можливість збору та аналізу великих обсягів даних, що дозволяє маркетологам краще розуміти поведінку споживачів, їхні уподобання та поточні ринкові тенденції.

Кінцева мета таких зусиль полягає в тому, щоб вплинути на рішення споживачів, стимулюючи їх до здійснення покупки або іншої бажаної дії. Крім цього, важливим аспектом є встановлення постійної взаємодії з брендом, що підвищує рівень лояльності та сприяє повторним покупкам.

Цей процес детально описано в таблиці 1, яка демонструє ключові інструменти діджитал-маркетингу та їхній вплив на створення лояльності до бренду.

Таблиця 1. Ключові інструменти діджитал-маркетингу

№	Інструменти	Характеристика
1	Соціальні мережі	Платформи, як-от Facebook, Instagram, Twitter, LinkedIn, дозволяють брендам взаємодіяти безпосередньо зі своєю аудиторією. Ці канали ідеальні для створення спільноти навколо бренду, поширення контенту, проведення рекламних кампаній та відстеження споживацьких трендів.
2	Пошукова оптимізація (SEO)	Оптимізація веб-сайту та його контенту для пошукових систем, як-от Google, є критично важливою для забезпечення видимості бренду в інтернеті. SEO допомагає залучити органічний (неоплачуваний) трафік на сайт через ефективне використання ключових слів, якісного контенту та оптимізації структури сайту.
3	Контент-маркетинг	Створення та розповсюдження цінного контенту, який інформує, розважає або освічує аудиторію, є основою для будь-якої ефективної маркетингової стратегії. Це може включати блоги, відео, електронні книги, інфографіку, що допомагає підвищити авторитет бренду і залучити потенційних клієнтів.
4	Електронний маркетинг	Відправка персоналізованих, релевантних інформаційних та рекламних листів потенційним або існуючим клієнтам дозволяє підтримувати постійний зв'язок з аудиторією, збільшувати лояльність і стимулювати продажі.
5	Оплата за клік (PPC) реклама	Це рекламні кампанії, де бренди платять за кожен клік на їхні рекламні оголошення в інтернеті. Популярні платформи для PPC включають Google AdWords та рекламу в соціальних мережах. PPC дозволяє швидко залучити трафік і має високу здатність до точного налаштування цільової аудиторії.

Джерело: особисті спостереження автора

Завдяки інтеграції цих методів компанії здатні адаптуватися до змін споживацьких вимог та ефективно зміцнювати лояльність до свого бренду.

Однією з основних переваг діджитал-маркетингу є можливість збору та аналізу великих обсягів даних, що дозволяє маркетологам краще розуміти поведінку споживачів, їхні уподобання та ринкові тенденції. Використання різноманітних інструментів і платформ сприяє ефективному збору та обробці даних, що, в свою чергу, веде до створення персоналізованих та релевантних маркетингових кампаній. Деякі з найпопулярніших інструментів, які допомагають у зборі та аналізі даних, включають:

1. Google Analytics: надає можливість аналізувати трафік на сайті, поведінку користувачів та їх взаємодію з контентом. Дозволяє відстежувати конверсії, показники залученості та ефективність рекламних кампаній.

2. CRM-системи (Customer Relationship Management): такі як Salesforce, HubSpot або KeyCRM, допомагають зберігати, аналізувати та керувати інформацією про клієнтів, що дозволяє персоналізувати комунікацію та підвищити лояльність.

3. Платформи для аналізу соціальних медіа: інструменти, як Hootsuite або Sprout Social, дозволяють відстежувати згадки про бренд, аналізувати залученість та визначати тенденції в споживчих вподобаннях у соціальних мережах.

Завдяки інтеграції цих методів компанії здатні адаптуватися до змін споживацьких вимог та ефективно зміцнювати лояльність до свого бренду.

Взагалі, діджитал-маркетинг відіграє ключову роль у персоналізації взаємодії з клієнтами, адже сучасні технології дозволяють створювати індивідуалізовані пропозиції, які відповідають потребам і вподобанням споживачів. Завдяки діджитал-технологіям компанії можуть надсилати персоналізовані електронні листи, що враховують історію покупок та інтереси клієнтів, підвищуючи ефективність комунікації.

Технології штучного інтелекту (AI) можуть використовуватися для створення персоналізованих рекомендацій, автоматизуючи процес пропозицій продуктів на основі історії покупок та уподобань клієнтів. Наприклад, Netflix та Amazon використовують алгоритми машинного навчання для формування рекомендаційного контенту. Завдяки цим діджитал-інструментам компанії можуть не лише залучати нових клієнтів, але й зміцнювати довіру та прихильність існуючих споживачів, адаптуючи свої маркетингові стратегії під індивідуальні потреби кожного.

Застосування інноваційних підходів у комунікаціях дозволяє компаніям не лише залучати нових клієнтів, але й формувати емоційні зв'язки з уже існуючими. У таблиці 2 представлені успішні приклади кампаній провідних брендів, які демонструють ефективність діджитал-маркетингу в побудові лояльності до бренду.

Таблиця 2. Успішні приклади кампаній провідних брендів

Компанія	Маркетингова кампанія
Nike	У кампанії "Dream Crazy" Nike зосередилася на надихаючих історіях спортсменів, зокрема Каперніку, що бореться за соціальну справедливість. Кампанія використовувала відео, соціальні мережі та спонсорство, щоб залучити аудиторію та підвищити лояльність до бренду. В результаті кампанії Nike отримала зростання продажів та позитивний відгук від споживачів.
Coca-Cola	Coca-Cola запустила кампанію "Share a Coke", де замінила традиційний логотип на пляшках і банках іменами споживачів. Це сприяло персоналізації продукту, і споживачі почали ділитися фотографіями своїх пляшок у соціальних мережах. Кампанія підвищила продажі і залучила нову аудиторію, а також стала символом того, як діджитал-маркетинг може формувати емоційні зв'язки з брендом.

Dove	Кампанія Dove "Real Beauty" фокусувалася на самооцінці жінок і прийнятті натуральної краси. За допомогою соціальних мереж та відео Dove закликала жінок поділитися своїми історіями. Ця кампанія підвищила обізнаність про бренд і лояльність серед споживачок, сприяючи зростанню продажів.
------	--

Джерело: проаналізовано автором [5,6]

В умовах постійних змін у цифровому середовищі, успішні бренди повинні адаптувати свої стратегії, спираючись на аналіз даних і потреби споживачів, аби залишатися конкурентоспроможними на ринку.

Отже, для досягнення успіху на ринку в умовах зростаючої конкуренції компанії повинні впроваджувати інноваційні підходи у свої digital-стратегії, базуючи їх на аналізі даних і потребах споживачів, щоб забезпечити стійку лояльність до свого бренду.

Список використаної літератури:

1. Капрій Олена Петрівна, Капраль Ольга Растиславівна. Діджитал-маркетинг як ефективний засіб просування бренду. Наукова стаття. Випуск 59, 2024 рік. (дата звернення: 14.10.24);
2. Shanmugam, G., Rajendran, D., Thanarajan, T., Murugaraj, S.S., Rajendran, S. Artificial intelligence as a catalyst in digital marketing: Enhancing profitability and market potential. Ingénierie des Systèmes d'Information, vol. 28, no. 6, pp. 1627–1636. 2023 рік. (дата звернення: 14.10.24);
3. Кобець Дмитро Лейонтійович. Вплив діджиталізації на маркетингові стратегії на ринку B2C. Наукова стаття. Випуск 47, 2023 рік. (дата звернення: 14.10.2024);
4. Бруско І. В., Редчиць М. В. Стратегія цифрової трансформації і цифрова зрілість підприємств як умова забезпечення конкурентоспроможності у XXI столітті. Ефективне управління економікою: інформаційні технології, маркетинг, бізнес. Матеріали Міжнародної науково-практичної конференції. Черкаський державний технологічний університет. Черкаси : ЧДТУ, 2021 рік. С. 21–25. (дата звернення: 14.10.24);
5. Коротенко Оля. Кейс Dove. Електронний ресурс. URL: <http://surl.li/bcpvwk> (дата звернення: 14.10.2024);
6. Share a Coke. Електронний ресурс. URL: <https://vikna.if.ua/cikavo/50027/view> (дата звернення: 14.10.2024).

Ключові слова: діджитал-маркетинг, лояльність до бренду, персоналізація, маркетингові кампанії, комунікація з клієнтами, взаємодія з контентом.

Keywords: digital marketing, brand loyalty, personalization, marketing campaigns, customer communication, content interaction.

Науковій керівник: к.т.н. доц. Задерейко Олександр

УПРАВЛІННЯ РИЗИКАМИ: ПРОЦЕС ТА СТРАТЕГІЇ РЕАГУВАННЯ

Шаповалов Богдан

*студент кафедри безпеки інформаційних технологій
Національного університету «Львівська політехніка»*

Актуальність управління кіберризиками значно зросла у зв'язку з швидким розвитком цифрових технологій, що призвело до збільшення кількості кібератак та загроз для безпеки інформаційних систем компаній.

Згідно з останніми дослідженнями, у джерелі [1] розглядаються методи управління ризиками кібербезпеки, що включають ідентифікацію критичних активів та оцінку потенційних вразливостей, які можуть спричинити значні збитки для організацій. В іншому дослідженні [2] розроблені інноваційні методи аналізу ризиків на основі штучного інтелекту, що дозволяють оперативніше виявляти загрози та підвищувати ефективність кіберзахисту. Крім того, дослідження [3] зосереджується на оцінці рівня ризику для різних секторів та висвітлює важливість адаптації підходів до управління ризиками залежно від галузевих особливостей компанії. Такі напрацювання дозволяють вдосконалити процеси виявлення та реагування на ризики кібербезпеки.

Управління кіберризиками – це процес виявлення, пріоритезації, управління та моніторингу ризиків для інформаційних систем. Ці ризики не можна усунути повністю, але програми управління кіберризиками можуть допомогти зменшити вплив і ймовірність загроз. Компанії використовують процес управління ризиками кібербезпеки, щоб точно визначити свої найкритичніші загрози та вибрати правильні заходи IT-безпеки для захисту інформаційних систем від кібератак та інших цифрових і фізичних загроз на основі своїх бізнес-пріоритетів, IT-інфраструктури та рівня ресурсів. Важко оцінити кіберризики з повною впевненістю. Компанії рідко мають повне уявлення про тактику кіберзлочинців, вразливості власної мережі або більш непередбачувані ризики, такі як суворі погодні умови та недбалість співробітників. Одні й ті ж види кібератак можуть мати різні наслідки для різних компаній [4]. Національний інститут стандартів і технологій (NIST) [5], пропонує підходити до управління кіберризиками як до безперервного, ітеративного процесу, а не як до одноразового заходу. Регулярний перегляд процесу дозволяє компанії впроваджувати нову інформацію та реагувати на нові події в ширшому ландшафті загроз і власних IT-системах. Щоб гарантувати, що рішення щодо ризиків враховують пріоритети та досвід усієї організації, процесом, як правило, керує сукупність зацікавлених сторін. Команди з управління кіберризиками можуть включати директорів, виконавчих керівників, таких як генеральний директор та директор з інформаційної безпеки, членів команди з IT та безпеки, юристів та HR, а також представників інших бізнес-підрозділів.

Розглянемо технологічний ланцюжок управління ризиками (рис. 1) та опишемо кожен з цих кроків детальніше.



Рисунок 1 – Технологічний ланцюжок управління ризиками

1. Формування ризиків. Формулювання ризику – це акт визначення контексту, в якому приймаються ризикові рішення. Формулюючи ризики на самому початку, компанії можуть узгодити свої стратегії управління ризиками із загальними бізнес-стратегіями. Таке вирівнювання допомагає уникнути не-ефективних і дорогих помилок, таких як розгортання елементів керування, які заважають ключовим бізнес-функціям. Щоб сформулювати ризики, компанії визначають такі аспекти: сфера застосування, інвентаризація та пріоритезація активів, організаційні ресурси та пріоритети, законодавчі та нормативні вимоги. Ці та інші міркування дають компанії загальні орієнтири при прийнятті рішень про ризики. Вони також допомагають компанії визначити свою толерантність до ризику, тобто види ризиків, які вона може прийняти, і види, які вона не може.

2. Оцінка ризиків. Компанії проводять оцінку ризиків кібербезпеки для виявлення загроз і вразливостей, оцінки їх потенційного впливу та визначення пріоритетів найкритичніших ризиків. Такий процес залежить від пріоритетів, обсягу та толерантності до ризику компанії.

Загрози — це фактори, що можуть порушити роботу ІТ-систем, викрасити дані або поставити під загрозу інформаційну безпеку. Загрози бувають різними: від навмисних кібератак до випадкових помилок співробітників. Також загрозу можуть становити стихійні лиха, як-от землетруси чи урагани, які здатні пошкодити критичні інформаційні системи.

Вразливості — це слабкі місця в системах, процесах або активах, які можуть бути використані загрозами. Наприклад, неправильне налаштування брандмауера може дати шкідливому програмному забезпеченню доступ до мережі, а помилка в операційній системі — відкрити можливості для дистанційного захоплення пристрою. Слабкі політики доступу також можуть сприяти підвищенню рівня вразливості.

Наслідки — це потенційні збитки, яких може зазнати компанія через реалізацію загроз. Це може включати порушення роботи критично важливих сервісів, втрату доходу, крадіжку чи знищення конфіденційних даних. Наслідки можуть поширюватися і на клієнтів, чиї персональні дані можуть бути викрадені під час витоку інформації.

Оскільки складно кількісно оцінити точний вплив загрози, часто застосовують якісні дані, як-от історичні тенденції або приклади атак на інші організації. Після врахування цих факторів компанія формує профіль ризику, пріоритезуючи ризики за рівнем критичності.

3. Реагування на ризики. За результатами оцінки ризиків компанія визначає, як вона буде реагувати на потенційні ризики. Ризики, які вважаються вкрай малоймовірними, або ризики з незначним впливом, можуть бути прийняті, оскільки інвестування в заходи безпеки може бути дорожчим, ніж сам ризик. Ймовірні ризики та ризики з більш високими наслідками, як правило, будуть враховані.

Зниження ризиків. Пом'якшення наслідків – це використання засобів контролю безпеки, які ускладнюють використання вразливості або мінімізують вплив експлуатації. Приклади включають розміщення системи запобігання вторгнень навколо цінного активу та впровадження планів реагування на інциденти для швидкого виявлення загроз і боротьби з ними.

Усунення ризиків. Виправлення означає повне усунення вразливості, щоб нею не можна було скористатися: виправлення помилки в ПЗ або виведення з експлуатації вразливого активу.

Передача ризиків. Якщо пом'якшення наслідків та їх усунення недоцільні, компанія може перекласти відповідальність за ризик на іншу сторону. Купівля поліса кіберстрахування є найпоширенішим способом передачі ризиків компаніями.

Розподіл ризиків. Коли ризики розподіляються, можливість збитків переходить від індивіда до групи. Корпорація є хорошим прикладом розподілу ризиків – кілька інвесторів об'єднують свій капітал, і кожен несе лише частину ризику того, що підприємство може збанкрутувати.

Прийняття та утримання ризиків. Після того, як були впроваджені всі заходи з розподілу ризиків, передачі ризику та зниження ризику, деякий ризик залишиться, оскільки усунути весь ризик практично неможливо (крім як шляхом уникнення ризику). Це називається залишковим ризиком.

4. Моніторинг ризиків. Організація стежить за своїми новими засобами контролю безпеки, щоб переконатися, що вони працюють належним чином і відповідають відповідним нормативним вимогам. Організація також відстежує ширший ландшафт загроз і власну ІТ-екосистему. Зміни в будь-якому з них – поява нових загроз або додавання нових ІТ-активів – можуть відкрити нові вразливості або зробити застарілими раніше ефективні засоби контролю. Підтримуючи постійне спостереження, компанія може коригувати свою програму кібербезпеки та стратегію управління ризиками майже в режимі реального часу.

В даній роботі розглянуто процес управління кіберризиками, його основні етапи та методи впливу на ризики. Під час дослідження вдалося розробити ефективні підходи до ідентифікації, оцінки та реагування на ризики, що є актуальним для сучасних інформаційних систем. Це дає можливість забезпечити надійний захист компанії від різноманітних загроз, знижуючи ймовірність успішних атак. Напрацювання можуть стати корисними для бізнесів різних масштабів у формуванні надійної стратегії управління кіберризиками.

Список використаних джерел:

1. Heimdal Security. How to Conduct a Cybersecurity Risk Assessment [Електронний ресурс] // Heimdal Security. – Режим доступу: <https://heimdalsecurity.com/blog/cybersecurity-risk-assessment/> – Дата звернення: 03.11.2024.
2. Infosecurity Europe. How to Perform a Cybersecurity Risk Assessment [Електронний ресурс] // Infosecurity Europe. – Режим доступу: <https://www.infosecurityeurope.com/en-gb/blog/guides-checklists/how-to-perform-cybersecurity-risk-assessment.html> – Дата звернення: 03.11.2024.
3. Imperva. Cybersecurity Risk Management [Електронний ресурс] // Imperva. – Режим доступу: <https://www.imperva.com/learn/data-security/cybersecurity-risk-management/> – Дата звернення: 03.11.2024.
4. IBM. What is cyber risk management? [Електронний ресурс] // IBM. – Режим доступу: <https://www.ibm.com/topics/cyber-risk-management> – Дата звернення: 05.11.2024.
5. National Institute of Standards and Technology. Cybersecurity [Електронний ресурс] // National Institute of Standards and Technology. – Режим доступу: <https://www.nist.gov/cybersecurity> – Дата звернення: 05.11.2024.

Ключові слова: кіберризик, управління кіберризиками, реагування на ризики, кібербезпека, загрози.

Keywords: cyber risk, cyber risk management, response to risks, cybersecurity, threats.

Секція 4. НОРМАТИВНО-ПРАВОВІ ЗАСАДИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ГАРМОНІЗАЦІЯ НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА З ЄВРОПЕЙСЬКИМИ СТАНДАРТАМИ У СФЕРІ КІБЕРБЕЗПЕКИ

Ларченко Марина

кандидат юридичних наук, доцент, доцент кафедри кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка»;

доцент кафедри політології, права та філософії Ніжинського державного університету імені Миколи Гоголя

Вступ. Глобалізація та цифровізація суспільства привели до стрімкого зростання кіберзагроз, що створює нові виклики для держав у забезпеченні безпеки інформаційного простору. Європейський Союз (ЄС) активно формує стандарти для боротьби з кіберзагрозами, спрямовані на підвищення стійкості кіберінфраструктури та захист даних. Для країн, які прагнуть інтегруватися в європейський простір, гармонізація національного законодавства з європейськими стандартами у сфері кібербезпеки є стратегічно важливим завданням.

Метою дослідження є аналіз основних європейських стандартів у сфері кібербезпеки, оцінка відповідності національного законодавства цим стандартам та пропозиції практичних кроків для їх гармонізації.

Директива NIS (Network and Information Security Directive) є основоположним документом, що визначає мінімальні вимоги до кібербезпеки для країн-членів ЄС. Її основні цілі: 1) покращення національних стратегій у сфері кібербезпеки; 2) посилення співпраці між державами-членами ЄС; 3) забезпечення безпеки критичної інфраструктури (енергетика, транспорт, охорона здоров'я, фінанси).

У 2022 році було ухвалено NIS 2, яка враховує нові виклики, наприклад, посилення обов'язків операторів важливих послуг та цифрових провайдерів [1].

GDPR (General Data Protection Regulation) є одним із ключових документів у сфері захисту даних, що також має значний вплив на кібербезпеку. Вона встановлює правила щодо обробки персональних даних і накладає значні штрафи за порушення безпеки.

Європейське агентство з кібербезпеки (**ENISA**) сприяє впровадженню європейських стандартів, розробляє рекомендації та організовує навчання для підвищення компетенцій у сфері кіберзахисту.

У той же час, національні правові акти щодо кібербезпеки часто не відповідають європейським стандартам через: 1) відсутність інтегрованого підходу до управління ризиками; 2) недостатній обмін інформацією між державними органами та приватними структурами; 3) низький рівень захисту критичної інфраструктури.

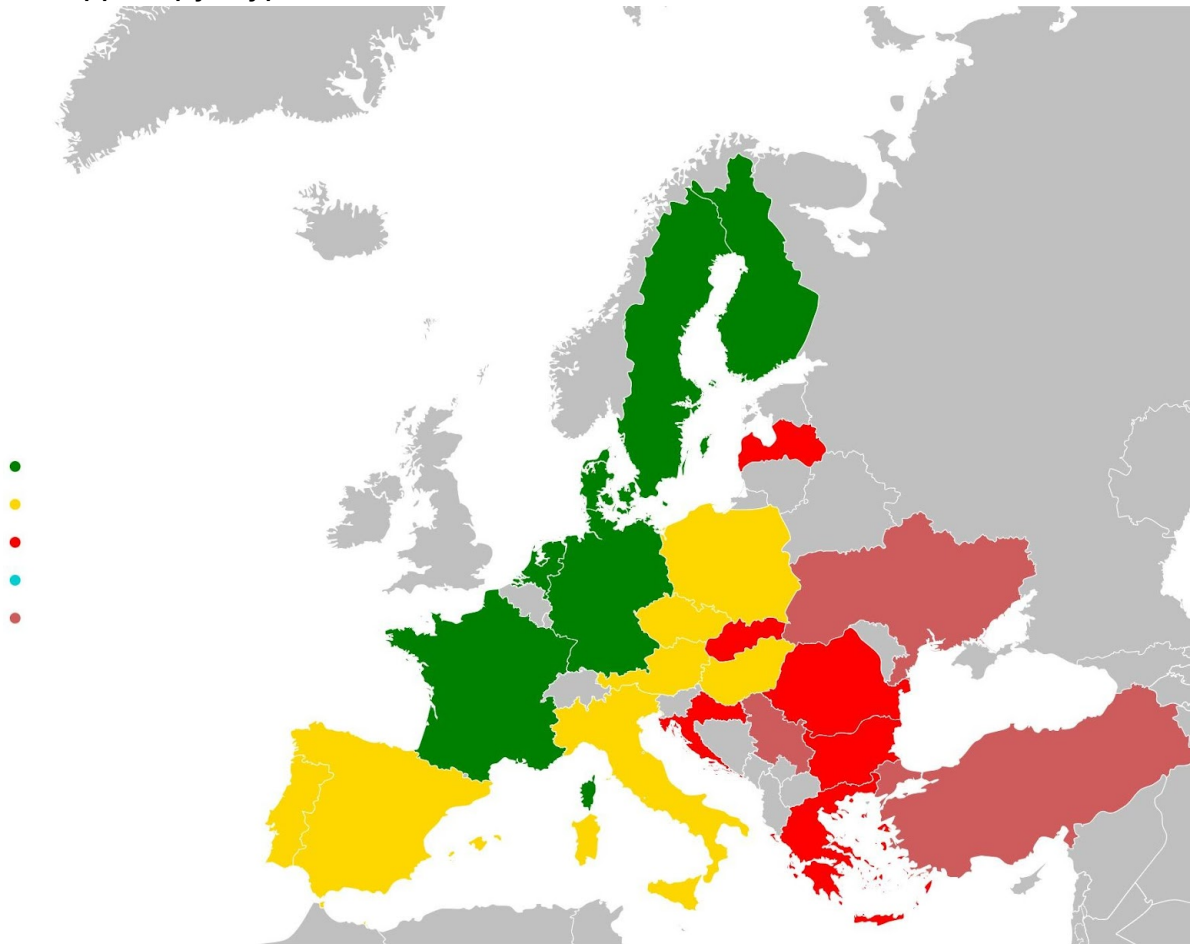


Рисунок 1. Карта кібербезпеки в Європі, яка демонструє рівень імплементації стандартів NIS і GDPR країнами ЄС (на основі публічної інформації).

На рисунку 1 зображено 4 групи країн Європи. Зеленим кольором позначено країни ЄС, які повністю імплементували стандарти NIS і GDPR, мають добре розвинені механізми кібербезпеки та захисту даних; жовтим кольором позначено країни, які впровадили більшість положень стандартів, але ще мають певні недоліки у правовому чи технічному забезпеченні; червоним кольором позначені країни, які знаходяться на початкових етапах адаптації стандартів або мають значні прогалини в їх реалізації; бордовим кольором позначені країни, які не входять до ЄС, але працюють над гармонізацією законодавства для співпраці з ЄС [2].

Чинні українські закони, такі як Закон «Про основні засади забезпечення кібербезпеки України», охоплюють основні аспекти захисту, але потребують розширення в частині міжнародної співпраці та запровадження практик аудиту кібербезпеки.

Вбачається, що в загальних рисах шляхи гармонізації українського законодавства з європейськими стандартами у сфері кібербезпеки можуть бути такими:

1. адаптація Директиви NIS має включати запровадження обов'язкових кібераудитів для критичної інфраструктури та створення ефективної системи моніторингу кіберінцидентів;
2. імплементація норм GDPR має включати розробку національного регламенту із захисту даних, що відповідає вимогам GDPR та навчання фахівців щодо відповідності новим правилам обробки персональних даних;
- 3) впровадження практик обміну інформацією передбачає налагодження співпраці між державними та приватними організаціями через інформаційно-аналітичні центри та участь у міжнародних платформах обміну даними про кіберзагрози [3].

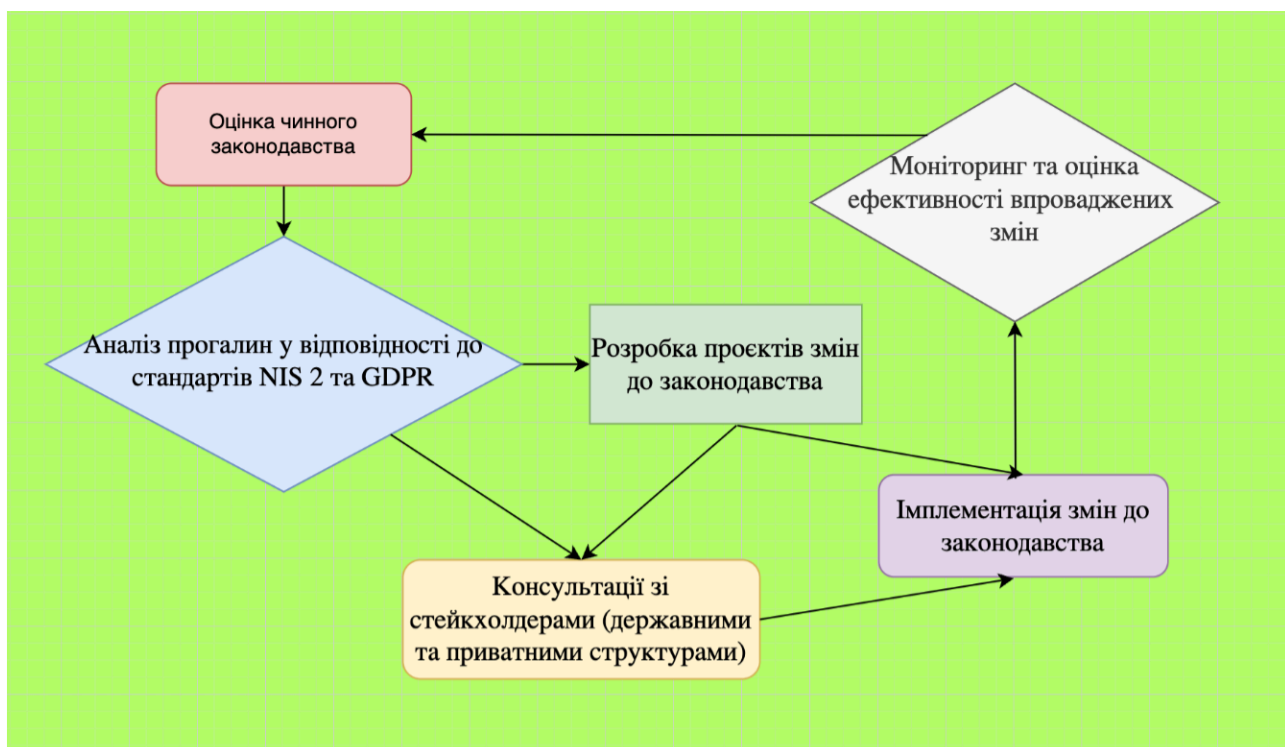


Рисунок 2. Авторська модель гармонізації законодавства – блок-схема з основними етапами адаптації українського законодавства до стандартів NIS 2 і GDPR.

Висновки. Необхідні для гармонізації законодавчі ініціативи передбачають розробку нових законодавчих актів або внесення змін до чинних з урахуванням вимог NIS 2 та GDPR та посилення відповідальності операторів

критичної інфраструктури за недотримання стандартів кібербезпеки. В межах інституційної підтримки необхідним є зміцнення організаційної спроможності державних органів у сфері кібербезпеки та розширення повноважень спеціалізованих установ, таких як CERT-UA. Важливим етапом є впровадження освітніх програм та підвищення професійної кваліфікації певних категорій осіб шляхом проведення тренінгів для державних службовців і представників приватного сектору, а також проведення масштабних національних кампаній для популяризації кібергігієни серед населення.

Гармонізація національного законодавства з європейськими стандартами у сфері кібербезпеки є складним, але необхідним процесом, який дозволить підвищити рівень захисту інформаційного простору. Цей крок сприятиме не лише інтеграції до європейського правового простору, але й зміцненню позицій держави у галузі протидії сучасним кіберзагрозам.

Список джерел

1. ENISA. (n.d.). *The NIS2 Directive: Strengthening Cybersecurity Across the EU*. Retrieved November 18, 2024. URL: <https://www.enisa.europa.eu>
2. European Union. (n.d.). *Cybersecurity Regulation in the European Union: Policies and Implementation*. Retrieved November 18, 2024. URL: <https://www.enisa.europa.eu>
3. ENISA. (n.d.). *EU Cybersecurity Certification Framework: Implications for Member States*. Retrieved November 18, 2024. URL: <https://www.enisa.europa.eu>

Ключові слова: гармонізація законодавства, кібербезпека, європейські стандарти, директива NIS, GDPR, адаптація законодавства, міжнародне співробітництво.

Keywords: harmonization of legislation, cybersecurity, European standards, NIS directive, GDPR, adaptation of legislation, international cooperation.

СИСТЕМНИЙ ПІДХІД ПРИ УПРАВЛІННІ КІБЕРРИЗИКАМИ В УМОВАХ ВІЙНИ

Саврацький Олександр

*аспірант кафедри кібербезпеки Національний університет
«Одеська юридична академія»*

Сучасна війна характеризується не лише збройними зіткненнями, але й масовими кібератаками, що мають на меті порушення роботи об'єктів критичної інфраструктури, дестабілізацію економіки та завдання шкоди соціальній безпеці. У таких умовах забезпечення стійкості інформаційних систем держави, бізнесу та інших інституцій стає стратегічно важливим завданням, виконання якого є неможливим без організованого системного підходу до управління кіберризиками.

Системний підхід до управління кіберризиками передбачає, що всі компоненти кіберзахисту, такі як виявлення, реагування, нейтралізація та від-

новлення, повинні працювати злагоджено і скоординовано. Кожен елемент має бути інтегрованим у єдину структуру, що забезпечує безперервність процесів та готовність до ефективного реагування на кіберінциденти. У межах системного підходу управління ризиками розглядається не як окремий процес, а як цілісна складова стратегічного планування і реалізації загальної безпекової політики [1].

Одним із ключових аспектів системного підходу є оцінка поточного стану кіберзахисту та ідентифікація вразливостей об'єкта. Зазначений процес включає глибокий аналіз архітектури інформаційних систем, оцінку потенційних загроз та вивчення можливих наслідків для економічних, соціальних і військових структур. У контексті війни особливу увагу приділяють аналізу кіберзагроз з боку агресора, що може охоплювати дезінформаційні кампанії, спроби блокування комунікацій та маніпуляції з даними. Оцінка ризиків дає змогу визначити критичні вразливості, які потребують першочергового захисту, а також обирати оптимальні методи протидії [2].

Важливою частиною системного підходу є створення ефективної комунікаційної структури, яка забезпечує обмін інформацією між різними підрозділами, координує зусилля з протидії атакам та забезпечує своєчасне реагування. Зокрема, потрібно розробити централізовану платформу для моніторингу, аналізу та координації дій у реальному часі, що надасть можливість вчасно реагувати на кіберінциденти та мінімізувати їх наслідки.

Управління кіберризиками також включає постійне навчання та підвищення обізнаності співробітників щодо основ інформаційної безпеки. Час війни вимагає особливого рівня готовності, тому всі учасники процесів повинні бути обізнані з можливими загрозами та алгоритмами дій у разі кіберінциденту. Це включає як базову обізнаність про небезпеки фішингу, соціальної інженерії та шкідливого програмного забезпечення, так і конкретні технічні навички для осіб, що безпосередньо працюють з інформаційними системами. Регулярне навчання дозволяє знизити ризики людських помилок, які часто стають одним із факторів успішних атак [3].

Важливим компонентом системного підходу є також тестування кіберзахищеності через проведення контрольних заходів, таких як пенетраційне тестування, симуляції та інші методи, що дозволяють виявити вразливості у захисних механізмах. Проведення таких тестів дає змогу оцінити рівень готовності до можливих атак та ефективність реалізованих заходів захисту. У ході війни такі заходи стають особливо необхідними, оскільки агресор використовує всі можливі засоби для посилення своїх атак і проникнення в інформаційні системи держави чи організацій. Тестування та регулярний аудит захисних систем дозволяють зберігати контроль над ситуацією, виявляти можливі прогалини та оперативно їх усувати.

Крім того, сучасний підхід до управління кіберризиками в умовах війни передбачає активне використання штучного інтелекту та машинного навчання для моніторингу та аналізу потенційних загроз у режимі реального часу. Вказані технології дозволяють швидше виявляти підозрілі активності, аналізувати великі обсяги даних і прогнозувати можливі напрямки розвитку атак. Інтеграція штучного інтелекту у системи кіберзахисту підвищує ефективність та швидкість реагування на кіберінциденти, що особливо важливо у випадках масштабних та скоординованих атак [4].

Отже, системний підхід до управління кіберризиками є необхідною умовою забезпечення стійкості держави перед комплексними кіберзагрозами, які супроводжують сучасні війни. Він інтегрує всі компоненти кіберзахисту, включаючи ідентифікацію вразливостей, моніторинг загроз, постійне навчання персоналу, розробку планів реагування та використання новітніх технологій для швидкого аналізу даних і реагування. Злагоджена робота цих елементів у єдиній системі дозволяє не лише попереджати та нейтралізувати загрози, але й мінімізувати наслідки кібератак, спрямованих на дестабілізацію критичних інфраструктур та порушення соціальної стабільності.

Особливого значення набуває інтеграція кіберзахисту в загальну систему національної безпеки, що передбачає тісну взаємодію державних структур, приватного сектору і громадянського суспільства. Адже системний підхід забезпечує більш комплексний і проактивний захист, що допомагає державі залишатися готовою до потенційних загроз і знижувати вразливість до сучасних видів агресії. Це, в кінцевому підсумку, зміцнює стійкість суспільства перед кіберризиками, захищає стратегічні інтереси та зберігає здатність країни підтримувати економічну, соціальну та військову стабільність навіть в умовах активного збройного протистояння.

Список використаних джерел:

1. Білявська, Ю., Шестак, Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Commodities and markets*. 2022. № 43(3), С. 47-59.
2. Апацький В., Тарасенко І. Проблеми та перспективи страхування кіберризиків в Україні. Проблеми інтеграції освіти, науки та бізнесу в умовах глобалізації: тези доповідей V Міжнародної науково-практичної конференції, 6 жовтня 2023 р. Київ: КНУТД, 2023. С. 86–88.
3. Мазник Л. В., Дзуліт З. П. Управління діяльністю фахівців з кібербезпеки в умовах повномасштабного вторгнення. *Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку*. 2023. № 2 (9). С. 54–65.
4. Задерейко А., Трофименко О., Логінова Н., Прокоп Ю., Кухаренко С. Захист даних користувачів в інформаційних системах. Сучасна спеціальна техніка. 2022. № 1(70). С. 16-30.

Ключові слова: системний підхід, кіберризики, кіберзахист, інфраструктура, моніторинг.

Keywords: systematic approach, cyber risks, cyber defense, infrastructure, monitoring.

АНАЛІЗ НОРМАТИВНО-ПРАВОВИХ АКТІВ ЗАХИСТУ ІНФОРМАЦІЇ У СФЕРІ МЕДІА В УКРАЇНІ

Кухаренко Сергій

*Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат технічних наук, доцент*

Зоз Олена

*Національного університету «Одеська юридична академія»
студентка 1 курсу магістратури факультету кібербезпеки та інформаційних
технологій*

Захист даних і інформації є однією з ключових складових функціонування медіа, особливо в умовах сучасних кіберзагроз і війни в Україні. Інформаційна безпека в медіа включає як захист персональних даних користувачів, так і конфіденційність журналістських джерел, що стає критично важливим для забезпечення чесної та прозорої інформації для суспільства. У даній роботі розглянуто організацію систем захисту даних у медіа-сфері України, актуальні проблеми та можливі напрямки вдосконалення. Також проведено огляд нормативно-правового забезпечення захисту даних у цій галузі, включаючи українські закони та міжнародні стандарти, які регулюють питання безпеки інформації.

В Україні законодавство щодо прозорості захисту даних почало активно розвиватися в період 2020-2022 і цей процес продовжується до тепер. Уряд спільно з громадськими діячами, медіа компаніями розробляють стандарти, які відповідатимуть найкращим світовим практикам щодо захисту інформації і водночас прозорості структур медіа, зокрема, загальноєвропейському регламенту GDPR (General Data Protection Regulation).

Серед найважливіших законодавчих актів у сфері медіа можливо виділити наступні:

1. Закон України «Про інформацію», який визначає загальні правила поводження з інформацією, її доступ, захист, обмеження і відповідальність за розголошення. Важливою частиною цього закону є захист персональних даних, а також зобов'язання журналістів щодо дотримання законних прав громадян на недоторканність їхнього особистого життя.

Згідно з цим законом, заборонено розголошувати особисті дані громадян без їхньої згоди, за винятком випадків, коли це виправдано суспільною необхідністю, наприклад, якщо йдеться про злочинні дії або порушення публічних інтересів. Також закон встановлює обов'язок медіа отримувати згоду від суб'єктів інформації перед публікацією персональних даних, що відповідає європейським стандартам [1].

Порушення цього закону може призвести до адміністративної або кримінальної відповідальності, залежно від характеру і тяжкості порушення.

2. Закон України «Про захист персональних даних» прямо регулює обробку, зберігання та передачу персональних даних, встановлюючи правила, які стосуються збору даних користувачів медіа-платформ та ОТТ (Over-the-top – надання відеопослуг через Інтернет) сервісів. Особлива увага приділяється вимогам до захисту персональних даних, забезпеченню конфіденційності та їхнього безпечного використання [2].

Для медіа компаній та журналістів цей закон важливий у контексті збереження анонімності джерел та захисту приватної інформації під час підготовки та публікації матеріалів. Закон визначає обмеження на передачу персональних даних третім сторонам без згоди суб'єкта даних, а також встановлює механізми контролю за зберіганням таких даних.

За порушення положень цього закону передбачені штрафи, зокрема для юридичних осіб, які можуть досягати значних сум, а також можливість притягнення до кримінальної відповідальності в разі серйозного порушення.

3. Закон України «Про медіа». Закон, прийнятий у грудні 2022 року, спрямований на гармонізацію українського законодавства із європейськими стандартами. Він визначає правові основи діяльності медіа, включно з інтернет-платформами та ОТТ-сервісами, які активно використовують персональні дані користувачів для поширення контенту [3].

Одна з ключових норм закону – це вимога дотримання стандартів захисту персональних даних під час діяльності медіа платформ, включно з тими, що пропонують платформи з потоковим відео. Закон також встановлює права і обов'язки медіа у сфері поширення суспільно важливої інформації, зокрема щодо публікацій, які можуть зачіпати персональні дані публічних осіб.

Закон передбачає як адміністративну, так і кримінальну відповідальність за недотримання вимог щодо захисту даних та прав громадян на конфіденційність.

4. Закон України «Про авторське право і суміжні права». Цей закон стосується більше правовласників контенту, ніж безпосередньо захисту персональних даних, але його положення також впливають на діяльність медіа компаній. Закон регулює захист прав журналістів на їхні матеріали, а також передбачає штрафи та кримінальну відповідальність за плагіат або неправомірне використання інтелектуальної власності [4].

5. Закон України «Про доступ до публічної інформації» регулює права громадян на доступ до публічної інформації, а також захищає інтереси журналістів при отриманні доступу до важливої суспільної інформації. Проте закон також встановлює обмеження щодо розголошення конфіденційних пер-

сональних даних, які можуть бути включені в публічні реєстри або інші державні інформаційні джерела [5].

Закон передбачає дисциплінарну, адміністративну та навіть кримінальну відповідальність за порушення його норм.

6. Цивільний кодекс України (ЦКУ) регулює основні аспекти договірних відносин, включаючи угоди про нерозголошення (NDA). Згідно з ЦКУ, договір може бути укладений для захисту конфіденційної інформації, а сторони договору зобов'язані дотримуватися взятих на себе зобов'язань, включаючи нерозголошення певних даних. Відповідно до статті 525 ЦКУ, порушення умов договору є підставою для застосування санкцій, включаючи відшкодування збитків і стягнення моральної шкоди [6].

Ключова увага приділяється конфіденційній інформації, визначеній у ст. 507 ЦКУ, де зазначається, що сторони договору можуть укласти угоди щодо захисту від розголошення інформації, яка становить комерційну або професійну таємницю. У випадку порушення таких угод сторони можуть вимагати компенсації через суд або за допомогою передбачених договором санкцій.

7. Господарський кодекс України (ГКУ) встановлює правила для регулювання економічних відносин між суб'єктами господарювання, включаючи комерційні угоди з нерозголошення. Стаття 36 ГКУ прямо визначає право суб'єктів господарювання укласти договори про збереження комерційної таємниці. ГКУ також визначає відповідальність за порушення договору, передбачаючи можливість застосування штрафів або інших санкцій за розголошення конфіденційної інформації [7].

8. Загальний регламент захисту даних (GDPR) також має вплив на компанії в Україні, навіть якщо сам регламент стосується країн ЄС. Це важливо для українських медіа та інших компаній, що працюють з даними громадян ЄС, оскільки вони повинні дотримуватися вимог GDPR [8].

Основні положення GDPR, що стосуються України:

1. *Екстериторіальність*: GDPR застосовується не лише до компаній, розташованих в ЄС, а й до тих, які обробляють персональні дані громадян ЄС. Це означає, що українські медіа-платформи, які мають користувачів з Європейського Союзу, повинні дотримуватися вимог регламенту.

2. *Згода на обробку даних*: Українські компанії, які надають послуги громадянам ЄС, повинні отримувати явну згоду користувачів на збір та обробку їхніх даних. Це також стосується OTT-платформ та журналістських видань, що збирають персональні дані для надання послуг або таргетованої реклами.

3. *Права користувачів*: GDPR гарантує права користувачам, такі як право на доступ до своїх даних, їх виправлення, видалення («право бути за-

бутим»), обмеження обробки або передача даних іншим постачальникам послуг. В українських реаліях ці права також повинні бути впроваджені в практику.

4. *Захист даних*: GDPR вимагає впровадження технічних та організаційних заходів для захисту даних користувачів. Це означає, що українські медіа-компанії повинні забезпечувати високий рівень безпеки під час збору та обробки даних, включаючи використання шифрування, політик конфіденційності та інших механізмів захисту.

5. *Відповідальність*: За порушення положень GDPR передбачені серйозні штрафи, які можуть сягати до 20 мільйонів євро або 4% від річного світового обороту компанії. Це мотивує українські компанії впроваджувати належні механізми захисту даних для уникнення санкцій.

GDPR створює підвищену відповідальність для медіа-компаній, що працюють на міжнародному ринку, зобов'язуючи їх адаптувати свої політики щодо захисту даних для відповідності європейським стандартам.

Отже, на нашу думку українське законодавство у сфері захисту інформації та персональних даних в сфері медіа загалом відповідає європейським стандартам, проте залишається багато проблем, пов'язаних із практичною імплементацією цих норм. Зміцнення кібербезпеки в медіа, зокрема у сфері OTT-платформ, стає все більш важливим завданням, особливо в умовах війни.

Список використаних джерел:

1. Закон України «Про інформацію». Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2657-12>
2. Закон України «Про захист персональних даних». Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>
3. Закон України «Про медіа». Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2849-20>
4. Закон України «Про авторське право і суміжні права». Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/3792-12>
5. Закон України «Про доступ до публічної інформації». URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
6. Цивільний кодекс України. URL: <http://surl.li/bmavno>
7. Господарський кодекс України. URL: <http://surl.li/lhqkhn>
8. Європейський Союз. General Data Protection Regulation (GDPR). URL: <https://gdpr-info.eu>

Ключові слова: захист інформації, система захисту даних, інформація, аналіз, медіа, захист персональних даних, кібербезпека.

Key words: information protection, data protection system, information, analysis, media, personal data protection, cyber security.

ЗМІСТ

Секція 1. АЛГОРИТМІЧНІ ТА ТЕХНІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ ...10

АНАЛІЗ СТІЙКОСТУ ПОТОЧНОГО ШИФРУ RC4 10

Щербина Юрій

Казакова Надія

Фразе-Фразенко Олексій

МОДЕЛЬ ВПЛИВУ КІБЕРЗАГРОЗ ТА КІБЕРАТАК НА ВІДНОВЛЕННЯ ФУНКЦІОНАЛЬНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ 12

Бойко Віктор

ВДОСКОНАЛЕННЯ ПРОЦЕСУ ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ 15

Кіх Михайло

Нємкова Олена

QUANTUM PERIOD FINDING AS A THREAT FOR POST-QUANTUM CRYPTOGRAPHIC PRIMITIVES 20

Yevgen Kotukh

АУТЕНТИФІКАЦІЯ ЗА ДОПОМОГОЮ JSON WEB TOKEN 24

Кухаренко Сергій

Овчинников Микола

ВИКОРИСТАННЯ РЕСУРСОМІСТКИХ ПАСТОК ДЛЯ УСКЛАДНЕННЯ АТАКИ НА ВЕБСЕРВЕР 28

Бойко Віктор

Спесівцев Микола

АВТОМАТИЗАЦІЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ З ВИКОРИСТАННЯМ ФРЕЙМВОРКА METASPLOIT 31

Бойко Віктор

Пілявський Владислав

АВТОМАТИЗОВАНИЙ АНАЛІЗ ТРАФІКА ДЛЯ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ 33

Бойко Віктор

Журавський Георгій

ДОСЛІДЖЕННЯ БЕЗПЕКИ ЛОКАЛЬНИХ МЕРЕЖ 38

Бойко Віктор

Верба Костянтин

ВИКОРИСТАННЯ ТЕГІВ ID3V2 ДЛЯ ЗАХИСТУ АВТОРСЬКИХ ПРАВ НА ЗВУКОВІ ФАЙЛИ MP3 41

Овчинников Микола

КОМПЛЕКСНИЙ СИСТЕМНИЙ АНАЛІЗ МЕТОДІВ ЗАХИСТУ ВІД ФІШИНГОВИХ АТАК: ПОЄДНАННЯ ТЕХНІЧНИХ І ОРГАНІЗАЦІЙНИХ ПІДХОДІВ ДЛЯ КОРПОРАТИВНИХ МЕРЕЖ 43

Баланюк Микита

ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА ОСНОВІ КЛІТИННИХ АВТОМАТІВ. 48

Бойко Віктор

Балабан Володимир

USING POLICY AS CODE FOR AUTOMATED SECURITY CONTROL IN KUBERNETES 51

Вахула Олександр

АНАЛІЗ КІБЕРЗАГРОЗ У ХМАРНИХ ОБЧИСЛЕННЯХ: МЕТОДИ ЗАХИСТУ ТА КОН-
ФІДЕНЦІЙНОСТІ ДАНИХ 53

Грезіна Олена

РОЛЬ СУБ'ЄКТИВНИХ ФАКТОРІВ АВТЕНТИФІКАЦІЇ ДЛЯ КІБЕРБЕЗПЕКИ.....55

Голосова Ірина

ІНСТРУМЕНТИ ПРОТИДІЇ КІБЕРЗАГРОЗАМ В ІНДУСТРІЇ КОМП'ЮТЕРНИХ ІГОР....58

Скідан Владислав

ТЕОРЕТИЧНІ СПОСОБИ ПОКРАЩЕННЯ КРИПТОСТІЙКОСТІ ГЕНЕРАТОРІВ ПСЕВ-
ДОВИПАДКОВИХ ЧИСЕЛ 60

Олег Цебак

ВИКОРИСТАННЯ АЛГОРИТМІЧНИХ ТА ТЕХНІЧНИХ АСПЕКТІВ.....63

КІБЕРБЕЗПЕКИ В МЕРЕЖІ ІОТ 63

Підлісний Юрій

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ МЕДИЧНОЇ ДІАГНОСТИКИ 66

ІЗ ЗАСТОСУВАННЯМ НЕЙРОМЕРЕЖ 66

Юзва Анна

Собчук Валентин

Біляєв Дмитро

ПРОБЛЕМА ЗАХИСТУ МЕРЕЖЕВИХ МАРШРУТИЗАТОРІВ 69

Овсянко Дмитро

ЗАХИСТ ВІД ЗОВНІШНІХ ТА ВНУТРІШНІХ КІБЕРЗАГРОЗ.....73

Олександр Колесніков

АНАЛІЗ СУЧАСНИХ ТРЕНДІВ АТАК АРТ-ГРУП 76

Опанович Максим

ЕМУЛЯЦІЯ DOS/DDOS АТАК В ІНФОРМАЦІЙНИХ СИСТЕМАХ.....79

Кузьменко Денис

ПРОЕКТУВАННЯ ЗАСОБУ ПЕРЕДАЧІ ПРИХОВАНИХ ПОВІДОМЛЕНЬ ЗА ДОПОМО-
ГОЮ DNS-ТУНЕЛЮВАННЯ 82

Павлюк Олександр - Юрій

Нечипор Степан

ПЕРЕВАГИ І НЕДОЛІКИ ХМАРНИХ СХОВИЩ ДЛЯ КЕРУВАННЯ ПАРОЛЯМИ ICLOUD ТА CHROME.....	85
---	----

В'ячеслав Бевза

ПЕРСПЕКТИВИ ТА ВІДКРИТІ ПРОБЛЕМИ ЗАСТОСУВАННЯ.....	88
--	----

ПЕРЕТВОРЕННЯ УОЛША-АДАМАРА ДЛЯ ПОБУДОВИ АЛГОРИТМІВ СТИСКУ ГРАФІЧНОЇ ІНФОРМАЦІЇ.....	88
---	----

Соколов Артем

Хусід Натан

АНАЛІЗ ВРАЗЛИВОСТЕЙ КОРПОРАТИВНОЇ МЕРЕЖІ В УМОВАХ НЕСАНКЦІОНОВАНОГО ФІЗИЧНОГО ДОСТУПУ.....	91
--	----

Іващук Даніель

ТЕОРЕТИЧНІ ЗАСАДИ ЗНАХОДЖЕННЯ ПРИХОВАНОВОГО КАНАЛУ ЗВ'ЯЗКУ В ОБЛАСТІ ПЕРЕТВОРЕНЬ УОЛША-АДАМАРА	93
--	----

Соколов Артем

Лановська Олександра

АВТОМАТИЗАЦІЯ ТЕСТУВАННЯ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	97
---	----

Максимович Максим

BYOD (BRING YOUR OWN DEVICE) RISK: A GROWING CONCERN IN CONFLICT ZONES – UKRAINE'S CASE	100
---	-----

Олена Зоз

СИСТЕМА АВТОМАТИЧНОГО ЗБОРУ ДАНИХ НА ОСНОВІ ЗАПИТІВ МОБІЛЬНИХ ПРИСТРОЇВ	102
---	-----

Оліярчук Тарас

ЗАХИСТ KUBERNETES ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО СЕКРЕТНИХ ДАНИХ ЗА ДОПОМОГОЮ ШИФРУВАННЯ.....	105
---	-----

Дарієнко Дмитро

МОДЕЛЮВАННЯ ТА РЕАЛІЗАЦІЯ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ....	107
---	-----

Савранчук Владислава

Секція 2. ШТУЧНИЙ ІНТЕЛЕКТ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЗАДАЧАХ КІБЕРБЕЗПЕКИ.....	110
--	------------

РИЗИКИ ВИКОРИСТАННЯ ГРАФІЧНОГО КОНТЕНТУ, СТВОРЕНОГО ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ	110
---	-----

Логінова Наталія

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В РОБОТІ СИСТЕМНОГО АНАЛІТИКА	112
---	-----

Трофименко Олена

Стрілець Михайло

АПАРАТНИЙ ЗАХИСТ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ NGFW МЕРЕЖЕВИХ ЕКРАНІВ.....	115
--	-----

Задерейко Олександр

ШТУЧНИЙ ІНТЕЛЕКТ У КІБЕРБЕЗПЕЦІ ЕНЕРГЕТИЧНИХ СИСТЕМ	118
<i>Куклінова Тетяна</i>	
СИСТЕМИ АВТОРИЗАЦІЇ ТА АВТЕНТИФІКАЦІЇ ЯК ОСНОВА	122
ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ.....	122
<i>Головашич Сергій</i>	
<i>Половінкін Миколай</i>	
<i>Ровда Володимир</i>	
ЗАХИСТ ЧУТЛИВОЇ ІНФОРМАЦІЇ ОРГАНІЗАЦІЇ ПРИ ВИКОРИСТАННІ ХМАРНИХ СЕРВІСІВ	124
<i>Чепурна Олена</i>	
<i>Литвин Олександра</i>	
ПОШУК ВЕЛИКИХ ПРОСТИХ ЧИСЕЛ ПЕРЕВІРКОЮ ЗА ТЕСТОМ ФЕРМА НА ПЛАТ- ФОРМІ CUDA.....	127
<i>Чикунів Павло</i>	
<i>Ковальський Олександр</i>	
ГЕНЕРАТИВНИЙ ШТУЧНИЙ ІНТЕЛЕКТ В GAMEDEV	130
<i>Трофименко Олена</i>	
<i>Бондаренко Максим</i>	
MESHU AI ЯК АЛЬТЕРНАТИВА ПРОГРАМАМ 3D МОДЕЛЮВАННЯ	132
<i>Толокнов Анатолій</i>	
<i>Шляхтицький Дмитро</i>	
РОЗРОБКА ІНТЕРАКТИВНИХ СИСТЕМ НА ОСНОВІ ШТУЧНОГО	134
ІНТЕЛЕКТУ	134
<i>Мільченко Олександр</i>	
ПРИНЦИПИ АНАЛІЗАТОРА ПЕРЕНАПРАВЛЕННЯ DON-ТРАФІКУ	137
<i>Федчук Тарас</i>	
ВБУДОВАНІ РУШІЇ 3D МОДЕЛЮВАННЯ ЯК ЗАМІНА ПОВНИХ.....	141
ПРОГРАМ ДЛЯ МОДЕЛЮВАННЯ.....	141
<i>Толокнов Анатолій</i>	
<i>Бондарева Анна</i>	
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ЗАДАЧАХ ПРОТИДІЇ	144
КІБЕРТЕРОРИЗМУ	144
<i>Кухаренко Сергій</i>	
<i>Стрілець Михайло</i>	
ОРГАНІЗАЦІЯ ТА РОЗГОРТАННЯ СИСТЕМИ РЕЗЕРВНОГО	147
КОПІЮВАННЯ З ВИКОРИСТАННЯМ BORG.....	147
<i>Бойко Віктор</i>	
<i>Хорус Олександр</i>	

РОЗРОБКА ПРОГРАМНОЇ СИСТЕМИ З ЕЛЕМЕНТАМИ ШІ ДЛЯ ОЦІНКИ НАСТРОЇВ ТА ПОВЕДІНКИ КОРИСТУВАЧІВ ТА ВИЯВЛЕННЯ БОТ-АКТИВНОСТІ.....	151
<i>Ольвінська Аліна</i>	
<i>Петрова Марія</i>	
<i>Лойшин Максим</i>	
ЗАСТОСУВАННЯ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ.....	154
ДЛЯ КОМП'ЮТЕРНОГО ЗОРУ.....	154
<i>Артем Ткачук</i>	
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ ІН- ФОРМАЦІЙНИХ МОДЕЛЕЙ СКЛАДНИХ СИСТЕМ.....	156
<i>Куклінова Софія</i>	
ІНТЕГРАЦІЯ СУЧАСНИХ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ	160
В МОБІЛЬНИХ ЗАСТОСУНКАХ ДЛЯ ВІРТУАЛЬНИХ КОНСУЛЬТАЦІЙ	160
<i>Брума Крістіна</i>	
ІНФОРМАЦІЙНА СИСТЕМА ВИКОРИСТАННЯ НЕЙРОМЕРЕЖЕВОГО ПІДХОДУ ДЛЯ ВИРІШЕННЯ ЗАВДАННЯ ПРОГНОЗУВАННЯ ЗМІСТУ ЦИФРОВИХ ЗОБРАЖЕНЬ...	166
<i>Бондаренко Сергій</i>	
МЕТОДИ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ ДЛЯ ЗАХИСТУ ВІД КІБЕРАТАК.....	168
<i>Вавілов Микита</i>	
АНАЛІЗ ВИТОКІВ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ СИСТЕМ	173
<i>Власенко Даніїл</i>	
СТВОРЕННЯ МОБІЛЬНОГО ЗАСТОСУНКУ ДЛЯ ПОШУКУ ВОДІЇВ ТА ПОПУТНИКІВ. АНАЛІЗ КОНКУРЕНТІВ	176
<i>Косяк Микола</i>	
АНАЛІЗ СУЧАСНИХ ЗАСОБІВ РЕБ ЯК ІНСТРУМЕНТІВ ПОРУШЕННЯ КІБЕРБЕЗПЕКИ 182	
<i>Бибик Роман</i>	
ЗАСТОСУВАННЯ АЛГОРИТМУ МАШИННОГО НАВЧАННЯ ISOLATION FOREST ДЛЯ ВИЯВЛЕННЯ АНОМАЛЬНИХ ДІЙ КОРИСТУВАЧІВ.....	187
<i>Лабур Ярослав</i>	
ВИКОРИСТАННЯ МЕРЕЖЕВОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ ПРИХОВАНИХ ЗАКО- НОМІРНОСТЕЙ У ВЕЛИКИХ ДАНИХ.....	190
<i>Савенко Михайло</i>	
ВИКОРИСТАННЯ PYTHON ДЛЯ АНОНІМІЗАЦІЇ ВЕБ-ЗАПИТІВ.....	195
<i>Москаленко Олексій</i>	
КІБЕРБЕЗПЕКА АВТОНОМНИХ ДРОНІВ: ЗАХИСТ ВІД АТАК.....	197
НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ	197
<i>Новосельський Дмитро</i>	

РОЗГЛЯД ТЕХНОЛОГІЙ BIG DATA ЯК ІНСТРУМЕНТУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОБОТИ ПІДПРИЄМСТВ РОЗДРІБНОЇ ТОРГІВЛІ.....	200
--	-----

Осадчук Анастасія

ШТУЧНИЙ ІНТЕЛЕКТ У ВИЯВЛЕННІ КІБЕРЗАГРОЗ ТА РЕАГУВАННІ НА НИХ.....	203
--	-----

Струк Данило

ЕФЕКТИВНІСТЬ ВИКОРИСТАННЯ TYPESCRIPT У ВЕЛИКИХ.....	205
---	-----

ПРОЄКТАХ.....	205
---------------	-----

Шагалін Кіріл

ЕЛЕКТРОННІ СИСТЕМИ ВВЕДЕННЯ ЗАПИСІВ (ELD) РОБОЧОГО ДНЯ ВОДІЯ ВАНТАЖНОГО ТРАНСПОРТУ	210
--	-----

Питомець Ярослав

TACKLING SHADOW IT AND RISK ANALYSIS IN PUBLIC CLOUD INFRASTRUCTURE	212
---	-----

Марценюк Євгеній

МЕТОДИ ОПТИМІЗАЦІЇ ПРОДУКТИВНОСТІ ДЕЦЕНТРАЛІЗОВАНИХ БАЗ ДАНИХ НА ОСНОВІ БЛОКЧЕЙН-ТЕХНОЛОГІЇ.....	215
--	-----

Петрів Петро

Секція 3. УПРАВЛІНСЬКІ, СОЦІАЛЬНІ ТА ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ 217

ОПТИМІЗАЦІЯ ПІДХОДІВ ДО ЦІНОУТВОРЕННЯ НА ПОСЛУГИ	217
--	-----

КІБЕРБЕЗПЕКИ.....	217
-------------------	-----

Горбаченко Станіслав

Разінкін Нікіта

УПРАВЛІНСЬКІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ.....	220
---	-----

В'юник Ольга

АНАЛІЗ НАСТРОЇВ ЯК ОДИН ІЗ АСПЕКТІВ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ.....	222
---	-----

Синенко Марина

Зотєєв Станіслав

ОФІСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ ВІЗУАЛІЗАЦІЇ МАРКЕТИНГОВИХ ДАНИХ..	225
---	-----

Лобода Юлія

СУЧАСНІ ВИКЛИКИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ІТ-КОМПАНІЯХ.....	227
---	-----

Немченко Тетяна

Рудь Ростислав

АКТУАЛЬНІ ІНСТРУМЕНТИ ДЛЯ ІННОВАЦІЙНОГО РОЗВИТКУ	230
--	-----

Пунченко Наталія

МЕТОДИ АНАЛІЗУ ТА ЗАХИСТУ ВІД КІБЕРАТАК. МЕТОДИ АНАЛІЗУ ПОВЕДІНКИ КІБЕРЗЛОЧИНЦЯ.....	233
<i>Бойко Віктор</i>	
<i>Ніякий Олександр</i>	
КІБЕРЗАХИСТ ЯК ІНСТРУМЕНТ СУЧАСНОГО РИЗИК-МЕНЕДЖМЕНТУ.....	235
<i>Кірович Андрій</i>	
ВПЛИВ КІБЕРЗАГРОЗ НА ЕФЕКТИВНІСТЬ ЛОГІСТИЧНОЇ ДІЯЛЬНОСТІ.....	239
<i>Фомичев Дмитро</i>	
ІННОВАЦІЙНІ ПІДХОДИ ДО КОНТРОЛЮ ДОСТУПУ ДО ІНФОРМАЦІЇ ДЛЯ ПЕРСОНАЛУ З ВИКОРИСТАННЯМ БЛОКЧЕЙН-ТЕХНОЛОГІЙ	242
<i>Ямнич Андрій</i>	
ПОСИЛЕННЯ ЗАХОДІВ БЕЗПЕКИ ПРОТИ ЦИФРОВИХ ЗАГРОЗ У ТРАНСКОРДОННИХ ФІНАНСОВИХ СИСТЕМАХ.....	246
<i>Гуренко Марк</i>	
ВИКОРИСТАННЯ CRM ДЛЯ ЗБІЛЬШЕННЯ ОБСЯГІВ ПРОДАЖІВ	250
<i>Дем'янова Тетяна</i>	
ІНФОРМАЦІЙНИЙ ПРОСТІР УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ	253
<i>Дробишевська Вікторія</i>	
ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В БАНКІВСЬКІЙ СФЕРІ.....	256
<i>Закірко Юрій</i>	
КІБЕРБЕЗПЕКА, ЯК НЕОБХІДНА СКЛАДОВА МАРКЕТИНГОВИХ	258
ІНСТРУМЕНТІВ	258
<i>Кошева Катерина</i>	
THE IMPACT OF HYBRID THREATS ON THE CYBER SECURITY OF CRITICAL INFRASTRUCTURE IN THE CONTEXT OF MODERN GLOBAL CHALLENGES	261
<i>Page Nikita</i>	
ВПЛИВ DIGITAL-СТРАТЕГІЇ НА ПОБУДОВУ ЛОЯЛЬНОСТІ ДО БРЕНДУ	263
<i>Нігуренко Аміна</i>	
УПРАВЛІННЯ РИЗИКАМИ: ПРОЦЕС ТА СТРАТЕГІЇ РЕАГУВАННЯ	267
<i>Шаповалов Богдан</i>	
Секція 4. НОРМАТИВНО-ПРАВОВІ ЗАСАДИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ	271
ГАРМОНІЗАЦІЯ НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА З ЄВРОПЕЙСЬКИМИ СТАНДАРТАМИ У СФЕРІ КІБЕРБЕЗПЕКИ	271
<i>Ларченко Марина</i>	
СИСТЕМНИЙ ПІДХІД ПРИ УПРАВЛІННІ КІБЕРРИЗИКАМИ В УМОВАХ ВІЙНИ.....	274
<i>Саврацький Олександр</i>	

АНАЛІЗ НОРМАТИВНО-ПРАВОВИХ АКТІВ ЗАХИСТУ ІНФОРМАЦІЇ У СФЕРІ МЕДІА В УКРАЇНІ	277
---	-----

Кухаренко Сергій

Зоз Олена

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ ТА ПРАКТИКА

**МАТЕРІАЛИ
V МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ**

*22 листопада 2024 року
м. Одеса*

Відповідальній редактор: О.В. Дикий

Дизайн та верстка:
М.Ю. Овчинников



**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»**

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МАТЕРІАЛИ V МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

**КІБЕРБЕЗПЕКА
В СУЧАСНОМУ СВІТІ:
АКТУАЛЬНІ ВИКЛИКИ
ТА ПРАКТИКА**

22 листопада 2024 року, м. Одеса