НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
ІМ. М.Є. ЖУКОВСЬКОГО
„ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"
Кафедра комп'ютерних систем, мереж і кібербезпеки

СТУДЕНТСЬКА КОНФЕРЕНЦІЯ ІНФОРМАЦІЙНА, ФУНКЦІЙНА І КІБЕРБЕЗПЕКА

СКІФіК

Матеріали четвертої
науково-технічної конференції

29 - 30 листопада 2024 року

ХАРКІВ - 2024

НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ ІМ. М.Є. ЖУКОВСЬКОГО "ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"

Кафедра комп'ютерних систем, мереж і кібербезпеки

СТУДЕНТСЬКА КОНФЕРЕНЦІЯ ІНФОРМАЦІЙНА, ФУНКЦІЙНА і КІБЕРБЕЗПЕКА

СКІФіК

Матеріали четвертої
науково-технічної конференції
29 – 30 листопада 2024 року

Харків 2024

УДК 004.056
С 88

У збірнику подано тези доповідей четвертої науково-технічної студентської конференції «Студентська Конференція Інформаційна, Функційна і Кібербезпека». Розглянуті питання за такими напрямами: інформаційна безпека; функційна безпека; кібербезпека; системи симетричного та асиметричного шифрування, системи захисту інформації для веб та мобільних додатків, методи атак та захисту за допомогою штучного інтелекту, смарт-системи, інтернет речей та автономні системи. Конференція поділена на дві секції: інформаційна безпека; функційна безпека.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

С 88 Студентська конференція інформаційна, функційна і кібербезпека СКІФіК: матеріали четвертої науково-технічної конференції 29-30 листопада 2024 року. – Харків: ФОП Бровін О.В., 2024. – 174 с.
ISBN 978-617-8238-78-0

ПЛАН ПЕРШОГО ДНЯ КОНФЕРЕНЦІЇ

<table>
<tr><td colspan="3">29 листопада 2024 року, Час: 15:00 – 19:00, онлайн</td></tr>
<tr><td>15:00
–
15:10</td><td colspan="2">Вітальне слово</td></tr>
<tr><td>15:10
–
15:15</td><td colspan="2">Вітальне слово спонсора конференції «Харківський IT Кластер»</td></tr>
<tr><td>15:15
–
15:35</td><td colspan="2">Speech by a master’s student from the Hellenic Military Academy, Greece
Pavlos Konstantinidis
Topic: SMAD: A Real Time Network Attack Detector.</td></tr>
<tr><td>15:35
–
15:55</td><td colspan="2">Виступ магістранта кафедри 503, НАУ «ХАІ», Україна; Fullstack-розробник
Лісних Олександр Ігорович
Тема: Аналіз вразливостей OWASP TOP 10 та захист за допомогою брендмауеру.</td></tr>
<tr><td>15:55
–
16:00</td><td colspan="2">Перерва</td></tr>
<tr><td rowspan="3">16:00
–
18:45</td><td>Секція 1</td><td>Секція 2</td></tr>
<tr><td>Інформаційна безпека</td><td>Функційна безпека</td></tr>
<tr><td>https://meet.google.com/xwr-mxbv-dpc</td><td>https://meet.google.com/afr-deqo-ghv</td></tr>
<tr><td>18:45
–
19:00</td><td colspan="2">Обговорення результатів роботи секцій</td></tr>
</table>

ПЛАН ДРУГОГО ДНЯ КОНФЕРЕНЦІЇ

<table>
<tr><td colspan="3">30 листопада 2024 року, Час: 10:00 – 14:00, онлайн</td></tr>
<tr><td>10:00
–
10:05</td><td colspan="2">Оголошення Оргкомітету</td></tr>
<tr><td>10:05
–
10:10</td><td colspan="2">Вітальне слово спонсора конференції НВП «Радій»</td></tr>
<tr><td>10:10
–
10:30</td><td colspan="2">Speech by researcher from the Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, Bulgaria
Yulian Hristov
Topic: Future Media Challenges in the Age of AI.</td></tr>
<tr><td>10:30
–
10:50</td><td colspan="2">Виступ аспіранта кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», Україна; CIO в NewtonPromservice
Демура Руслан Іванович
Тема: Using zero trust technologies to protect UAVs in the modern cyberspace environment.</td></tr>
<tr><td>10:50
–
10:55</td><td colspan="2">Перерва</td></tr>
<tr><td rowspan="3">10:55
–
13:30</td><td>Секція 1</td><td>Секція 2</td></tr>
<tr><td>Інформаційна безпека</td><td>Функційна безпека</td></tr>
<tr><td>https://meet.google.com/xwr-mxbv-dpc</td><td>https://meet.google.com/afr-deqo-ghv</td></tr>
<tr><td>13:30
–
13:45</td><td colspan="2">Перерва</td></tr>
<tr><td>13:45
–
14:00</td><td colspan="2">Підсумкове пленарне засідання</td></tr>
</table>

ПРОГРАМА КОНФЕРЕНЦІЇ

29 – 30 листопада 2024 року, Онлайн формат

Відкриття конференції, привітання учасників організаторами конференції та запрошеними гостями

Пленарні доповіді:

Speech by a master's student from the Hellenic Military Academy, Greece; **Pavlos Konstantinidis**. Topic: «SMAD: A Real Time Network Attack Detector».

Магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ»; **Лісних Олександр Ігорович**. Тема доповіді: «Аналіз вразливостей OWASP TOP TEN та захист за допомогою брендмауеру».

Speech by researcher from the Institute of Information and Communication Technologies, Bulgarian Academy of Sciences; **Yulian Hristov**. Topic: «Future Media Challenges in the Age of AI».

Аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ»; **Демура Руслан Іванович**. Тема доповіді: «Using zero trust technologies to protect UAVs in the modern cyberspace environment».

РОБОТА СЕКЦІЙ

Секція 1. Інформаційна безпека
Посилання: https://meet.google.com/xwr-mxbv-dpc
Модератор: Юдін Олесь Вікторович
Спів модератори: Герасимюк Дар'я Вікторівна

Секція 2. Функційна безпека
Посилання: https://meet.google.com/afr-deqo-ghv
Модератор: Землянко Георгій Андрійович
Спів модератор: Федоренко Дар'я Дмитрівна

ТЕЗИ ДОПОВІДЕЙ

Секція 1. Інформаційна безпека

Секція 1

АНАЛІЗ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ ШІ ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В СИСТЕМАХ КІБЕРЗАХИСТУ

Ахтирська С.В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Землянко. Г. А.

Актуальність. Стрімкий розвиток сучасних інформаційних технологій призвів до зростання кількості, складності та швидкості здійснення кібератак, що ускладнює їхнє ефективне виявлення та реагування за допомогою лише людських ресурсів. Крім того, слід зазначити, що людський фактор є частим джерелом вразливості в системах кібербезпеки, що робить ці системи менш стійкими до атак. Близько 74% кібер інцидентів мають людський елемент (помилки співробітників та користувачів програмним забезпеченням). Використання штучного інтелекту (ШІ) для автоматичного виявлення вразливостей відкриває нові можливості, дозволяючи системам швидко реагувати на потенційні загрози через глибокий аналіз даних і виявлення слабких місць [1, 2].

Метою даної роботи є аналіз можливого використання ШІ для виявлення вразливостей у системах кіберзахисту.

Основні положення. Інструменти кібербезпеки з використанням ШІ можуть бути використані для аналізу великих наборів даних, щоб ідентифікувати аномальну поведінку після виявлення закономірностей в поведінці користувачів, забезпечення безпеки в хмарі, у системах керування ідентичністю та доступом (IAM), при розслідуванні кібер інцидентів та реагуванні на них [3]. Після виявлення підозрілої активності ШІ може надіслати відповідне сповіщення фахівцю з безпеки, таким чином спрощуючи завдання співробітникам і залишаючи прийняття остаточного рішення за людиною [4].

Проте, крім користі від ШІ, існують також певні ризики, такі як: витоки даних, помилкові спрацьовування, пропущені атаки та труднощі з інтерпретацією виявлених аномалій. Проте, завдяки алгоритмам машинного навчання, здатності ШІ адаптуватися до змін та навчатися на раніше виявлених незвичайних активностях, можна знизити ризики

впровадження технологій ШІ у системи захисту. Саме тому тренування ШІ та якість вхідних даних, які використовувались, має критично важливе значення для його подальшого коректного та ефективного функціонування [4, 5].

Висновки. Основні переваги безпеки з використанням ШІ полягає в здатності швидко виявляти вразливості, аналізуючи мережевий трафік, також у знаходженні прогалин в безпеці, які людина може пропустити. Продумане використання засобів ШІ, коректно проведене навчання та регулярне оновлення моделей ШІ допоможуть мінімізувати згадані ризики від впровадження технології та ефективніше виконувати завдання, при цьому залишаючи остаточне рішення за людиною.

Список літератури

1. AI in cybersecurity: use cases, implementation, solution and development. *LeewayHertz*. URL – https://www.leewayhertz.com/ai-in-cybersecurity (дата звернення: 28.10.2024).
2. 74% data breaches are due to human error | infosec. *Cybersecurity Training*. URL – https://www.infosecinstitute.com/resources/security-awareness/human-error-responsible-data-breaches (дата звернення: 04.11.2024).
3. Kaur R., Gabrijelčič D., Klobučar T. Artificial intelligence for cybersecurity: literature review and future research directions. Information fusion. 2023. Volume 97. DOI: https://doi.org/10.1016/j.inffus.2023.101804.
4. Що таке ШІ для кібербезпеки? *Microsoft*. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-ai-for-cybersecurity#heading-ocafd6 (дата звернення: 28.10.2024).
5. Managing cybersecurity and privacy risks in the age of artificial intelligence: launching a new program at NIST. *NIST*. URL: https://www.nist.gov/blogs/cybersecurity-insights/managing-cybersecurity-and-privacy-risks-age-artificial-intelligence (дата звернення: 03.11.2024).

Відомості про авторів

Ахтирська Софія Вячеславівна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», s.v.akhtyrska@student.csn.khai.edu
Землянко Георгій Андрійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», PhD з кібербезпеки, g.zemlynko@khai.edu

Секція 1

НАДІЙНІСТЬ СУЧАСНИХ МЕТОДІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Баклицька А. Р.
Національний університет «Запорізька політехніка»
Науковий керівник: Зайко Т. А.

Актуальність. Однією з актуальних задач розвитку інформаційних технологій на сучасному етапі є забезпечення надійного захисту інформації. Ідентифікація дозволяє суб'єкту назвати себе. Сучасний рівень розвитку комп'ютерних технологій дозволяє використовувати унікальність біометричних ознак, як основу для ідентифікації особи та надання їй доступу. Великою проблемою у сучасних комп'ютерних системах є несанкціонований доступ. Тож, вміння методів протистояти підробкам та захист біометричних даних особи відіграє важливу роль для надійності сучасних методів біометричної ідентифікації [1].

Метою даної роботи є дослідження надійності сучасних систем біометричної ідентифікації.

Біологічні ознаки є унікальними, тому їх компрометація може стати фатальною унеможливлюючи змінити біологічні шаблони для захисту доступу. Окрім цього, алгоритми можуть натрапити на спроби сфабрикувати біологічні ознаки за допомогою засобів мультимедіа.

Основні положення. Сучасні методи біометричної ідентифікації забезпечують зручність і безпеку в різних сферах, але потребують ефективного захисту від зловмисників. Liveness Detection перевіряє автентичність біометричних зразків, зменшуючи ризик підробок, тоді як біометрія, яку можна скасувати, дозволяє уникати компрометації через зміну зразків [2]. Зберігання даних у локальних захищених середовищах, як Secure Enclave чи TEE, забезпечує ізоляцію та шифрування. Мультимодальні системи підвищують точність і надійність, поєднуючи кілька біометричних методів, а гомоморфне шифрування дозволяє працювати із зашифрованими даними, зберігаючи їхню конфіденційність навіть у разі зламу. Методи які використовується для виявлення спроби підробки шляхом визначення того, чи є джерело біометричного зразка живою людиною чи фальшивим зображенням. Рішення Active Liveness насамперед шукають ознаки життя. Вони спонукають користувача виконати дію, яку неможливо легко відтворити за допомогою підробки. Вони також можуть включати кілька модальностей, наприклад аналіз

натискання клавіш або розпізнавання мовця. Пасивні алгоритми живучості в основному шукають ознаки підробки, але також можуть пасивно шукати ознаки життя. Окрім, аналізу руху алгоритми аналізують визначення глибини та аналіз текстур, досліджуючи деталі шкіри чи відбитків пальців. Виявлення Liveness гарантує, що збираються лише справжні біометричні дані, необхідні для ідентифікації, зменшуючи ризик порушення конфіденційності через використання несанкціонованих матеріалів або зображень.

Висновки. Методи захисту біометричних даних постійно вдосконалюються, забезпечуючи як зручність користування, так і високий рівень безпеки. Інтеграція таких технологій, як гомоморфне шифрування, локальне зберігання, мультимодальні системи й алгоритми живучості, мінімізує ризики підробок і витоків даних, що є критично важливим для державних і банківських структур.

Список літератури

1. Бідюн П., Бондарчук В. Сучасні методи біометричної ідентифікації. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Том 1, № 18. 2009. С. 137 – 145. URL: https://ela.kpi.ua/server/api/core/bitstreams/7f1251ba-7156-4730-8a08-3ae82ddbc1f3/content (дата звернення: 02.11.2024).
2. Adler A. Cancelable Biometrics. In: Li S., Jain A. (eds) Encyclopedia of Biometrics. 2009. Springer, Boston, MA. DOI: https://doi.org/10.1007/978-0-387-73003-5_66.

Відомість про авторів

Баклицька Анастасія Романівна, студентка кафедри програмних засобів Національного університету «Запорізька політехніка», baklytskaanactasia@gmail.com
Зайко Тетяна Анатолівна, доцент кафедри програмних засобів Національного університету «Запорізька політехніка», к.т.н., доцент, nika270202@gmail.com

Секція 1

ЗАХИСТ ВІД КОМП'ЮТЕРНИХ ІНФЕКЦІЙ ЗА ДОПОМОГОЮ PROXY FIREWALLS

Болучевський М. Б.
Національний університет «Запорізька політехніка»
Науковий керівник: Зайко Т. А.

Актуальність. Проксі-брандмауер є важливою мірою безпеки, яка діє як посередник між пристроєм користувача та Інтернетом[1]. Він надає додатковий рівень захисту, контролюючи вхідний і вихідний трафік, захищаючи мережу від несанкціонованого доступу, кіберзагроз та фільтруючи небажаний контент. Однією з ключових проблем у сучасних мережах є забезпечення безпеки в умовах зростаючих кіберзагроз. Потрібно не лише запобігати несанкціонованому доступу до мережі, але й забезпечувати захист від шкідливого трафіку, при цьому зберігаючи продуктивність мережі. Проксі-брандмауер має вирішити ці питання, гарантуючи безпеку, але з мінімальними впливами на швидкість та продуктивність мережі.

Метою роботи є дослідження можливостей захисту від комп'ютерних інфекцій за допомогою проксі-брандмауеру.

Основні положення. Проксі-брандмауер використовує IP- та протокольні фільтри для блокування несанкціонованого доступу і глибокої перевірки вмісту, що входить і виходить із мережі. Він також може кешувати документи та обмежувати прямі з'єднання між користувачем і зовнішніми сайтами, підвищуючи безпеку[2]. Алгоритм роботи користувача через проксі-брандмауер виглядає наступним чином: Користувач запитує Інтернет через такий протокол, як протокол передачі файлів (FTP) або протокол передачі гіпертексту (HTTP). Комп'ютер користувача намагається створити сеанс між ним та сервером, відправляючи пакет повідомлення синхронізації (SYN) зі своєї IP-адреси на IP-адресу сервера. Проксі-брандмауер перехоплює запит і, якщо політика дозволяє, відповідає пакетом повідомлення синхронізації-підтвердження (SYN-ACK) з IP-адреси запитаного сервера. Коли пакет SYN-ACK отримано комп'ютером користувача, він відправляє фінальний пакет ACK на IP-адресу сервера. Це гарантує підключення до проксі-сервера, але не дійсне підключення протоколу керування передачею (TCP). Проксі завершує підключення до зовнішнього сервера, відправляючи пакет SYN зі своєї IP-адреси. Коли він отримує пакет SYN-ACK сервер, він

відповідає пакетом ACK. Це забезпечує дійсне TCP-з'єднання між проксі та комп'ютером користувача, а також між проксі та зовнішнім сервером. Запити, виконані через з'єднання клієнт-проксі, а потім через з'єднання проксі-сервер, будуть аналізуватися, щоб переконатися в їх коректності та відповідності корпоративній політиці, доки одна зі сторін не розірве з'єднання. Цей процес забезпечує високозахищену мережу, яка забезпечує глибоку перевірку вмісту кожного пакета, що входить та виходить із мережі [3]. Однак, проксі-брандмауер має свої недоліки, такі як уповільнення трафіку через створення нових з'єднань для кожного пакета. Це може створити вузькі місця в мережі й негативно вплинути на продуктивність.

Висновки. Проксі-брандмауер є важливим інструментом для створення мережевої безпеки, який надає високий рівень захисту мережі за допомогою фільтрації та глибокої перевірки даних. Він допомагає уникати прямих з'єднань з небажаними ресурсами та запобігає більшості кіберзагроз. Проте, необхідно враховувати можливі недоліки, такі як зниження продуктивності, і правильно адаптувати його до потреб конкретної мережі для оптимальної роботи.

Список літератури

1. What is a Proxy firewall. *CitizenSide*. URL – https://citizenside.com/technology/what-is-a-proxy-firewall (дата звернення 12.11.2024).
2. Understanding How Proxy Firewalls Protect Applications. *Firewall Fundamentals*. URL – https://firewallfundamentals.com/proxy-firewalls-protect-applications (дата звернення 12.11.2024).
3. What Is a Proxy Firewall and How Does It Work? *Fortinet*. URL – https://www.fortinet.com/de/resources/cyberglossary/proxy-firewall (дата звернення 12.11.2024).

Відомості про авторів

Болучевський Максим Борисович, студент кафедри програмних засобів Національного університету «Запорізька політехніка», bnm260811@gmail.com
Зайко Тетяна Анатолівна, доцент кафедри програмних засобів Національного університету «Запорізька політехніка», к.т.н., доцент, nika270202@gmail.com

Секція 1

MODERN APPROACHES TO SOLVING THE PROBLEMS OF POST-QUANTUM CRYPTOGRAPHY

Serhii Butenko
National Aerospace University «Kharkiv Aviation Institute»
Research adviser: Vladimir Pevnev
Language adviser: Iryna Shulga

Actuality. Today, a large number of corporations and governments consider quantum computers and related quantum computing to be one of the most promising areas for fundamental research. The development of these technologies may pose a threat of compromising all widely used cryptographic algorithms. For this reason, the study of the impact of quantum computing on modern and promising crypto algorithms is a priority task [1].

The purpose is to study the impact of quantum computing on modern crypto algorithms. Identify opportunities to improve crypto algorithms to minimize and/or eliminate the likelihood of their possible compromise. Investigate promising crypto algorithms created to solve the problems of post-quantum cryptography.

Main points. When researching the impact of advanced quantum computers on modern cryptographic systems the primary task is to determine their potential computing capabilities. Today cryptography researchers most often assume that large-scale quantum computers will allow compromising all modern crypto algorithms in a relatively short period of time. In this case, symmetric encryption algorithms with a key length of 256 bits and asymmetric algorithms with a key length of 2048 bits (for the RSA algorithm) and 256 bits (for the ECC algorithm) are considered as modern. Also, modern crypto algorithms include hashing algorithms with length of output sequence equal to 256-bit [2].

In the process of improving existing encryption and hashing algorithms the main approach is to increase the key length for encryption algorithms and the length of the output sequence for hashing algorithms respectively. According to the conclusions of most researchers the minimum permissible key length should be 512 bits. This will ensure the crypto resistance of these algorithms in the near future [3].

In the case of the asymmetric encryption algorithms researchers' opinions differ. In the analyzed scientific papers the researchers propose increasing the key length similarly to symmetric algorithms. But some researchers believe that increasing the key length will lead to a significant decrease in performance making them irrelevant [3].

The most authoritative report in this area is the NIST report. According to this report increasing the key length for symmetric encryption algorithms is

proposed. A similar approach for hashing algorithms is used (increasing the length of the output sequence). In the case of modern asymmetric algorithms their using is considered inappropriate [4].

Another approach is to create new algorithms. The main goal in this case is to increase the complexity of the brute-force search problem. The complexity of solving these problems allows to ensure the required level of crypto resistance [5].

Conclusions. Most researchers today identify large-scale quantum computers as a significant threat to the compromise of modern crypto algorithms. According to the study modern versions of crypto algorithms should be considered potentially vulnerable if a large-scale quantum computer with a significant number of qubits is created. Based on these modern symmetric crypto algorithms require increasing key length which will ensure an appropriate level of cryptographic resistance. In the case of asymmetric encryption algorithms a replacement according to the requirements for post-quantum cryptography will need to be created.

List of references

1. A Survey about Post Quantum Cryptography Methods / J. R. J. EAI Endorsed Transactions on Internet of Things. 2024. Volume 10. DOI: 4108/eetiot.5099.
2. Pinto J. Post-Quantum Cryptography. ARIS2 - Advanced Research on Information Systems Security. 2022. Volume 2(2). Page 4–16. DOI: 10.56394/aris2.v2i2.17.
3. Post-Quantum Cryptography trends and perspectives. European Scientific e-Journal. 2021. DOI: 10.47451/inn2024-03-01.
4. Chen L., Stephen J. Report on Post-Quantum Cryptography. 15 p. DOI: 10.6028/NIST.IR.8105.
5. Post Quantum Cryptography: A Review of Techniques, Challenges and Standardizations / R. Bavdekar. 2023 International Conference on Information Networking (ICOIN). Thailand. 2023. DOI: 10.1109/icoin56518.2023.10048976.

Author Information

Serhii Butenko, a PhD student from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», s.butenko@student.csn.khai.edu
Vladimir Pevnev, Dr. Sc., professor from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», v.pevnev@csn.khai.edu
Iryna Shulga, PhD of Pedagogic Sciences, associate professor, Head of the Department of Foreign Languages, National Aerospace University «Kharkiv Aviation Institute», i.shulga@khai.edu

Секція 1

ВИКОРИСТАННЯ OSINT ДЛЯ ПОБУДОВИ ЕФЕКТИВНИХ СТРАТЕГІЙ КІБЕРЗАХИСТУ

Вірський Я. М.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Тецький А. Г.

Актуальність. У сучасному цифровому середовищі, із зростанням кількості та складності кібератак, організації потребують швидкого доступу до інформації для виявлення, аналізу та нейтралізації кіберзагроз. Open-Source Intelligence (OSINT), що базується на зборі та аналізі відкритих джерел інформації, є одним із ключових компонентів побудови надійних стратегій кіберзахисту[1]. Завдяки OSINT можна виявляти слабкі місця в IT-інфраструктурі, аналізувати поведінку потенційних зловмисників та відстежувати витоки даних. OSINT активно застосовується для ідентифікації вразливостей в IT-інфраструктурі, моніторингу даркнету, аналізу активності у соціальних мережах та відстеження витоків даних[2]. Разом із тим, важливими залишаються виклики, пов'язані із правовими обмеженнями та етикою використання цих інструментів.

Метою даної роботи є дослідження можливостей використання OSINT для розробки ефективних стратегій кіберзахисту, проаналізувати інструменти та методи OSINT, а також визначити їх роль у підвищенні стійкості до кібератак. Розгляд успішних прикладів застосування OSINT у попередженні атак на критичну інфраструктуру, моніторингу даркнету та протидії фішинговим кампаніям.

Основні положення. Аналіз популярних інструментів, таких як Shodan, Maltego, SpiderFoot, які дозволяють ідентифікувати загрози, відстежувати витоки даних та аналізувати активність у кіберпросторі[3]. Застосування OSINT для моніторингу мережі, виявлення аномальної активності, формування профілів загроз та оцінки потенційних ризиків. Дослідження обмежень та викликів у застосуванні OSINT у різних юрисдикціях, зокрема відповідність до GDPR та інших міжнародних стандартів[4].

Висновки. OSINT є важливим компонентом для побудови ефективних стратегій кіберзахисту, що дозволяє зменшити ризики несанкціонованого доступу, витоків даних та інших кіберзагроз. Водночас, успішне використання OSINT вимагає інтеграції інструментів у загальну систему

безпеки, високого рівня компетенцій фахівців та дотримання правових і етичних норм.

Список літератури

1. OSINT and Cyber Security News, Blogs and Publications. *HackYourMom*. URL – https://hackyourmom.com/osvita/novyny-blogy-ta-publikacziyi-pro-osint-ta-kiberbezpeku-chastyna-2 (дата звернення: 10.11.2024).
2. OSINT як частина системи кіберзахисту. *Інформаційна Корпоративна Служба*. URL – https://x-scif.info/articles-and-literature/metodyka-vyyavlennya-obyektiv-kiberbezpeky-na-bazi-tehnologiyi-osint (дата звернення: 10.11.2024).
3. Мірошніченко І. О., Ланде Д. В. Роль методів OSINT в кібербезпеці та їх застосування під час воєнних конфліктів. *Теоретичні і прикладні проблеми фізики, математики та інформатики*. 2024. С. 3. URL: https://ela.kpi.ua/handle/123456789/69980 (дата звернення: 10.11.2024).
4. Небезпека інструментів OSINT та способи пом'якшення наслідків їх використання для організації. *VentureBeat*. URL – https://venturebeat.com/2021/03/10/aqua-security-protects-containerized-apps-and-infrastructure-raises-135m (дата звернення: 13.11.2024).

Відомості про авторів

Вірський Ярослав Михайлович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.m.virsjkyy@student.csn.khai.edu
Тецький Артем Григорович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.tetskiy@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ ШЛЯХІВ ПІДВИЩЕННЯ БЕЗПЕКИ В КОНТЕЙНЕРАХ KUBERNETES: АНАЛІЗ ТА ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

Власов Ю. О.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник: Узун Д. Д.

Актуальність. З ростом використання Kubernetes у хмарних середовищах збільшується і ймовірність потенційних атак на безпеку даних. Розуміння та управління безпекою в Kubernetes стає ключовою проблемою для забезпечення стійкості системи від можливих загроз. Результат також показує, що 94% організацій стикалися принаймні з одним інцидентом безпеки за останні 12 місяців, серед яких 69% проблем безпеки пов'язані з неправильною конфігурацією [1]. З моменту свого започаткування у 2014 році Kubernetes встановив себе як фактичний інструмент для автоматизованої оркестрації контейнерів [2]. Хвиля вразливостей ядра Linux, таких як Dirty COW, які можуть бути використані для виходу з контейнерів, збільшила страхи щодо недостатньої ізоляції контейнерів [3]. Додатково, згідно з доповіддю IBM про вартість порушення захищеності даних, середні витрати на наслідки порушення захищеності даних у 2023 році становлять 4,35 мільйона доларів, що на 13% більше, ніж у 2020 році, що ілюструє масштаб цих проблем безпеки [4].

Метою даного дослідження є аналіз інструментів та методів забезпечення безпеки в Kubernetes та розробка практичних рекомендацій щодо підвищення рівня безпеки в масштабованих кластерах.

Основні положення. Аналізуючи ринок хмарних технологій, виявлено, що Kubernetes стає основним інструментом для розгортання та управління додатками в хмарних та гібридних середовищах. Однак, зростання використання Kubernetes призводить до збільшення кількості потенційних атак та вразливостей, що потребує комплексного підходу до забезпечення безпеки. Для ефективного захисту середовища виконання програм у Kubernetes використовуються різноманітні інструменти та підходи. На етапах до та під час виконання програми активно використовуються такі засоби: Kubesec, OPA GateKeeper, Falco, AppArmor Seccomp, та ін. Крім того, принципи, такі як принцип найменшого доступу, захист на всіх рівнях і безпека на основі дизайну, є ключовими стратегіями у розробці безпечних систем [5]. У роботі проведено аналіз переваг та недоліків різних

інструментів, а також надано рекомендації з їх ефективного використання для комплексного захисту системи від потенційних загроз на всіх етапах роботи та обслуговування.

Висновки. Дослідження показує необхідність постійного вдосконалення стратегій безпеки в Kubernetes та активної участі спеціалістів у забезпеченні безпеки в хмарних середовищах. Рекомендації безпеки включають у себе використання інструментів моніторингу загроз, виявлення вразливостей та заходів з підвищення безпеки в масштабованих Kubernetes-кластерах.

Список літератури

1. Shamim S. I. Mitigating security attacks in kubernetes manifests for security best practices violation. ESEC/FSE '21: 29th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, м. Athens Greece. New York, NY, USA, 2021. DOI: https://doi.org/10.1145/3468264.3473495.
2. Security Misconfigurations in Open Source Kubernetes Manifests: An Empirical Study / A. Rahman та ін. ACM Transactions on Software Engineering and Methodology. 2023. DOI: https://doi.org/10.1145/3579639.
3. Viktorsson W., Klein C., Tordsson J. Security-Performance Trade-offs of Kubernetes Container Runtimes. 2020 28th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), France, 2020. DOI: https://doi.org/10.1109/mascots50786.2020.9285946 (дата звернення: 01.05.2024).
4. IBM Data Breach. *IBM*. URL – https://www.ibm.com/reports/data-breach (дата звернення: 01.05.2024).
5. Saltzer J. H., Schroeder M. D. The protection of information in computer systems. Proceedings of the IEEE. 1975. Volume 63(9). Page 1278–1308. DOI: https://doi.org/10.1109/proc.1975.9939.

Відомості про авторів

Власов Юрій Олексійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.vlasov@student.csn.khai.edu
Узун Дмитро Дмитрович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., доцент, d.uzun@csn.khai.edu

Секція 1

КІБЕРБЕЗПЕКА В ЕПОХУ ШТУЧНОГО ІНТЕЛЕКТУ

Ганзера М. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Морозова О. І.

Актуальність. Сьогодні стрімкий розвиток штучного інтелекту (ШІ) сильно впливає та змінює багато сфер, особливо технологічну, і кібербезпека також не стала винятком [1]. ШІ може бути як частиною надійного захисту систем, так і стати «мозком» продуманих та фатальних кібератак [2]. Наразі ШІ вже використовується у великих компаніях для аналізу, відстеження та запобігання різного роду атак [3]. Тому з часом, тема пов'язана з використанням ШІ для захисту від кібератак буде тільки набирати більших оборотів та звучати все частіше.

Метою даної роботи є аналіз, як штучний інтелект впливає та буде впливати на сферу кібербезпеки, дослідити потенціал ШІ як інструменту захисту від кібератак або навпаки, як частину атаки [4].

Основні положення. Прогноз, що глобальна кіберзлочинність коштуватиме понад $23 трлн до 2027 року не є втішним, тому співпраця ШІ з кібербезпекою є найоптимальнішим варіантом в даний момент. Кібербезпека на основі ШІ має низку переваг, таких як управління ідентифікацією, що гарантує захист даних і мереж від несанкціонованого доступу, моніторинг у реальному часі, який захищає як локальних, так і віддалених користувачів, а також покращена видимість, яка виявляє прогалини в системі безпеки [3]. Для розуміння того, як ШІ може допомогти у захисті, потрібно знати алгоритми його використання в атаках. Розроблення просунутого шкідливого програмного забезпечення може використовувати алгоритми машинного навчання для створення шкідливого програмного забезпечення, яке самооптимізується на основі реакції середовища, яке намагається заразити, таким чином уникаючи систем, які зазвичай використовуються для його виявлення (антивірусів). Deepfakes: створюють аудіо або відео, які здаються реальними, але не є такими насправді, і можуть використовувати їх для створення дезінформаційних кампаній, погроз, шантажу користувачів і навіть обманювати алгоритми контролю доступу або аутентифікації організацій для доступу до несанкціонованих систем. Але завдяки ШІ можна відстежити нормальну поведінку користувачів і систем у мережі, а також спостерігати за ними, щоб виявляти незвичну активність. Алгоритми

штучного інтелекту також можуть аналізувати програмний код для пошуку потенційних вразливостей для вчасного виявлення та виправлення їх, щоб кіберзлочинці не змогли ними скористатися. Ще однією великою перевагою штучного інтелекту у світі кібербезпеки є можливість автоматизації реагування на інциденти, наприклад, автоматичне блокування підозрілих IP-адрес, що дозволяє швидше відповідати на кіберзагрози. Таким чином, в роботі були розглянуті деякі з переваг ШІ і того, як він може допомогти організаціям зменшити свої ризики та вразливості в більш ефективний і дієвий спосіб.

Висновки. Підсумовуючи, можна сказати, що ШІ безумовно є сильним інструментом, але він сам по собі не є поганим чи хорошим, таким його робить той, хто ним користується. Для того, щоб максимально використовувати можливості ШІ та мінімізувати ризики, необхідно створювати нові методи захисту, підвищувати етичні стандарти та розробляти регуляторні рамки для його використання у кіберпросторі.

Список літератури

1. The impact of AI: Cybersecurity challenges and opportunities. *Pluralsigth.* URL – https://www.pluralsight.com/resources/blog/cybersecurity/ai-impact-cybersecurity#future-of-ai-security (дата звернення: 19.10.2024).
2. Generative AI and Cybersecurity: Strengthening Both Defenses and Threats. *Bain & Company*. URL – https://www.bain.com/insights/generative-ai-and-cybersecurity-strengthening-both-defenses-and-threats-tech-report-2023/ (дата звернення: 19.10.2024).
3. AI Cybersecurity: 18 Companies. *BuiltIn*. URL – https://builtin.com/artificial-intelligence/artificial-intelligence-cybersecurity (дата звернення: 20.10.2024).
4. The Impact and Limitations of Artificial Intelligence in Cybersecurity. *SSRN*. URL – https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323317 (дата звернення: 21.10.2024).
5. AI for Cybersecurity A Handbook of Use Cases by Peng Liu, Tao Liu. *Penn State Cyber Security Lab*. URL – https://psucybersecuritylab.github.io/book.pdf (дата звернення: 21.10.2024).

Відомості про авторів

Ганзера Марина Олексіївна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.o.ganzera@student.csn.khai.edu
Морозова Ольга Ігорівна, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, o.morozova@csn.khai.edu

Секція 1

АНАЛІЗ ІСТОРІЇ ТА ФУНКЦІОНАЛУ ПЕРШИХ ШКІДЛИВИХ ПРОГРАМ

Горбач А. В.
Вінницький Національний Технічний Університет
Научний керівник: Маліновський В. І.

Актуальність. Перші шкідливі програми, такі як Creeper, Brain, Jerusalem, Form, вірус I Love You і хробак Морріс були першими в історії і стали основою для розвитку сучасних вірусів і шкідливих ПЗ модулів у сучасному цифровому середовищі, що стало передумовою появи класу шкідливого програмного забезпечення(ШПЗ), яке зараз є однією із основних типів кіберзагроз для компбтерних систем. Ці ранні шкідливі програми не лише продемонстрували можливість експлуатації уразливостей в обчислювальних системах, але й сприяли створенню перших антивірусних програм, які ставали важливою частиною захисту від нових кіберзагроз. У міру розвитку технологій і появи нових видів атак на комп'ютерні системи і мережі ці віруси стали важливими етапами в еволюції і становленні кібербезпеки.

Метою даної роботи є дослідження перших шкідливих програм і аналіз їхнього впливу на еволюцію ШПЗ для визначення основних тенденцій у розвитку кіберзагроз і антивірусних систем.

Основні положення. Проведений аналіз показав, що основними вірусами, які мали найбільший вплив на інформаційні комп'ютерні системи були: Creeper, Brain, Jerusalem, Form, вірус I Love You . Кожен із них мав функціонал ШПЗ і був окремим програмним модулем, що мав свій унікальний алгоритм роботи, унікальний код, hash-сигнатурні значення і різні функціональні можливості впливу на інформаційні системи, зокрема. Creeper – перший комп'ютерний черв'як, який поширювався через мережу ARPAnet в 1971 році [1]. Creeper не змінював файли чи завдавав руйнівного впливу на систему, а лише переміщувався з комп'ютера на комп'ютер, залишаючи повідомлення: «I AM CREEPER. CATCH ME IF YOU CAN!». Це і стало основою для створення першої антивірусної програми Reaper, яка видаляла Creeper з інфікованої системи. Він реалізувався через самовідтворення коду в мережі, заражаючи комп'ютери. Brain – перший вірус, що спричинив глобальну епідемію [2]. Він був створений пакистанськими братами Алві в 1986 році як захист для медичного ПЗ, яке використовувалося для моніторингу серцевого ритму. Цей вірус працював

через зараження завантажувальних секторів дисків, що дозволяло йому активуватися щоразу при запуску комп'ютера, автоматично поширюючись через підключення зовнішніх носіїв. Хробак Морріса – перший хробак, який спричинив масштабну кіберкатастрофу в 1988 році, який був спроектований для дослідження масштабів ARPAnet [4]. Проблеми виникли, коли хробак некоректно перевіряв свою наявність, що призводило до надмірного самокопіювання і перевантаження систем. Він поширювався по комп'ютерах, виводячи з ладу мережі через непотрібне дублювання.

Висновки. Історія перших шкідливих програм відображає еволюцію кіберзагроз і необхідність створення ефективних методів боротьби з ними. Creeper, Brain та хробак Морріса стали важливими етапами в розвитку кібербезпеки, оскільки продемонстрували реальні вразливості в обчислювальних системах та ініціювали створення антивірусних програм і систем захисту інформації. Ці віруси заклали основи для розробки сучасних засобів кіберзахисту, і їхній аналіз допомагає краще розуміти розвиток нових загроз у цифровому середовищі.

Список літератури

1. Creeper: The World's First Computer Virus. *Exambeam*. URL: https://www.exabeam.com/blog/infosec-trends/creeper-the-worlds-first-computer-virus (дата звернення: 11.11.24).
2. Brain (computer virus) Найбільш знамениті олдові віруси комп'ютерної ери. *HackYourMom*. URL: https://hackyourmom.com/osvita/najbilsh-znamenyti-oldovi-virusy-kompyuternoyi-ery (дата звернення: 12.11.24).
3. I Love You (computer virus) Computer Hope. *Computer Hope*. URL: https://www.computerhope.com/vinfo/iloveyou.htm (дата звернення: 14.11.24).

Відомості про авторів

Горбач Аліна Вікторівна, студентка кафедри захисту інформації, Вінницький Національний Технічний Університет, horbachalina08@gmail.com
Маліновський Вадим Ігоревич**,** доцент кафедри захисту інформації, Вінницький Національний Технічний Університет, к.т.н., v.malinovskyi@vntu.edu.ua

Секція 1

ОСНОВНІ ПРАВИЛА КІБЕРГІГІЄНИ ПРИ ВИКОРИСТАННІ ЕЛЕКТРОНОЇ ПОШТИ

Горковлюк В. М.
Вінницький національний технічний університет, Вінниця, Україна
Науковий керівник: Майданевич Л. О.

Актуальність. Безпека електронної пошти має дуже велике значення на арені цифрової трансформації, оскільки це основний спосіб спілкування в бізнесі та обміну конфіденційною інформацією. Це, що супроводжується зростаючими кіберзагрозами (такими як фішинг і перехоплення даних, а також посилення регуляторного тиску на захист даних), робить покращену безпеку електронної пошти обов'язковою. Не тільки для запобігання витоку інформації, але й для збереження довіри клієнтів та партнерів. З інтеграцією в систему нових технологій і платформ захист електронної пошти слід розглядати як частину загальної стратегії кібербезпеки організації.

Метою даної роботи є дослідження основних способів та методів захисту електронної пошти .

Основні положення. Безпека електронної пошти означає захист облікових записів і повідомлень від несанкціонованого доступу, втрати даних і таких загроз, як: зловмисне програмне забезпечення, спам і фішинг. Кіберзлочинці здебільшого атакують електронну пошту, оскільки це найуспішніший спосіб отримати доступ до облікових записів користувачів і пристроїв. Такі атаки зазвичай відбуваються через людську недбалість, і лише одна помилка може призвести до серйозних наслідків для безпеки організації [1]. Серед найпоширеніших загроз для електронної пошти можемо зазначити такі: фішинг (сучасні фішингові електронні листи видають себе за відомий бренд з метою обману змусити одержувача натиснути шкідливу URL-адресу [2]); спам (комерційні компанії використовують спам для масової розсилки рекламної інформації [1]); підробка (це випадки, коли кіберзлочинці підробляють когось із довіреної організації чи фізичної особи, щоб використовувати електронну пошту для обману з метою переказу грошей або конфіденційних даних [1]); ШПЗ (до найпоширеніших типів шкідливого програмного забезпечення належать віруси, хробаки, зловмисні програми з вимогою викупута шпигунське ПЗ [2]). Враховуючи вказані загрози можемо сформулювати наступні правила кібергігієни при використанні електронної пошти. Створюйте надійний

пароль (використовуйте довгий, складний пароль з комбінацією великих і малих літер, чисел і спеціальних символів; не використовуйте один і той самий пароль для різних облікових записів). Увімкніть двофакторну автентифікацію. Будьте обережні з підозрілими листами (не відкривайте листи від невідомих або підозрілих відправників; уникайте відкриття вкладень і переходу за посиланнями, які можуть містити шкідливе ПЗ або фішингові посилання). Перевіряйте адресу відправника (уважно звіряйте адресу відправника, оскільки шахраї часто використовують схожі адреси, щоб ввести вас в оману). Не давайте бездумно особисту інформацію (ніколи не діліться персональними даними не встановивши важливість її надання). Регулярно оновлюйте антивірусне програмне забезпечення. Будьте обережні з автоматичними налаштуваннями та пересиланнями (уникайте автоматичного завантаження зображень у листах, щоб уникнути спаму або збору інформації про ваше місцезнаходження). Перевіряйте налаштування конфіденційності (регулярно переглядайте та коригуйте налаштування приватності вашого поштового облікового запису, щоб забезпечити належний рівень захисту) [1, 2].

Висновки. Безпека електронної пошти є важливим елементом загальної стратегії кібербезпеки. Уразливість облікових записів як окремих користувачів, так і компаній, може створювати серйозні ризики для бізнесу, надаючи доступ до спаму, фішингових атак чи захоплення облікових записів. Дотримання запропонованих правил допоможе захистити вашу електронну пошту від злому, шахрайства та витоку конфіденційної інформації.

Список літератури

1. Визначення захисту електронної пошти. *Microsoft.* URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-email-security#Email-security-defined (дата звертання 12.11.2024).
2. Безпека пошти: основні рекомендації для захисту скриньок від онлайн-загроз. *Eset*. URL: https://www.eset.com/ua/about/newsroom/press-releases/security-tips/bezopasnost-pochty-vneshniye-i-vnutrenniye-faktory-zashchity-pochty/ (дата звертання 12.11.2024).

Відомості про авторів

Горковлюк Вадим Миколайович, студент кафедри захисту інформації, ВНТУ, vadikcoin94@gmail.com
Майданевич Леонід Олександрович, ст. викладач кафедри захисту інформації, ВНТУ, к. філос. н., lmaidanevych@ukr.net

Секція 1

КОМПЛЕКСНІ ЗАСОБИ ЗАХИСТУ ВЕБРЕСУРСІВ ВІД ПОШИРЕНИХ АТАК

Гребньов Д.О.
Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»
Науковий керівник: Тецький А.Г.

Актуальність. У сучасному світі веб ресурси займають якщо не найважливіше місце у різних сферах нашого повсякденного життя, то хоча б одне з найпопулярніших місць, вони охоплюють такі сфери життя як бізнес, освіта, соціальні мережі, розваги та й багато інших аспектів повсякденного життя. Вебресурси в наш час набувають неабиякої популярності та розповсюдження в побутовому житті користувачів, що своєю чергою призводить до збільшення інформації, котра зберігається або передається вебресурсами в інтернеті. Дане зростання кількості інформації, котра зберігається або передається вебресурсами, спонукає зловмисників до все більш витончених та складних атак для отримання даної інформації або до примусу звичайного користувача виконати зловмисні дії.

Метою роботи є аналіз сучасних поширених атак на вебресурси та вибір комплексних засобів захисту веб ресурсів від розглянутих атак.

Основні положення. Сучасні зловмисники використовують дедалі складніші методи реалізації своїх атак, комбінуючи їх для досягнення своєї мети, що й ускладнює захист вебресурсів. Виділяють такі найпопулярніші види атак на вебресурси, як атаки на основі паролей, атаки на порушення автентифікації, обхід каталогів, людина посередині, атаки на відмову в обслуговуванні, міжсайтовий скріптинг та міжсайтова підробка запитів [1]. Хоч дані атаки і є поширеними, але захиститися одним методом не вдасться, для цього і потрібно впроваджувати комплексну систему захисту, навіть від одного типу атаки. Наприклад для захисту від атак на відмову в обслуговуванні можна використовувати брандмауери, адаптивний моніторинг, кешування та обмеження швидкості [2]. Якщо розглядати атаки людина посередині, то захистом може слугувати оновлення програмного забезпечення, використання VPN (Virtual Private Network), постійний моніторинг мережі, використовувати двофакторну автентифікацію, перевіряти справжність сертифікати веб ресурсів та шифрувати дані [3]. Переходячи до атаки міжсайтової підробки запитів, то захистом може бути

використання CSRF-токенів, SameSite у файлах cookie, використовувати принцип найменших привілеїв [4].

Висновки. Враховуючи стрімке зростання попиту вебресурсів у повсякденному житті, захист інформації є першочерговим завданням. Водночас неможливо захистити веб ресурс, використовуючи лише один метод захисту, наразі потрібно використовувати комплексні засоби захисту веб ресурсів, щоб знизити рівень загрози самому веб ресурсу та забезпечити безперебійність його роботи для звичайного користувача.

Список літератури

1. The 10 Most Common Website Security Attacks (and How to Protect Yourself). *Tripwire | Security and Integrity Management Solutions*. URL: https://www.tripwire.com/state-of-security/most-common-website-security-attacks-and-how-to-protect-yourself (дата звернення: 01.11.2024).
2. How to prevent ddos attacks. *Cloudflare*. URL – https://www.cloudflare.com/learning/ddos/how-to-prevent-ddos-attacks (дата звернення: 01.11.2024).
3. Malik F. 10 Ways to Prevent Man-in-the-Middle (MITM) Attacks | StrongDM. *StrongDM: Your Partner in Zero Trust Privileged Access*. URL: https://www.strongdm.com/blog/man-in-the-middle-attack-prevention (дата звернення: 06.11.2024).
4. Cross-Site Request Forgery (CSRF) Protection-Synchronizer Token Pattern. *Medium*. URL – https://medium.com/@bhathz222/cross-site-request-forgery-csrf-protection-synchronizer-token-pattern-610032ff8f20 (дата звернення: 07.11.2024).

Відомості про авторів

Гребньов Данило Олександрович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.o.grebnjov@student.csn.khai.edu

Тецький Артем Григорович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.tetskiy@csn.khai.edu

Секція 1

РОЗРОБЛЕННЯ МЕТОДУ ЗАХИСТУ ВІД ФІЗИЧНОЇ ПІДМІНИ ПРИСТРОЇВ ОХОРОННОЇ СИГНАЛІЗАЦІЇ У ОБ'ЄКТАХ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ

Григор'єв А. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Морозова О. І.

Актуальність. Сучасні технології значно змінюють наше повсякденне життя, роблять процеси більш ефективними та спрощують їх [1]. Однак, зі зростанням застосування пристроїв охоронної сигналізації в різних галузях, з'являються нові виклики стосовно їх безпеки та захисту від можливих загроз. Тому проблема захисту від фізичної підміни таких охоронних пристроїв стає дуже актуальною, особливо в контексті збільшення застосування технології інтернету речей, де ці пристрої використовуються для збору та передачі даних у реальному часі [2]. Сучасні системи охоронних сигналізацій не завжди забезпечують ефективний захист від фізичної підміни пристроїв, що може стати причиною можливих вторгнень і крадіжок інформації. Недолік в захисті може бути використаний зловмисниками для незаконного доступу до системи та викрадення даних з метою їх подальшого використання з особистою користю [3].

Метою роботи є розроблення та впровадження ефективних методів захисту, які забезпечують надійність та безпеку використання пристроїв охоронних сигналізації в умовах збільшеного ризику фізичної підміни [4].

Основні положення. Дослідження та розроблення методів захисту включають в себе використання криптографічних методів шифрування даних, що забезпечують конфіденційність та цілісність даних, що пережаються, ускладнюючи їх перехоплення та підміну зловмисниками. Важливим аспектом є проєктування фізичних захисних корпусів для охоронних пристроїв, що ускладнюють доступ до внутрішніх компонентів за допомогою ударостійких матеріалів, датчиків розкриття та механізмів самознищення при спробі несанкціонованого доступу. Інтеграція систем виявлення вторгнень (IDS) дозволяє слідкувати за активністю та виявляти аномальні дії, які можуть свідчити про спробу фізичної підміни або несанкціонованого доступу, автоматично сповіщаючи адміністраторів про підозрілі події та запускаючи контрзаходи [5].

Висновки. Захист від фізичної підміни охоронних пристроїв є критично важливим завданням у сучасному технологічному середовищі. Його вирішення вимагає комплексного підходу та спільних зусиль фахівців у галузі технологій та безпеки для забезпечення надійності та безпечне використання цих пристроїв. Це включає впровадження передових криптографічних методів, фізичних захисних механізмів, систем виявлення вторгнень, регулярне оновлення стандартів безпеки, багатофакторну аутентифікацію, постійний моніторинг та аудит. Тільки завдяки комплексному підходу та використанню новітніх технологій можна ефективно знизити ризики, пов'язані з фізичною підміною охоронних пристроїв, та забезпечити їх безперебійну та безпечну роботу в умовах сучасних загроз.

Список літератури

1. Іванов П. О., Петрова Л. М. Аналіз ефективності сучасних охоронних датчиків у системах безпеки. У кн.: Технології безпеки: матеріали конференції «Сучасні виклики безпеки», 15-16 жовтня 2020 р., м. Київ, м. Львів, м. Одеса, м. Дрезден : [у 2 т.]. Т. 2 / Київський нац. ун-т [та ін.]. – Київ: Видавництво Науковий світ, 2020. – 112 с.

2. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури / ДержНДІ Спецзв'язку УДК 004.056, 2015. – 58-60 с.

3. Системи контролю і управління доступом від А до Я. *Deps*. URL: https://deps.ua/ua/knowegable-base/reference-information/7824.html (дата звернення: 23.10.2024).

4. Професійна безпека системи. *Ajax*. URL: https://ajax.systems/ua/ (дата звернення: 23.10.2024).

5. Мазур Ю. О., Зелінська О. В. Особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу. Прикладні аспекти сучасних міждисциплінарних досліджень: матеріали І Всеукраїнської науковопрактичної конференції (м. Вінниця, 26 листопада 2021 р.). Вінниця: ДонНУ імені Василя Стуса, 2021. С. 102–103. URL: https://jpasmd.donnu.edu.ua/issue/view/403 (дата звернення: 23.10.2024).

Відомості про авторів

Григор'єв Андрій Олексійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.o.hryhoriev@student.csn.khai.edu

Морозова Ольга Ігорівна, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, o.morozova@csn.khai.edu

Секція 1

РЕФЛЕКСИВНИЙ АНАЛІЗ ВРАЗЛИВОСТЕЙ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ НА ОСНОВІ ПРОМПТІВ

Друзь Д. Р.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Науковий керівник: Смирнов С. А.

Актуальність. У сучасному цифровому світі великі мовні моделі (ВММ) стали невід'ємною частиною технологічного ландшафту, здобувши широке визнання та застосування в різноманітних сферах, від обробки природної мови до генерації контенту [1]. Однак, попри їхні потужні можливості, ці моделі часто мають вразливості, які можуть становити загрозу для їх безпечного та етичного використання.

Метою роботи є дослідити великі мовні моделі на рефлексивність для подальшого перенесення методів рефлексивного аналізу на мовні моделі.

Основне положення. Рефлексія – це властивість свідомості людини створювати образ об'єкту своєї уваги, в тому числі здатність суб'єкту зайняти позицію спостерігача за своїми думками та вчинками. У рефлексивному аналізі об'єктом дослідження є індивід здатний до рефлексії. Головною задачею є зробити моральний вибір [2]. В рамках дослідження модель вибору враховує 3 зміні: зовнішній вплив, очікуваний вплив та намір або бажання до вибору відповідно:

$$A = F(a, F(b, c))$$

Кожна з цих змінних визначена на множині булевих елементів, тобто може приймати лише 2 значення 1 – добро або 0 – зло. Результатом обчислення цієї функції є готовність суб'єкту зробити хорошу або погану дію. Мовна модель є моделлю людини, що в свою чергу здатна до рефлексії. Тому стає питання чи можна застосувати рефлексивний аналіз для великих мовних моделей з метою обходження внутрішніх фільтрів контенту. На даний момент з такою ціллю використовуються атаки на основі промпт запитів, такі як prompt injection та jailbreak attack [3]. Промпт (prompt) – це вхідний текст або інструкція, яка спрямовує модель на генерацію бажаного виводу. Промпт може містити в собі:

- інструкція/завдання – що саме потрібно зробити;
- контекст – додаткова інформація для кращого розуміння завдання;
- формат – бажана структура відповіді;
- обмеження – специфічні вимоги чи рамки.

Jailbreak attack (атака «втечі з в'язниці») – це форма злому, метою якої є обхід етичних гарантій моделі ШІ та отримання забороненої інформації. Він використовує креативні підказки простою мовою, щоб обманом змусити генеративні системи штучного інтелекту видавати інформацію, яку в іншому випадку блокували б їхні фільтри вмісту [4]. Prompt injection – це тип кібератаки на великі мовні моделі (LLM). Хакери маскують зловмисні дані під дозволені промпти, маніпулюючи генеративними системами штучного інтелекту (GenAI) для витоку конфіденційних даних, поширення дезінформації або ще гірше. Ці атаки націлені на обходження фільтрів контенту ВММ, але вони не спираються на рефлексивний аналіз.

Висновки. Було проведено дослідження стосовно рефлексивності та рефлексивного аналізу, вивчено методи перевірки моделей на відношення до тієї чи іншої етичної системи. Були розглянуті найпопулярніші атаки генеративних моделей зі штучним інтелектом на прикладі Chat GPT. Також були проаналізовані структура та принцип їх роботи. За допомогою інтернет-джерел було продемонстрована робота Jailbreak attack та Prompt injection для старих версій чат боту GPT, а також були наведені ілюстративні матеріали з демонстрацією роботи представлених атак для останньої доступної версії Chat GPT.

Список літератури

1. How can I trick a chat bot to answer questions he is not supposed to? Quora. URL – https://www.quora.com/How-can-I-trick-a-chat-bot-to-answer-questions-he-is-not-supposed-to (дата звернення 12.11.2024).
2. AI jailbreaks: What they are and how they can be mitigated. *Microsoft*. https://www.microsoft.com/en-us/security/blog/2024/06/04/ai-jailbreaks-what-they-are-and-how-they-can-be-mitigated (дата звернення 12.11.2024).
3. ChatGPT Jailbreak Prompts: How to Unchain ChatGPT. *Kanaries*. https://docs.kanaries.net/articles/chatgpt-jailbreak-prompt (дата звернення 12.11.2024)
4. What is a prompt injection attack? *IBM*. URL – https://www.ibm.com/topics/prompt-injection (дата звернення 12.11.2024)

Інформація про авторів

Друзь Данило Русланович, студент кафедри інформаційної безпеки, КПІ ім. Ігоря Сікорського, dandru-ipt23@lll.kpi.ua
Смирнов Сергій Анатолійович, доцент кафедри інформаційної безпеки, КПІ ім. Ігоря Сікорського, к. ф.-м. н., с.н.с., sergsm-ipt@lll.kpi.ua

Section 1

USING ZERO TRUST TECHNOLOGIES TO PROTECT UAVs IN THE MODERN CYBERSPACE ENVIRONMENT

Ruslan Demura
National Aerospace University «Kharkiv Aviation Institute»
Research adviser: Vyacheslav Kharchenko
Language adviser: Iryna Shulga

The relevance of ensuring cybersecurity of unmanned aerial vehicles (UAVs) is rapidly increasing. Their growing popularity in military commercial and research applications is becoming critical [1]. In this context, the Zero Trust approach, which focuses on verifying every interaction in the network, offers a reliable way to protect UAV communication channels, control and operating systems. In today's cyberspace, it is of vital importance to prevent unauthorised access, data interception and drone hacking by providing protection through authentication, segmentation and monitoring.

The purpose of this paper is to substantiate the need for and propose the use of Zero Trust technology to protect information assets of UAVs operating in the modern aggressive cyberspace.

Main points. Zero Trust is a cybersecurity model that provides for the verification of every user and device without trust by default, regardless of their location [2].

Key arguments that determine the need to use Zero Trust to protect UAV cyber assets:

– vulnerabilities in UAV communication channels and control systems can lead to data loss, technology theft, or disruption of operations [3];

– Zero Trust implies the absence of «trust» between network elements meaning that every interaction in the system must be verified and protected;

– Zero Trust requires multi-level authentication and reliable data encryption to provide protection even if a part of the network is compromised [4];

– for secure Zero Trust operations, artificial intelligence and machine learning algorithms are used to analyze network behavior, which helps to detect suspicious activities and respond to them before they cause harm;

– the network segmentation limits each device access only to the resources it needs [5];

– with the development of swarm technologies, Zero Trust approaches can scale to protect hundreds of UAVs in swarms that interact with each other and with the base station;

– as cyber threats and cyberattack tools become more sophisticated, the importance of Zero Trust for UAVs is increasing. Modern research and technology is aimed at creating adaptive solutions that will protect UAVs, even in conditions of unstable communication and dynamic combat situations.

Conclusions. The research identifies specific challenges that arise when adapting Zero Trust for unmanned aerial vehicles due to limited computing resources and unstable connectivity. The research found that multi-level authentication, continuous anomaly monitoring, and dynamic network segmentation can significantly reduce UAV security risks, even in the event a compromise of individual system elements.

List of references

1. Syed N., Shah S., Shaghaghi A., Anwar A., Baig Z., Doss R. Zero trust architecture (ZTA): A comprehensive survey. IEEE Access 2024, 11. 57143–57179. DOI: 10.1109/access.2022.3174679.
2. V. Stafford, «Zero trust architecture», NIST special publication, Volume 800, Page 207, 2020.
3. Dhar S., Bose I., «Securing IoT Devices Using Zero Trust and Blockchain», Journal of Organizational Computing and Electronic. 2021. Volume 31(1). Page 18-34.
4. Phiayura P., Teerakanok S. A Comprehensive Framework for Migrating to Zero Trust Architecture. IEEE Access. 2023. Page 1. DOI: https://doi.org/10.1109/access.2023.3248622.
5. Li S., Iqbal M., Saxena N. Future Industry Internet of Things with Zero-trust Security. Information Systems Frontiers 2022.

Information about the authors

Ruslan Demura, a PhD student from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», r.i.demura@csn.khai.edu
Vyacheslav Kharchenko, Doctor of Science, Professor, Head of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», v.kharchenko@csn.khai.edu
Iryna Shulga, PhD of Pedagogic Sciences, associate professor, Head of the Department of Foreign Languages, National Aerospace University «Kharkiv Aviation Institute», i.shulga@khai.edu

Секція 1

ІНТЕЛЕКТУАЛЬНІ ЗАСОБИ КІБЕРБЕЗПЕКИ В ІНТЕРНЕТ ТА НЕЙРОМЕРЕЖЕВЕ ВИЯВЛЕННЯ ДЕЗІНФОРМАЦІЇ

Денисенко Б. О.
Хмельницький національний університет
Науковий керівник: Залуцька О. О.

Актуальність. В умовах стрімкого розвитку цифрових технологій та соціальних мереж перед суспільством постає проблема зростання дезінформації, яка може серйозно впливати на політичну стабільність, економічну безпеку та громадське здоров'я. Дезінформація, маскуючись під правдиву інформацію, підриває довіру до традиційних джерел інформації та журналістики [1]. Для захисту від дезінформації в Інтернет використовуються різноманітні засоби кібербезпеки, провідну роль серед яких займають засновані на використанні штучних нейронних мереж.

Метою дослідження є розробка методу виявлення дезінформації у вебповідомленнях за допомогою штучних нейронних мереж.

Основні положення. У ході роботи було розроблено метод виявлення дезінформації в вебповідомленнях для підвищення кібербезпеки за допомогою штучних нейронних мереж, який дозволяє аналізувати вхідний текст і визначати ступінь дезінформації в повідомленні. На вхід подається текстове повідомлення, яке спочатку проходить через етап кодування тексту за допомогою текстового енкодера (Text Encoder). Після цього оброблені дані передаються до нейронної мережі, яка аналізує їх на предмет достовірності. На виході модель повертає результат, визначаючи, чи є інформація фейковою («Fake Information»). «Feature extraction» або процес виділення ознак є ключовим етапом, що дозволяє зменшити розмірність даних і виокремити їх ключові характеристики для подальшої обробки чи класифікації. Цей процес передбачає перетворення сирих текстових даних у формат, зрозумілий для нейронної мережі, що сприяє ефективному навчанню. У цьому випадку застосовуються «Word embeddings», які представляють слова як щільні вектори в неперервному векторному просторі, де схожі за значенням слова розташовані ближче одне до одного. Одним із таких методів є GloVe. Результатом дослідження є створена інформаційна система для виявлення дезінформації за допомогою штучних нейронних мереж. Під час навчання система досягла точності 99% на навчальній вибірці та 91% на тестовій вибірці.

Висновки. Отримані результати підтверджують перспективність використання нейронних мереж у завданнях, пов'язаних з автоматичним аналізом тексту та виявленням дезінформації для інтеграції в сучасні інтелектуальні засоби кібербезпеки в інтернет, а також надають підстави для подальшого вдосконалення методів нейромережевого виявлення дезінформації для підвищення точності і надійності засобів кібербезпеки.

Список літератури

1. Krak I., Molchanova M., Mazurets O., Sobko O., Zalutska O., Barmak O. Method for Neural Network Detecting Propaganda Techniques by Markers With Visual Analytic. CEUR Workshop Proceedings, 2024, Volume 3790, Page 158-170.

Відомості про авторів

Денисенко Богдан Олександрович, студент кафедри комп'ютерних наук Хмельницький національний університет, bohdandenysenko@khmnu.edu.ua
Залуцька Ольга Олександрівна, викладач кафедри комп'ютерних наук, Хмельницький національний університет, zalutskolha@gmail.com

Секція 1

МЕТОД ІДЕНТИФІКАЦІЇ ОСОБИСТОСТІ НА ОСНОВІ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ У РЕАЛЬНОМУ ЧАСІ ДЛЯ СИСТЕМ КІБЕРБЕЗПЕКИ

Дидо Р. А.
Хмельницький національний університет
Науковий керівник: Мазурець О. В.

Актуальність. Сучасні загрози у сфері кібербезпеки з кожним днем стають складнішими [1], що вимагає нових, більш досконалих інструментів для їх вирішення. Останні роки значний акцент робиться на авторизації в інформаційних системах підприємств за допомогою розпізнавання обличчя у реальному часі [2], що є засобом захисту від несанкціонованого доступу. Крім того, використання цієї технології сприяє захисту від зовнішніх кіберзагроз, адже ідентифікація за унікальними фізичними характеристиками ускладнює спроби зловмисників обійти систему.

Метою є створення методу ідентифікації особистості на основі розпізнавання обличчя в реальному часі для систем кібербезпеки державних і приватних установ і підприємств.

Основні положення. Метод ідентифікації особистості за зображенням обличчя у реальному часі засобами штучних нейронних мереж надає можливість автоматизувати процеси роботи компанії щодо біометричної ідентифікації з метою контроля доступу до інформаційних систем.

Метод ідентифікації особистості за зображенням обличчя для систем кібербезпеки базується на кількох ключових етапах, які забезпечують точну та швидку роботу системи. Вхідними даними для методу є навчена модель, яка здатна визначати приналежність людини до одного з двох класів: «Worker» або «Other_people».

На першому етапі завантажується навчена модель, що є основою для подальших операцій. На другому етапі здійснюється попередня обробка зображення: кольорове зображення конвертується у відтінки сірого, що дозволяє зменшити обсяг даних і спрощує обробку зображень. На третьому етапі для розпізнавання обличчя використовується маска, яка проектується на лице, що допомагає моделі точніше визначити риси обличчя. На четвертому етапі формується висновок про те чи є особа працівником підприємства чи ні.

Висновки. Отже, було розроблено метод ідентифікації особистості на основі розпізнавання обличчя в реальному часі. Створене програмне

забезпечення з використанням розробленого метода може знайти широке застосування для систем кібербезпеки, захищаючи конфіденційні системи та ресурси від шахрайства та несанкціонованого доступу, тим самим підвищуючи загальний рівень захисту особистих даних.

Список літератури

1. Кіберризики є головною проблемою 62% компаній – опитування Travelers щодо кіберзагроз. *Forinsurer*. URL: https://forinsurer.com/news/24/10/10/44279 (дата звернення 12.11.24).
2. Матеріали-семінару «Використання технологій штучного інтелекту. URL: http://surl.li/txbgeg (дата звернення 12.11.24).

Відомості про авторів

Дидо Ростислав Андрійович, студент спеціальності комп'ютерні науки Хмельницького національного університету, dydora@khmnu.edu.ua
Мазурець Олександр Вікторович, доцент кафедри комп'ютерних наук Хмельницького національного університету, к.т.н., доцент, mazuretso@khmnu.edu.ua

Секція 1

ДОСЛІДЖЕННЯ СТВОРЕННЯ ЗАВАДОСТІЙКИХ КАНАЛІВ ПОСЛІДОВНОГО ЗВ'ЯЗКУ НА БАЗІ МІКРОКОНТРОЛЕРІВ

Діденко І. І.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Перепилицин А. Є.

Актуальність. Надійна передача даних є однім з самих важливих аспектів створення систем здатних працювати у довкіллі з різними джерелами перешкод. Любе спотворення даних у базових протоколах зв'язку може привести до часткової втрати даних або створення помилок у роботі системи, компрометуючи цілісність даних. Ефективним методів підвищення надійності зв'язку та виправлення помилок у повідомленнях є надлишкове кодування. Надлишкове кодування використовує математичні моделі, додаючи додаткову, контрольну, інформацію для виявлення та алгоритмічного виправлення помилок. Такими рішеннями є багато алгоритмів, код Голея, код Ріда-Соломона, турбокод та інші коди, котрі здібні виправляти різну кількість помилок за рахунок зменшення ефективності передачі даних [1, 2]. Також побудова таких систем у smart house системах потребує можливості економічної роботи через вимоги автономної роботи від внутрішніх акумуляторів девайсів, отже має бути обрано доцільний алгоритм та мікроконтролер, на якому буде побудовано пристрій. З комерційно популярних рішень є безліч варіантів та доцільність їх для такої задачі не є явною [4]. У свій час джерелами шуму, котрі можуть вплинути на канал зв'язку, можуть стати як побутові прилади так й помилки у створенні та налагоджені приладів, наприклад smart house системи [3].

Метою даної роботи є вивчення та покращення технологій захищеного передавання даних за допомогою послідовних каналів зв'язку. Для досягнення цієї мети необхідно вирішити наступні задачі: аналіз існуючих надлишкових кодів, дослідження існуючих рішень для побудови систем на базі мікроконтролерів та аналіз їх енергоспоживання.

Основні положення. Для створення надійної системи необхідно гарантувати цілісність даних, які будуть передаватися між елементами системи, від одного пристрою до іншого різного типами каналів. Також ця надійна система має працювати у режимі максимального енергозбереження з такою ж стійкістю до завад у передачі даних. Це має бути гарантовано обраними методами надлишкового кодування та здібностями

мікроконтролерів. Одноядерні мікроконтролери Atmega328P та серія мікроконтролерів STM32L* та STM32F* мають найбільший потенціал, коли двоядерні мікроконтролери ESP32 пропонують високу обчислювальну потужність [5].

Висновки. У сучасних реаліях, коли у кожному домі є безліч приладів та деякі з них можуть вплинути на комунікацію між іншими пристроями, створення стійкої системи зв'язку між пристроями є одним із головних напрямків створення мережі зв'язаних smart приладів. Більшість протоколів послідовного зв'язку не мають стійких вбудованих рішень для виправлення помилок у отриманому повідомлені. Отже розробка завадостійкого зв'язку є важливою для підвищення ефективності цих протоколів. У цій роботі проведено аналіз ефективності, доцільності та енергоефективності деяких надлишкових кодів для використання у послідовних каналах зв'язку, такі як UART, RF канал, або IR канал. Розглянуто та обрано доцільний мікроконтролер від одної з компаній – Microchip (раніше Atmel), STMicroelectronics та Espressif Systems.

Список літератури

1. W. Cary Huffman, Vera Pless, Fundamentals of Error Correcting Codes. Cambridge University. 2003.
2. Shu Lin, Daniel J. Costello, Jr., Error Control Coding Second Edition. 2004.
3. Robin Getz, Bob Moeckel. Understanding and Eliminating EMI in Microcontroller applications. Texas Instruments. 2003.
4. Hamdy M. Youseff, Radwa Ahmed, Alaa A. El-Bary, Efficient Connectivity in Smart Homes: Enhancing Living Comfort through IoT Infrastructure. *Sensors* 2024, 24, 2761. DOI: https://doi.org/10.3390/s24092761.
5. Документація мікроконтролерів STM32. *ST*. URL: https://www.st.com/en/microcontrollers-microprocessors (дата звернення: 14.11.2024).

Відомості про авторів

Діденко Іван Ігорович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.didenko@student.csn.khai.edu
Перепелицин Артем Євгенович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., доцент, a.perepelitsyn@csn.khai.edu

Section 1

THE USE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: OPPORTUNITIES AND RISKS

Daria Drakon
V.N. Karazin Kharkiv National University
Scientific adviser: Natalya Stiahlyk

Relevance. The modern world is rapidly moving towards digitalization, and as technology advances, the number and complexity of cyber threats continue to grow. According to research data [1], in 2023, the number of cyberattacks on private and public organizations increased by 35%, highlighting the need for innovative solutions in cybersecurity. Artificial Intelligence (AI) is becoming increasingly popular as it enables the automation of complex processes, analysis of vast amounts of data, and adaptation to new threats [2]. With the constant increase in network attacks, the use of AI to protect confidential information has become essential, and its role in security will only grow in the future. Therefore, it is crucial today to study the role of AI in cybersecurity and assess its opportunities and risks.

Objective. The objective of using artificial intelligence in cybersecurity is to enhance information protection levels and respond to threats in real-time [3]. AI aims to automate the process of detecting and preventing cyberattacks, improve large-scale data analysis to identify anomalies, and ensure the protection of personal and confidential information. The application of AI seeks to increase network security and the adaptability of security systems to emerging threats.

Principal provisions. AI in cybersecurity opens up new opportunities to improve protection levels. These include automatic threat detection and user behaviour analysis. Systems using machine learning algorithms can recognize suspicious patterns and anomalies in real-time, significantly increasing the speed and accuracy of threat detection [4]. For example, IBM's Watson AI is used for automated threat analysis, reducing detection and response time by 60% [5]. AI can also process large amounts of data, enabling deep analysis and quick response to new types of attacks. This is essential since traditional methods often cannot keep pace with the growing data volume. Additionally, AI can enhance personal data security through new authentication methods, such as biometrics, facial recognition, and voice recognition [5]. However, despite its positive aspects, AI is not without risks. The primary concern is the possibility of false positives, where legitimate behavior is interpreted as a threat, leading to unnecessary resource expenditure on processing false signals [3]. Additionally,

AI models are vulnerable to certain types of attacks, such as data manipulation, allowing attackers to bypass security algorithms [4]. The use of AI also raises ethical concerns, especially regarding privacy and transparency, as analyzing large amounts of data requires a responsible approach and proper management [5].

Conclusion. The use of artificial intelligence in cybersecurity holds great potential for fast and efficient responses to cyber threats. However, caution is needed when implementing AI, as its use is associated with certain risks in terms of security, privacy, and ethics. To achieve a high level of security, a balance must be found between automation and human oversight. In the future, AI may become one of the main tools in cybersecurity, but it is essential to ensure the transparency of its operation and adherence to ethical standards to prevent misuse and ensure effective protection.

References

1. Smith J., Jones L. Cybersecurity Threats in a Digital Age. Cybersecurity Journal. 2023. Volume 45(3), Page 134–152. DOI: https://doi.org/10.47672/ajir.1938.

2. Artificial Intelligence in Cybersecurity Market Size and Trends. *Global Market Insights*. URL – https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-ai-cyber-security-market-220634996.html#:~:text=The%20global%20Artificial%20Intelligence%20in,spans%20from%202023%20to%202028 (date of access: 20.10.2024).

3. Cooper R. Artificial Intelligence and Real-Time Threat Detection. TechPublishers. 2022. DOI: http://dx.doi.org/10.13140/RG.2.2.32615.87202.

4. Li H., Zhao W. Application of Machine Learning in Real-Time Threat Analysis. International Journal of Cybersecurity. 2022. Volume 18(2), 78–85, DOI: http://dx.doi.org/10.7753/IJCATR1309.1005.

5. IBM Watson for Cybersecurity: Real-World Applications. *IBM White Paper*. URL – https://newsroom.ibm.com/2024-08-05-ibm-introduces-new-generative-ai-powered-cybersecurity-assistant-for-threat-detection-and-response-services.

Information about the authors

Daria Drakon, student of the of Information Technology and Mathematical Modeling Department, ERI «Karazin Banking Institute», daria.drakon@student.karazin.ua

Natalya Stiahlyk, Ph.D., Head of the Department of Information Technology and Mathematical Modeling, Karazin Banking Institute, V.N. Karazin Kharkiv National University, natalia.stiahlyk@karazin.ua

Секція 1

КІБЕРГІГІЄНА: ОСНОВНІ ЗАГРОЗИ ТА ЗАСОБИ БОРОТЬБИ

Заліський В.С.
Вінницький національний технічний університет
Науковий керівник: Майданевич Л.О.

Актуальність. Ні для кого не секрет, що в кожному середовищі є загрози та небезпеки, як у реальному житті існують різні непередбачувані ситуації, мережа Інтернет також не є повністю безпечною. Глобальне поширення інформаційно-комунікативних технологій у суспільстві призвело до появи та розвитку принципово нового виду тероризму – інформаційного тероризму або кібертероризму [1]. З кожним днем тисячі користувачів стикаються як з проблемами в користуванні, так і з різними зловмисними діями, направленими на них та на інформацію, якою вони володіють. Кіберпростір сьогодні – невід'ємна частина життя всього населення. Для зручності краще уявити інтернет як окремий світ зі своїми правилами, законами та, звичайно, тими, хто їх порушує. Для цього чорні хакери вдаються до фішингу (виманювання) та соціальної інженерії (психологічні маніпуляції для доступу до інформації). Кібергігієна починається тоді, коли ми беремо телефон до рук й відмічаємо улюблену кав'ярню в постах у соціальних мережах, не задумуючись відповідаємо незнайомцям на повідомлення, або не реагуємо на те, що наші друзі чомусь пишуть нам в незвичній для себе манері [2].

Метою даної роботи є дослідження загроз в мережі Інтернет та засобів боротьби з ними.

Основні положення. Розглядаючи різні типи загроз, можна виділити ефективні методи протидії та їх усунення. Протягом довгого часу спеціалісти з кібербезпеки розробляли різні заходи та сервіси для перевірки безпеки та способи запобігання небезпек за допомогою засобів кібергігієни. Кібергігієна – це заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації [4]. Серед небезпек в мережі Інтернет основними виділяють: фішинг (виманювання інформації), BotNet, DDoS-атаки, шкідливе ПЗ, хакерські атаки, неправдива інформація, підозрілі посилання тощо. Для своєчасного виявлення небезпеки існують різноманітні методи кібергігієни та сервіси. Різноманітні сайти та ПЗ дозволяють перевіряти інші сайти, посилання, джерела інформації чи програмне забезпечення на надійність та

безпечність. Основними методами, що застосовуються для запобіганню загроз є використання антивірусного програмного забезпечення (ESET, Avast, Norton), створення складних та надійних паролів (сервіси для перевірки паролю на надійність: PasswordMonster), оновлення ПЗ, уникання відкритих мереж WiFi, перевірка посилань за допомогою спеціальних сервісів (VirusTotal, NordVPN LinkChecker, URLVoid), перевірка надійності джерела інформації, використання двофакторної аутентифікації, обережність з листами та вкладенням тощо [3]. Усі ці практики стали ключовими для зменшення ризику кіберзлочинів та підвищення захисту персональних даних.

Висновок. Кібергігієна є невід'ємною частиною життя кожного користувача Інтернету. Засоби кібергігієни допоможуть не лише безпечно використовувати цю мережу, а й запобігати витоку особистої інформації чи навіть несанкціонованому доступу до акаунтів користувача. Важливо, щоб користувачі продовжували навчатися та були обізнаними про нові загрози та способи їх нейтралізації, що сприятиме підвищенню загального рівня кібербезпеки.

Список літератури

1. Геращенко О. С. Кібертероризм як фактор загрози національній безпеці України: генеза поняття та шляхи протидії. *Південноукраїнський правничий часопис*. Одеса. 2016. №3-4. С. 39-42.
2. Кібергігієна: сучасний тренд чи комплексний підхід до розбудови системи національної кібербезпеки. *Національний кластер кібербезпеки*. URL: http://surl.li/fonxxs (дата звернення: 09.11.2024).
3. Доніч Д. Кібербезпека: актуальні загрози та методи захисту. *Lemon.School*. URL: http://surl.li/bucrfa (дата звернення: 09.11.2024).
4. Основні правила захисту даних – кібергігієна для активного Інтернет-користувача. *Eset*. URL: http://surl.li/nxyohz (дата звернення: 09.11.2024).

Відомості про авторів

Заліський Владислав Сергійович, студент кафедри захисту інформації, ВНТУ, vladzaliskiy686@gmail.com
Майданевич Леонід Олександрович, ст. викладач кафедри захисту інформації, ВНТУ, к.філос.н., lmaidanevych@ukr.net

Секція 1

ПРОБЛЕМАТИКА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ ТА КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В УКРАЇНІ

Івкова В. С.
Національний університет «Львівська політехніка»
Науковий керівник: Опірський І. Р.

Актуальність. В умовах швидкого розвитку інформаційних технологій, а також зростання цифрової взаємодії між особами, компаніями та державними структурами, забезпечення безпеки персональних даних набуває ключового значення. Необхідність захисту конфіденційної інформації посилюється через поширення кіберзагроз та кіберзлочинності, яка зумовлює ризик витоку, неправомірного доступу та використання даних. На тлі розвитку таких правових ініціатив, як GDPR в Європі та схожих законодавств у багатьох країнах світу, проблематика інформаційної безпеки стає однією з пріоритетних у наукових дослідженнях та в державній політиці [1-3].

Метою даної роботи є аналіз сучасних підходів до забезпечення безпеки персональних даних та конфіденційної інформації, вивчення загроз та вразливостей, а також визначення найефективніших методів захисту даних в умовах сучасних викликів. Дослідження спрямоване на формування рекомендацій для вдосконалення існуючих підходів до безпеки інформації на рівні організацій і користувачів.

Основні положення. Нещодавній кейс з фітнес-додатком «Strava», продемонстрував всьому світу, необхідність впровадження законодавчих та технологічних рішень щодо захисту персональних даних та конфіденційної інформації [4]. За даними французького видання «Le Monde», охоронці голів різних держав, не захищали свою активність та оприлюднили її [4]. Додаток отримав доступ до даних, які можуть розкрити наявність військових баз в усьому світі або їхнє розташування та маршрути, які військові пройшли там або навколо. Зокрема, журналістам вдалось зафіксувати пересування працівників служб охорони високопоставлених чиновників, зокрема під час професійних поїздок, можна було відстежити онлайн. На даний час, відомості про логіни, паролі, контактна інформація (сторінки в соціальних мережах, нікнейми в месенджерах, номери мобільних телефонів або адреси сервісів електронної пошти), фотографії, тощо, розміщені у відкритому доступі, не підпадають під визначення «персональні дані» або «конфіденційна інформація», зафіксовані в

національному законодавстві, а їх використання в Україні регламентоване лише політиками конфіденційності окремих електронних ресурсів, які кожен утримувач такого ресурсу визначає самостійно.

Висновки. Забезпечення безпеки персональних даних та конфіденційної інформації потребує комплексного підходу, що включає як технічні, так і організаційні та правові заходи. Важливим аспектом залишається підвищення обізнаності користувачів про загрози і методи захисту. Також перспективним напрямком є впровадження нових технологій, таких як штучний інтелект для аналізу загроз у реальному часі, і створення міжнародних стандартів для уніфікації підходів до захисту даних.

Список літератури

1. Про інформацію: Закон України від 02.10.1992 № 2657-XII: станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 17.11.2024).
2. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI: станом на 27 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 17.11.2024).
3. Загальний регламент про захист даних. *GDPR*. URL: https://gdpr-text.com/uk (дата звернення: 12.10.2024).
4. Фітнес-додаток Strava розкриває конфіденційну інформацію про своїх користувачів. *Судово-юридична газета*. URL: https://sud.ua/uk/news/obshchestvo/315235-fitnes-prilozhenie-strava-raskryvaet-konfidentsialnuyu-informatsiyu-o-svoikh-polzovatelyakh (дата звернення: 12.11.2024).

Відомості про авторів

Івкова Валерія Сергіївна, аспірантка кафедри захисту інформації Національного університету «Львівська політехніка», valeriia.s.ivkova@lpnu.ua

Опірський Іван Романович, завідувач кафедри захисту інформації, Національного університету «Львівська політехніка» д.т.н., професор, ivan.r.opirskyi@lpnu.ua

Секція 1

ФОРМУВАННЯ ТА УПРАВЛІННЯ КОМАНДАМИ НАУКОВИХ ПРОЄКТІВ З ВИКОРИСТАННЯМ МАТРИЦІ КОМПЕТЕНЦІЙ

Кириченко Д. С.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Морозова О. І.

Актуальність. Насьогодні в усьому світі дедалі більше зростає інтерес до управління проєктами (УП) як до найбільш ефективної управлінської діяльності й управлінської культури здійснення різноманітних проєктів. Наукові проєкти є основним рушієм науки у сучасних умовах розвитку науково-технічної революції. Під впливом науки тільки за останнє десятиліття відбулося істотне зрушення у співвідношенні факторів економічного росту промислово розвинених країн [1]. Успіх проєкту незмінно пов'язаний з добре сформованою, збалансованою проєктною командою, здатною виконувати всі завдання, пов’язані з проєктною діяльністю [2].

Метою роботи є дослідження фактору побудови і організації роботи команди наукового проєкту, оскільки застосування проєктного підходу в межах певної діяльності визначає необхідність формування проєктної команди, яка є одним із визначальних чинників успішності проєкту [3].

Основні положення. Складання списку всіх осіб, які беруть участь у проєкті, може стати відправною точкою у формуванні команди. Аналіз різних ролей, які люди відіграють у своїх організаціях, може привести нас до початкової групи осіб, яка стане основою для відбору в команду проєкту [2]. Ефективним інструментом для аналізу можливостей кожного окремого потенційного учасника проєктної команди є матриця компетенцій (competency matrix). Матриця компетенцій – це інструмент, який використовується для аналізу та оцінки рівнів кваліфікації окремих осіб або команд у різних проєктних компетенціях. Зазвичай вона складається з сітки або таблиці, де по одній осі перераховані компетенції, а по іншій осі – рівні кваліфікації або рейтинги. Керівники проєктів можуть використовувати цю матрицю для формування проєктної команди, обираючи кандидатів за необхідними критеріями, паралельно будуючи нову матрицю, завдяки чому можна заповнювати прогалини у вміннях та компетенціях команди, обираючи вільних кандидатів із підходящими показниками. Матриця компетенції вже готової команди може використовуватися для оцінки поточного рівня навичок членів команди,

визначення сфер, що потребують вдосконалення, та розробки цільових планів навчання або розвитку для підвищення загальної компетенції команди. Вона забезпечує візуальне представлення сильних і слабких сторін різних компетенцій, допомагаючи якісно розподіляти ресурси і покращувати загальну ефективність проєкту [4].

Висновки. Якісно сформована команда та ефективне управління нею є запорукою високо результативної роботи над науковими проєктами. Як показав аналіз, завдання формування команди має багато варіантів виконання, усі вони мають свої переваги та недоліки. Над підвищенням ефективності формування команд працюють кваліфіковані спеціалісти своєї галузі. Знайдено один з найефективніших варіантів вирішення проблеми – формування візуального представлення вмінь, навичок, та компетенцій потенційних учасників проєктної команди за допомогою матриці компетенцій. Подальший розвиток команди також ефективно здійснюється за допомогою цього інструменту. Існує нагальна потреба автоматизації процесу управління командою починаючи з етапу її формування, продовжуючи розподіленням мікро- та макро-завдань, і закінчуючи формуванням звітів.

Список літератури

1. Сусліков Л. М., Студеняк І. П. Управління науковими проектами. / Ужгородський національний університет. – Видавництво УжНУ «Говерла». URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/45073 (дата звернення 07.11.2024).
2. Dumitru Troanca. Building the project team and project ECT organization – challenges and obstacles / Lucian Blaga University of Sibiu, Romania, January 2011.
3. Євтушенко Г. І. Формування команди проєкту та організація її ефективної роботи / Східна Європа: економіка, бізнес та управління. 2019. Випуск 4(21).
4. Project Management Competency Matrix. *Bakkah*. URL – https://bakkah.com/knowledge-center/competency-matrix (дата звернення 07.11.2024).

Відомості про авторів

Кириченко Дмитро Сергійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.kirichenko@student.csn.khai.edu
Морозова Ольга Ігорівна, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, o.morozova@csn.khai.edu

Секція 1

КІБЕРБЕЗПЕКА РОЗУМНИХ БУДИНКІВ

Кіріченко Д. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Землянко Г. А.

Актуальність. Розумні будинки з інтегрованими пристроями Інтернету речей (IoT) значно підвищують комфорт і автоматизацію житлових приміщень, забезпечуючи контроль над освітленням, кліматом, безпекою та іншими системами. Кількість пристроїв IoT зростає приблизно на 18-20 відсотків на рік, і відповідний ризик кіберзагроз для приватності та безпеки також зростає [1]. Вразливості цих пристроїв, такі як недостатній захист даних, слабкі паролі та відсутність надійної автентифікації, створюють потенційні загрози для безпеки будинків. Така ситуація підкреслює важливість розробки та впровадження ефективних заходів кібербезпеки, спрямованих на захист персональних даних користувачів та мінімізацію ризику несанкціонованого доступу [2, 3].

Метою даної роботи є аналіз ризиків, загроз, вразливостей та методів захисту, що забезпечують кібербезпеку в системах розумного будинку.

Основні положення. В роботі розглядається архітектура та вразливості розумних будинків. Системи «Розумний будинок» містять мережеві пристрої, датчики та контролери, які взаємодіють через Інтернет, що підвищує ризик кіберзагроз. Основні вразливості включають слабкі паролі, недостатнє шифрування та ненадійну автентифікацію (особливо це стосується протоколів Zigbee та Z-Wave). Статистика показує, що 38% атак на пристрої IoT спричинені слабкими паролями та відсутністю двофакторної аутентифікації [2, 3]. Також в роботі представлені основні кіберзагрози для розумних будинків [2, 4]. Атаки можна розділити на: перехоплення даних, атаки на програмне забезпечення та соціальна інженерія. До атак перехоплення даних відносяться атаки на Zigbee та Z-Wave, які можуть призвести до перехоплення та фальсифікації даних. До атак на програмне забезпечення відноситься вразливості програмного забезпечення, що роблять пристрої мішенню для бот-мереж, таких як Mirai, які здійснюють DDoS-атаки. Приблизно 30% атак на домашні системи IoT успішно здійснюються з використанням методів соціальної інженерії. В роботі зазначаються наступні методи забезпечення кібербезпеки [1, 5]. Шифрування даних (наприклад, AES-256) для захисту під час передачі. Багатофакторна автентифікація для захисту віддаленого доступу.

Оновлення прошивок: Регулярні оновлення усувають відомі вразливості в Zigbee та Z-Wave. Брандмауери та фільтрація трафіку для захисту від вторгнень. Відповідність стандартам безпеки, рекомендованим Zigbee Alliance та IEEE. Відновлення після збоїв та підвищення обізнаності користувачів. Резервне копіювання, автоматичне оновлення та віддалений доступ забезпечують швидке відновлення систем у разі збою, також важливо навчити користувачів основним правилам безпеки, таким як використання унікальних паролів та оновлення програмного забезпечення [1, 5].

Висновки. Кібербезпека розумного будинку вимагає численних заходів захисту, включаючи шифрування даних, багатофакторну автентифікацію, регулярне оновлення та використання безпечних протоколів. Також важливо дотримуватися стандартів кібербезпеки і підвищувати обізнаність користувачів для захисту персональних даних і безпеки житлового простору.

Список літератури

1. Review of Smart-Home Security Using the Internet of Things / G. Vardakis et al. *Electronics*. 2024. Volume 13(16). Page 3343. DOI: https://doi.org/10.3390/electronics13163343.

2. Yin H. Wireless systems in smart home evolution and integration. *Highlights in science, engineering and technology*. 2024. Volume 111. Page 585–589. DOI: https://doi.org/10.54097/14fgga79.

3. Ehrenberg N. Smart Home Technologies: Convenience and Control. *Humane Autonomous Technology*. Cham, 2024. Page 181–198. DOI: https://doi.org/ 10.1007/978-3-031-66528-8_8.

4. Piedrahita Solorzano G.A., Flórez Gutiérrez A., Gordillo A.P. Data security threats on smart devices at home. *ARPHA conference abstracts*. 2023. Volume 6. DOI: https://doi.org/10.3897/aca.6.e106978.

5. Ansari A. M., Nazir M., Mustafa K. Smart homes app vulnerabilities, threats, and solutions: a systematic literature review. *Journal of network and systems management*. 2024. Volume 32(2). DOI: https://doi.org/10.1007/s10922-024-09803-1.

Відомості про авторів

Кіріченко Данило Володимирович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.v.kirichenko@student.csn.khai.ed

Землянко Георгій Андрійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», PhD з кібербезпеки, g.zemlynko@csn.khai.edu

Секція 1

БЕЗПЕКА ВИКОРИСТАННЯ CAPTCHA В РОЗРІЗІ РОЗВИТКУ СИСТЕМ РОЗПІЗНАВАННЯ ОБРАЗІВ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Ключник А.І.
Сумський державний університет, м. Суми, Україна
Науковий керівник: Науменко І. В.

Актуальність. Сьогодні відбувається активний розвиток систем автоматизації (ботів) та різноманітних асистентів, що дозволяють замінювати людину при виконнанні рутинних завдань. Але з поширенням використання систем штучного інтелекту постає проблема захисту від ботів, які можуть бути використані зловмисниками. Серед найпоширеніших сценаріїв є автоматизована реєстрація та підбір даних облікових записів, автоматизована розсилка повідомлень (SPAM), розповсюдження фейкової інформації, атаки на відмову в обслуговуванні (DDOS). На сьогоднішній день одним з найпоширеніших варіантів захисту є використання Captcha.

Однак зараз відбувається стрімкий розвиток систем штучного інтелекту (ШІ) на основі нейронних мереж та глибокого навчання (deep learning). Тому проблема стійкості автоматизованих тестів Тьюрінга до розв'язання за допомогою систем ШІ є дуже актуальною.

Мета. Проаналізувати стійкість автоматизованих тестів Тьюрінга (Captcha) до автоматизованого рішення за допомого різноманітних систем розпізнавання образів на базі штучного інтелекту.

Основні положення. Captcha - це повністю автоматизований тест Тьюрінга для розпізнавання роботів та людей. Ця технологія використовується для розрізнення реальних користувачів (людей) від систем автоматизації (ботів)[1]. Тести можуть бути різних форм: математичні, текстові, розпізнавання зображення. Людина здатна легко вирішити ці завдання, на відміну від бота.

Одним з найпоширініших типів Captcha є текстовий тест, який пропонує людині ввести декілька відозмінених літер або цифр, що людина бачить на зображенні. Іншим видом є графічний тест. У цьому випадку потрібно вибрати певні об'єкти на зображенні. Деякі сервіси використовують багатокрокові тести, що включають у себе комбінацію графічного тесту та аналізу поведінки користувача для виявлення систем автоматизації (ботів).

Для розпізнавання різних видів Captcha існують різноманітні реалізації нейронних мереж (CNN, RNN, YOLO), а також розширення для программ для розпізнавання текстових Captcha, такі як Fine Reader, Tesseract, Ocrad.

Стрімкий розвиток систем ШІ на основі глибокого навчання дозволяє таким системам проходити тести Тьюрінга практично не потребуючи додаткової адаптації[2]. Такі моделі, як ChatGPT, Gemini, наразі демонструють дуже високий рівень розв'язання Captcha, що інколи навіть перевершує рівень людини[3]. Також слід відмітити, що подальше збільшення складності є проблемним через зростання часу та зниження точності відповідей при проходженні тестів людиною [1].

Висновки. На даний момент розвиток нейронних мереж ШІ достатній для того, щоб вирішувати більшість графічних видів Captcha з достовірністю, що наближається до 99% [1,4]. Лише найновіши багатокрокові види тестів з аналізом поведінки користувачів мають достатньо велику складність до автоматизації та можуть бути характеризовані, як надійні. Тому для забезпечення захисту ресурсів необхідно завжди використовувати лише сучасні сервіси Captcha. Однак через стрімкий розвиток моделей ШІ та неможливість подальшого ускладнення тестів вже зараз потрібно займатись розробкою нових, більш надійних Captcha.

Список літератури

1. Searles A., Al et al. An Empirical Study & Evaluation of Modern CAPTCHAs // arXiv, 2023. DOI: 10.48550/arxiv.2307.12108

2. Biever C. ChatGPT broke the Turing test — the race is on for new ways to assess AI // Nature. 2023. №619. Page 686-689. DOI: https://doi.org/10.1038/d41586-023-02361-7.

3. Grad P. Bots are better at CAPTCHA than humans, researchers findю *Tech Xplore*. URL – https://techxplore.com/news/2023-08-bots-captcha-humans.html (дата звернення: 10.11.2024).

4. Plesner A., Votobel T., Wattenhofer R. Breaking reCAPTCHAv2. ArXiv, 2024. DOI: 10.48550/arXiv.2409.08831

Відомості про авторів

Ключник Андрій Ігорович, аспірант кафедри комп'ютерних наук, СумДУ, akluchnik.dp@gmail.com

Науменко Ігор Вікторович, начальник науково-дослідного відділу; Науково-дослідний центр ракетних військ і артилерії. к. військ. н.

Секція 1

ЗАСТОСУВАННЯ МОБІЛЬНИХ ОС У КРИТИЧНО ВАЖЛИВИХ СИСТЕМАХ

Литвинов О. А.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В.Я.

Актуальність. На даний момент у світі все переходить на керування з використанням ОС. Це приносить нові проблеми пов'язані с тим на якій саме ОС буде працювати та чи інша система. Найпоширеніші системи на так званому персональному комп'ютері Windows, Linux та її різновиди, також є macOS. Серед мобільних систем які використовують на даний час все сильно простіше: android та IOS, також нішевими є похідні дистрибутивів Linux, але вони використовуються значно рідше, android також є похідною, але все ж вважається як окрема система. Також системи поділяють по архітектурі центрального процесора x86 та ARM, не для всіх систем це має багато сенсу, бо наприклад Windows 11 працює на двох архітектурах, і може емалювати для запуску додатків протилежну архітектуру. Але в основі своїй комп'ютерні ОС працюють на першій архітектурі, а мобільні відповідно на другому типі. Але ця грань з кожним роком становиться більш розмитою. Як наслідок, компанії розглядають інтеграцію у свою систему нових ОС, включаючи мобільні, що привносить можливі проблеми з безпекою, тому перед інтеграцією, потрібно провести аналіз можливості використання ОС та її безпеку.

Мета. Метою роботи є аналіз можливості використання мобільних ОС та в цілому COTS пристроїв в критично важливих системах (КВС).

Основні положення. КВС – це комп'ютерні системи, які можуть призвести до травм, або загибелі людей у разі їх збою, або несправності, а також можуть завдати шкоди іншому обладнанню або навколишньому середовищу у разі несправності [1]. В першу чергу треба розглянути можливість загроз зараження пристроїв зловмисним ПЗ. Статистично на Android зловмисних програм на 744% більше ніж на Linux [2] який використовується як ядро у різних системах в тому ж числі критично-важливих. Частину загроз є можливість уникнути, обмеживши пристрою доступ до непотрібних для роботи сайтів та завантаження додатків. Згідно зі звітом про глобальні ризики Всесвітнього економічного форуму за 2022 рік, 95% проблем кібербезпеки пов'язані з людською помилкою [3]. Це є тривожним сигналом для всіх організацій. Тепер ці пристрої мають доступ до конфіденційних даних компанії та пряме підключення до корпоративної мережі. КВС можуть бути змішаними в випадках коли в цілому вся система не є критичною. Наприклад комерційний літак, він має управляючу

систему, та медійну, перша є КВС, а для другої сертифікування, як для першою, надмірне та затратне. Стандарти підтримують змішану критичність у випадках коли системи ізольовані одна від одної як фізично, так і логічно. Та така система повинна гарантувати що менш критична система не призведе до проблем с КВС [4].

Висновки. Проаналізовано можливість використання COTS пристроїв у КВС. Виявлено, що мобільні ОС, мають багато різних зловмисних програм. Небезпека використання мобільних ОС для контролю над критично важливими системами полягає в їх величині, що ускладнює їх сертифікацію та контроль за їх точністю. Це може призвести до помилок. COTS пристрої вже використовуються в КОС, але частіше всього вони не є мобільними ОС. COTS пристрої можуть бути лише частиною КОС, а не її цілком. Кожна система вимагає конкретних функцій, які повинні бути відлагоджені. У випадку мобільних ОС це означає додатковий час на відлагодження потрібних налаштувань.

Список літератури

1. W. Yeager, M. Leibham, J. Bartman. Safety-Critical Systems. *Web Archive* URL:https://web.archive.org/web/20201010000538/https://sites.google.com/site/cis115textbook/safety-critical-systems (дата звернення 26.10.2024).
2. Total amount of malware and PUA under Windows. *AV-ATLAS – Malware and PUA*. URL – https://portal.av-atlas.org/malware/statistics (дата звернення: 26.10.2024).
3. Зловмисне ПЗ для мобільних пристроїв у 2022 році. *КО IT для бізнесу*. URL:https://ko.com.ua/zlovmisne_pz_dlya_mobilnih_pristroyiv_u_2022_roci_142676 (дата звернення: 26.05.2024).
4. Jonsson E. Mobile Interaction with Safety Critical Systems : A feasibility study. 2015. URL: https://www.semanticscholar.org/paper/Mobile-Interaction-with-Safety-Critical-Systems-%3A-A-Jonsson/86fc8210c7da987327c96a24f87b7b4033f9a15c (дата звернення: 26.05.2024).

Відомості про авторів

Литвинов Олександр Андрійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.lytvynov@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

АНАЛІЗ ВРАЗЛИВОСТЕЙ OWASP TOP TEN ТА ЗАХИСТ ЗА ДОПОМОГОЮ БРЕНДМАУЕРУ

Лісних О. І.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Морозова О. І.

Актуальність. З ростом кіберзагроз та інтернет-економіки, вразливість веб-додатків є критичною. Зловмисники постійно шукають нові способи атак та вразливості для втручання в системи та крадіжки даних. Регулярний аналіз вразливостей, які з'являються, допомагає підвищити безпеку веб-додатків та запобігти можливим загрозам. Саме некомерційний фонд OWASP і їх списки найпопулярніших вразливостей надає можливості захистити свій додаток [1]. OWASP (Open Web Application Security Project) – це проєкт, спрямований на підвищення безпеки веб-додатків.

Метою даної роботи є аналіз вразливостей веб-додатків за результатами дослідження OWASP Top Ten та досягання надійної системи, яка може ефективно контролювати та фільтрувати мережевий трафік, запобігаючи проникненню шкідливих даних і атак за допомогою брандмауеру [2]. Брандмауери – це системи безпеки, які контролюють вхідний і вихідний мережевий трафік на основі заздалегідь визначених правил безпеки. Вони можуть бути апаратними, програмними або комбінацією обох.

Основні положення. В роботі буде проаналізовано вразливості зі списку OWASP Top Ten, серед них:

1. Порушений котроль доступу – контроль доступу застосовує політику таким чином, що користувачі не можуть діяти поза межами своїх передбачуваних дозволів [3].
2. Криптографічні збої – проблеми, пов'язані з криптографією, так як слабке шифрування [4].
3. Ін'єкції – вставка та виконання злоякісного ПЗ або коду на стороні додатку [5].

На основі аналізу вразливостей в веб-додатках, буде відображено схему, алгоритм та принцип роботи брандмауеру, який буде мати за ціль захистити додаток від найпопулярніших вразливостей. Брандмауер повинен бути здатним адаптуватися до нових загроз, забезпечувати гнучкість у налаштуванні правил безпеки та інтегруватися з іншими системами безпеки для забезпечення комплексного захисту. Основні функції брандмауера включають:

1. Фільтрація пакетів: аналіз і контроль мережевих пакетів, що проходять через брандмауер.
2. Інспекція стану: відстеження стану активних з'єднань і визначення, які пакети можуть проходити через брандмауер.
3. Захист від DDoS-атак: виявлення та блокування розподілених атак відмови в обслуговуванні.
4. VPN підтримка: забезпечення безпечного віддаленого доступу через віртуальні приватні мережі.

Висновки. Ефективний брандмауер повинен бути інтегрованим у загальну стратегію безпеки організації, забезпечуючи захист від сучасних загроз. Розробка та впровадження брандмауерів, які відповідають потребам організації, є важливим кроком у забезпеченні безпеки даних та систем. Враховуючи актуальність і постійний розвиток кіберзагроз, інвестиції в сучасні рішення для брандмауерів є необхідними для захисту бізнесу.

Список літератури

1. OWASP Top Ten. *OWASP*. URL – https://owasp.org/about (дата звернення: 05.11.2024).
2. OWASP Top Ten 2025. *OWASP*. URL – https://owasp.org/www-project-top-ten (дата звернення: 05.11.2024).
3. A1:2021 – Broken Access Control. *OWASP*. URL – https://owasp.org/Top10/A01_2021-Broken_Access_Control (дата звернення: 06.11.2024).
4. A2:2021 – Cryptographic Failures. *OWASP*. URL – https://owasp.org/Top10/A01_2021-Broken_Access_Control (дата звернення: 06.11.2024).
5. A3:2021 – Injection. *OWASP*. URL – Available at: https://owasp.org/Top10/A01_2021-Broken_Access_Control (дата звернення: 06.11.2024).

Відомості про авторів

Лісних Олександр Ігорович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.lisnykh@student.csn.khai.edu
Морозова Ольга Ігорівна, професор кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, o.morozova@khai.edu

Секція 1

АНАЛІЗ ЗАГРОЗ ПЛАТФОРМИ DOCKER В УМОВАХ СУЧАСНОЇ КОНТЕЙНЕРИЗАЦІЇ

Лобойко І. Є.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Землянко Г. А.

Актуальність. Контейнеризація стала ключовою складовою сучасних IT-систем, а Docker – однією з найпопулярніших платформ для її впровадження [1]. Контейнери Docker забезпечують однакове виконання коду незалежно від платформи, завдяки чому більшість розробників обирає їх для реалізації проектів [2].

Дослідження безпеки Docker стає особливо актуальним з ростом його популярності, що з часом буде приваблювати все більше зловмисників. Хоча в платформі Docker за час її існування було знайдено понад 37 вразливостей, головна небезпека надходить від контейнерів, вони не є ізольованими і можуть мати додаткові адміністративні привілеї [3].

Метою даної роботи є аналіз загроз платформи Docker у контексті сучасної контейнеризації. Також будуть розроблені рекомендації для підвищення рівня захисту під час використання даної платформи.

Основні положення. У рамках дослідження було виявлено кілька серйозних вразливостей платформи Docker, що безпосередньо пов’язані з її архітектурою та взаємозв'язком з хост-системою. Серед них [4]: Втеча з контейнера (CVE-2019-5736) – вразливість, що дозволяє зловмиснику перезаписати бінарний файл runc на хост-системі, отримуючи root-доступ і загрожуючи інфраструктурі. «Брудна труба» (CVE-2022-0847) – недолік у конвеєрі ядра, що дозволяє змінювати файли без доступу та підвищувати привілеї, загрожуючи конфіденційності даних. Неконтрольоване споживання ресурсів (CVE-2021-21285) – вразливість, що викликає аварійне завершення роботи демона Docker через неправильно сформований маніфест, що може призвести до відмови в обслуговуванні. Обхід каталогу (CVE-2014-9356) – вразливість, що надає доступ до чутливих файлів, загрожуючи безпеці контейнеризованих застосунків. Неправильна ініціалізація (CVE-2019-14271) – вразливість, що дозволяє ін’єкцію коду через динамічне завантаження бібліотек у середовищі chroot, підвищуючи ризик зловмисного втручання. Для запобігання вразливостям важливо слідкувати за оновленнями платформи Docker, завантажувати образи тільки з перевірених джерел і регулярно сканувати контейнери

додатковим ПЗ. Прикладом такого програмного забезпечення є Docker Bench [5]. Крім цього, слід дотримуватись наступних порад: уникати використання користувача root, обмежувати системні ресурси та kernel capabilities, а також налаштувати мінімальне середовище, щоб зменшити вектор атаки.

Висновки. Головна загроза при використанні Docker надходить від контейнерів, тому варто вживати заходів для забезпечення їх безпеки, зокрема використовувати непривілейованих користувачів, налаштувати мінімальне середовище та сканувати контейнери на наявність вразливостей або помилок конфігурації. Крім цього, можна вимкнути icc (inter-container connectivity) або запускати контейнери з read-only файловою системою.

Список літератури

1. Best Container Engine Software. *G2*. URL – https://www.g2.com/categories/container-engine (дата звернення: 31.10.2024).
2. Docker's 2024 State of Application Development Report Highlights Key Trends for Developers. *ADTmag*. URL – https://adtmag.com/Articles/2024/06/12/Docker-2024-State-of-AppDev-Report.aspx (дата звернення: 31.10.2024).
3. Docker Docker security vulnerabilities, CVEs, versions and CVE reports. *CVE security vulnerability database*. URL – https://www.cvedetails.com/product/28125/Docker-Docker.html?vendor_id=13534 (дата звернення: 31.10.2024).
4. Top 5 docker security vulnerabilities in 2023. *Snyk*. URL – https://snyk.io/learn/docker-security/top-5-vulnerabilities (дата звернення: 31.10.2024).
5. Docker Bench for Security. GitHub. URL: https://github.com/docker/docker-bench-security (дата звернення: 31.10.2024).

Відомості про авторів

Лобойко Ілля Євгенович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.loboiko@student.csn.khai.edu
Землянко Георгій Андрійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», PhD з кібербезпеки, g.zemlynko@csn.khai.edu

Секція 1

ПОГЛИБЛЕНИЙ АНАЛІЗ МЕТОДІВ ТЕХНІЧНОГО OSINT ТА RECON ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ

Луговцов Д. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Шостак А. В.

Актуальність. В умовах експоненційного зростання кіберзагроз та ускладнення векторів атак, методологія технічного OSINT (Open Source Intelligence) та Recon (reconnaissance) набуває критичного значення для проактивного виявлення вразливостей в інформаційних системах [1]. Інтеграція цих методів створює комплексний підхід до розвідки загроз, що дозволяє організаціям випереджати потенційні атаки та зміцнювати свою кібер стійкість у динамічному середовищі загроз.

Метою даної роботи є дослідження сучасних методів технічного OSINT та Recon для ефективного виявлення вразливостей інформаційних систем і мереж.

Основні положення. Технічний OSINT (Open-Source Intelligence) та Recon (Reconnaissance) є ключовими інструментами кібербезпеки, які дозволяють виявляти слабкі місця у системах на основі загальнодоступної інформації. OSINT передбачає збір даних з відкритих джерел (доменні записи, субдомени, IP-адреси, тощо), а Recon дозволяє глибше оцінити цільову систему, забезпечуючи проактивний підхід до захисту інфраструктури [2]. Одним із основних методів у технічному OSINT є «воронка»: процес починається із широкого збору даних, які потім проходять фільтрацію та аналіз для виділення найбільш релевантної інформації [3]. Такий підхід дає змогу зосередитися на критичних точках і зменшити обсяг хибнопозитивних результатів. Автоматизація процесів збору та аналізу за допомогою інструментів (наприклад: Censys, Nuclei, Nmap) підвищує ефективність та швидкість, що дозволяє обробляти великі обсяги інформації і зменшує ризик людських помилок. Інтеграція результатів OSINT та Recon у загальну стратегію кібербезпеки організації дозволяє не тільки захищати внутрішню інфраструктуру, а й здійснювати зовнішній моніторинг, що значно посилює захист від потенційних атак.

Висновки. Поглиблене застосування методів технічного OSINT та Recon дозволяє значно підвищити ефективність процесу виявлення вразливостей. Важливо впроваджувати систематичний підхід до

використання цих інструментів для створення більш безпечного середовища.

Список літератури

1. Open-Source Intelligence (OSINT) Report. *Vercara*. URL – https://vercara.com/resources/vercaras-open-source-intelligence-osint-report-november-1-november-7-2024 (дата звернення: 10.10.2024).
2. Главацька А., Ангельська О., Опірський І. Дослідження технології використання OSINT як нової загрози з деанонімізації особи в інтернет просторі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», Том 1(25), С. 19-50. DOI: https://doi.org/10.28925/2663-4023.2024.25.1950.
3. Mukhopadhyay A., Luther K. OSINT Clinic: Co-designing AI-Augmented Collaborative OSINT Investigations for Vulnerability Assessment. 2024. DOI: https://doi.org/10.48550/arXiv.2409.11672.

Відомості про авторів

Луговцов Денис Васильович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.v.luhovtsov@student.csn.khai.edu
Шостак Анатолій Васильович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., доцент, a.shostak@csn.khai.edu

Секція 1

АНАЛІЗ ПРИХОВАНОЇ ТЕХНІКИ ПЕРЕДАЧІ ДАНИХ МЕРЕЖЕЮ ЧЕРЕЗ DNS ТУНЕЛЮВАННЯ

Марценюк А. В.
Хмельницький національний університет
Науковий керівник: Регіда П. Г.

Актуальність. В контексті серверної та мережевої інфраструктури, одним із головних критеріїв побудови є впровадження безпечних практик, що можуть ускладнити фазу проникнення та постексплуатації інфраструктури. Проблема DNS тунелювання є достатньо поширеним недоліком мереж, що відноситься переважно до фази постексплуатації. Даний інструмент досить часто використовується зловмисниками з метою успішного пропускання трафіку повз забороняючі правила списків доступу та брандмауерів до точок контролю і керування (C2). Таким чином можна виділити те, що нехтування протидією до цього механізму може призвести до вразливостей безпеки, що є неприпустимим у поточних реаліях.

Метою є дослідження та аналіз техніки DNS тунелювання, ідентифікація основних критеріїв передачі даного типу трафіку. Також варто оцінити вплив цієї техніки на безпеку мережі.

Основні положення. DNS тунелювання – це техніка прихованої передачі даних через протокол DNS, при якій зловмисники використовують DNS-запити та відповіді для передачі мережевого трафіку, обходячи мережеві фільтри та міжмережеві екрани [1]. Цей метод часто використовується для отримання доступу до внутрішніх мереж, викрадення даних або управління шкідливим програмним забезпеченням. Згідно тому як протокол DNS (Domain Name System) визначений стандартом RFC – за замовчуванням це протокол, що призначений для трансляції (відображення) доменних імен у IP-адреси, відповідно до стандарту RFC 1034 та RFC 1035 [2]. Мережевий протокол DNS, початково був розроблений для ефективної і швидкої трансляції доменних імен у IP-адреси, але водночас із цим не передбачає вбудованих механізмів для аутентифікації, шифрування даних, а також перевірки цілісності даних [3]. Зазвичай найбільшу загрозу дана вразливість несе саме для приватних, невеликого та середнього розміру мереж. В більшості випадків це пов’язано саме із обмеженими ресурсами на складні технічні рішення моніторингу та виявлення мережевих аномалій [4], виявлення загроз та відсутність глибокого аналізу мережевого трафіку. Однією із ключових

проблем є те, що невдало налаштовані правила доступу дозволяють необмежений вихідний трафік на UDP порт 53 для будь-якого зовнішнього DNS-сервера. Таким чином, будь-яке програмне забезпечення з внутрішньої сторони мережі може здійснювати запити до публічних DNS-серверів без обмежень, надсилаючи в них інкапсульоване в запит «корисне навантаження», що переважно використовується для фази постексплуатації, для експортування конфіденційної інформації, управління зловмисним програмним забезпеченням (C2-канали), та обходу існуючих мережевих фільтрів для підтримання прихованого доступу до внутрішніх систем.

Висновки. DNS тунелювання є серйозною загрозою для сучасної мережевої безпеки, особливо в контексті малих та середніх підприємств. В умовах сучасних реалій нехтування заходами безпеки в контексті захисту DNS може призвести до значних втрат та компрометації даних, що є неприпустимим для організацій, які прагнуть забезпечити надійну мережеву безпеку.

Список літератури

1. RFC 5395: domain name system (DNS) IANA considerations. IETF Datatracker. URL: https://datatracker.ietf.org/doc/html/rfc5395 (дата звернення: 10.11.2024).
2. What is DNS Tunneling? *Akamai Glossary*. URL – https://www.akamai.com/glossary/what-is-dns-tunneling (дата звернення: 10.11.2024).
3. DNS Security. *ResearchGate*. URL: https://www.researchgate.net/publication/2586443_DNS_security (дата звернення: 10.11.2024).
4. Inuwa M, Das R. A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks. Internet of Things. 2024. P. 101162. DOI: https://doi.org/10.1016/j.iot.2024.101162.

Відомості про авторів

Марценюк Андрій Володимирович, студент кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет, andry.martsenyk@gmail.com
Регіда Павло Геннадійович, старший викладач кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет, pavlo.rehida@gmail.com

Секція 1

РОЗРОБКА СИСТЕМИ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ДЛЯ КОРПОРАТИВНОЇ МЕРЕЖІ

Мищенко М. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Піскачов О. І.

Актуальність. Сучасні корпоративні мережі часто стають мішенню для кібератак, які можуть завдати значних збитків як фінансових, так і репутаційних. Одним із найбільш ефективних методів захисту від несанкціонованого доступу є багатофакторна автентифікація (MFA), яка використовує декілька незалежних методів перевірки автентичності користувача [1]. Використання лише одного факту автентифікації, як от пароля, є недостатньо надійним у сучасних умовах. Впровадження MFA знижує ризик зловживання обліковими записами та забезпечує більш високий рівень безпеки корпоративних даних.

Мета. Ця доповідь присвячена дослідженню та розробці системи MFA для посилення захисту корпоративної мережі. Розглянуто сучасні методи MFA, їхню ефективність проти кібератак та практичні аспекти впровадження в корпоративному середовищі. Зосереджено увагу на аналізі загроз, виборі оптимальних методів автентифікації та рекомендаціях щодо інтеграції MFA з мінімізацією впливу на зручність користування для працівників.

Основні положення. MFA визначається як метод автентифікації, що використовує два або більше незалежних факторів для підтвердження особи користувача [2]. Ці фактори можуть включати те, що користувач знає (наприклад, пароль або PIN-код), те, що користувач має (наприклад, смартфон, токен, смарт-картку) та те, що користувач є (біометричні дані, такі як відбитки пальців або розпізнавання обличчя). MFA має ряд переваг, серед яких підвищений рівень безпеки, оскільки додаткові фактори значно ускладнюють несанкціонований доступ; захист від фішингу, оскільки навіть якщо зловмисник отримає пароль користувача, інші фактори залишаться недоступними; і відповідність регулятивним вимогам, адже багато галузей вимагають впровадження MFA для дотримання стандартів безпеки. Етапи впровадження системи MFA включають аналіз поточної інфраструктури, вибір оптимальних методів автентифікації для користувачів компанії, інтеграцію з існуючими системами управління доступом, навчання персоналу принципам роботи

MFA та постійний моніторинг ефективності системи [3]. Для успішного впровадження MFA потрібно налаштувати зручні методи автентифікації для мінімізації незручностей для користувачів, забезпечити технічну підтримку та резервні методи автентифікації, а також обережно поводитися з біометричними даними та іншою чутливою інформацією.

Висновок. Розробка та впровадження систем багатофакторної автентифікації є критично важливим кроком для забезпечення безпеки корпоративної мережі. Використання декількох факторів автентифікації значно знижує ризики, пов'язані з компрометацією облікових записів та несанкціонованим доступом до конфіденційної інформації. Хоча процес впровадження може бути складним і вимагати значних ресурсів, переваги, що надає така система, роблять її необхідною для сучасних підприємств. Постійний моніторинг, навчання користувачів та оновлення системи є ключовими аспектами для підтримки високого рівня безпеки у довгостроковій перспективі.

Список літератури

1. Сердюков Д. В., Сидоренко З. В. Багатофакторна автентифікація користувачів мобільних пристроїв у корпоративних мережах. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/865b80bc-9adb-437c-9f29-05afa55ee869/content (дата звернення: 02.09.2024).
2. Впровадження систем багатофакторної аутентифікації. *TechExpert IT Company*. URL: https://techexpert.ua/implementation-of-mfa-systems (дата звернення: 04.09.2024).
3. Організація двофакторної автентифікації для сервера OpenVPN. *TechExpert IT Company*. URL: https://techexpert.ua/2fa-for-open-vpn-server (дата звернення: 04.09.24).

Відомості про авторів

Мищенко Максим Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.myshchenko@student.csn.khai.edu
Піскачов Олександр Іванович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., с.н.с., a.piskachev@csn.khai.edu

Секція 2

ДОСЛІДЖЕННЯ ТА РОЗРОБКА СИСТЕМИ КЕРУВАННЯ КЛІМАТ-КОНТРОЛЕМ РОЗУМНОГО БУДИНКУ

Моїсеєнко Д. Д.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Желтухін О. В.

Актуальність. Показники якості повітря є дуже важливими як у повсякденному перебуванню людини, так і в ситуаціях які спричинені виробничім процесом, спеціальними умовами перебування в медичних закладах, а також у випадках спричинених військовими умовами.

Мета та задачі дослідження. Мета роботи полягає в розробці інтелектуальної підсистеми керування контролем «Розумного будинку» повинен вміти розпізнавати конкретні ситуації, що відбуваються в будівлі, і відповідним чином на них реагувати. Одна з систем може управляти поведінкою інших по заздалегідь виробленим алгоритмам. Основною особливістю інтелектуальної будівлі є об'єднання окремих підсистем в єдиний керований комплекс. Важливою особливістю і властивістю «розумного будинку», яка відрізняє його від інших способів організації життєвого простору, є те, що це найбільш прогресивна концепція взаємодії людини з житловим простором, коли людина однією командою задає бажану обстановку, а вже автоматика відстежує режими роботи всіх інженерних систем і електроприладів [1]. Система клімат-контролю працює на підставі закладених у неї алгоритмів, що дозволяють підтримувати встановлені параметри повітря серед і різних кліматичних зон в приміщеннях при мінімальних затратах енергоресурсів. Система дозволяє забезпечувати виконання різних операцій. З її допомогою проводиться нагрів або охолодження. При цьому виключається одночасна робота кондиціонера і системи опалення. Винятком може бути наявність теплої підлоги, що підтримує встановлену температуру в нижній частині кондиціонованого приміщення [2].

Методи дослідження. Згідно стратегії державної екологічної політики України визначеної на період до 2030 року, яка була затверджена Законом України від 28 лютого 2019 року № 2697-VIII, у розділі I «Існуючі проблеми та сучасний стан довкілля в Україні» зазначено, що забруднення атмосферного повітря є однією з найгостріших екологічних проблем, а розділ III містить стратегічні цілі та завдання, що безпосередньо пов'язані з управлінням якістю атмосферного повітря [3].

У роботі представлені матеріали по розробці спеціальної системи для моніторингу якості повітря [4]. Ця система отримала назву AQS, що трактується як наземна цифрова сенсорна система якості повітря. Ця платформа представлена апаратною і програмною реалізацією, що забезпечує використання недорогого пристрою для отримання даних про навколишнє середовище. До показників контролю віднесені концентрації газів: CO, CO2, NH3 та NO2, а також температура і вологість повітря.

Висновки. Розробка інтелектуальної системи контролю клімат контролю приватного приміщення, здатної забезпечити оптимальні умови забезпечення життєдіяльності людини і житлових та промислових приміщеннях за рахунок розумного керування системою обігріву, кондиціонування та очищення повітря у приміщенні і ощадливого використання енергоресурсів є важливою задачею для країни. Це дозволить заощадити електрику у межах України і підвищить індекс якості життя людей.

Список літератури

1. Patrascu M. Integrating Services and Agents for Control and Monitoring:Managing Emergencies in Smart Buildings. Service Orientation in Holonic and Multi-Agent Manufacturing and Robotics. / Patrascu., 2014. Page 544. DOI: https://doi.org/10.1007/978-3-319-04735-5_14.

2. ВООЗ вперше за 15 років посилила рекомендації щодо якості повітря. *Meduza*. URL: https://meduza.io/feature/2021/09/25/voz-vpervye-za-15-let-uzhestochila-rekomendatsii-po-kachestvu-vozduha (дата звернення: 23.10.2024).

3. Ангурець О., Хазан П., Колесникова К. Управління якістю атмосферного повітря: від концепції до впровадження: Звіт за результатами досліджень / у редакції М. Сороки. Прага-Київ: Arnika, 2021. С. 52. ISBN 978-80-87651-99-5.

4. Mustapha Si Tayeb, Mohamed Anis Benallal, Mohammed Salim Benabadji, Amine Houari «IoT monitoring system for air quality assessment and collecting data», Indonesian J Elec Eng & Comp Sci. 2022. Volume 28(3). Page 1592–1600. DOI: 10.11591/ijeecs.v28.i3.pp1592-1600.

Відомості про авторів

Моїсеєнко Денис Дмитрович, магістрант кафедри інформаційно-комунікаційних технологій імені О.О. Зеленського, НАКУ «ХАІ»

Желтухін Олександр Васильович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.zheltukhin@csn.khai.edu

Секція 1

АНАЛІЗ ПРИКЛАДНОГО ЗАСТОСУВАННЯ МЕТОДУ НЕЙРОМЕРЕЖЕВОГО ВИЯВЛЕННЯ ПОЛІТИЧНОЇ ПРОПАГАНДИ В ІНТЕРНЕТ-ДЖЕРЕЛАХ

Молчанова М. О.
Хмельницький національний університет
Науковий керівник: Бармак О. В.

Актуальність. Політична пропаганда є невід'ємним складником інформаційних кіберманіпуляцій і охоплює різні форми, методи та засоби впливу на людей, спрямовані на зміну їхніх психологічних настроїв у бажаному напрямі, тому своєчасне її виявлення залишається важливим завданням для інформаційних технологій [1]. Такі маніпулятивні дії часто використовуються для зміни суспільного психологічного клімату, мобілізації підтримки або дискредитації опонентів.

Метою роботи є аналіз прикладного застосування методу нейромережевого виявлення політичної пропаганди в інтернет-джерелах.

Основні положення. Метод виявлення політичної пропаганди в інтернет-контенті нейромережевими засобами обробки природної мови спрямований на ідентифікацію та аналіз контенту з можливими пропагандистськими чи маніпулятивними ознаками, який поширюється в Інтернеті [2]. Вхідними даними методу виявлення політичної пропаганди в інтернет-контенті є ансамбль навчених моделей рекурентних нейронних мереж з токенізаторами, і текст для аналізу. На першому кроці відбувається вибір і завантаження ансамблю RNN-моделей, а також їх токенізаторів. Наступним кроком здійснюється попередня обробка користувацького допису для аналізу, що включає в себе перетворення тексту у нижній регістр, видалення стоп-спів тощо. Далі попередньо оброблений текст перетворюється у числа, які будуть подані нейронним мережам на вхід для класифікації. Далі відбувається аналіз допису на наявність пропаганди, що включає одержання відсоткових показників наявності пропаганди за аналізом кожною RNN-моделлю. На наступному кроці здійснюється формування висновку стосовно наявності пропаганди. Пропонується використати два підходи – бінарний (стекінг) та дискретний (беггінг). Для бінарного підходу для визначення рівня пропаганди для нейромереж ансамблю отримуються бінарні оцінки. У дискретному підході оцінка нейромереж береться як дискретна величина з проміжку. Відповідно до вищевикладеного матеріалу, результатом роботи запропонованого методу

є відсоткова оцінка і відповідний рівень наявності пропаганди як за кожною RNN-моделлю ансамбля, а також відсоткова оцінка і узагальнені рівень наявності пропаганди у досліджуваному інтернет-контенті. Для оцінки ефективності розробленого методу було створено його програмну реалізацію мовою Python [3].

Висновки. Запропоновано і практично реалізовано метод виявлення політичної пропаганди в інтернет-джерелах, який працює з текстами українською мовою довжиною від 200-6300 символів, однак для коротших або довших текстів продуктивність погіршується. Згідно одержаних даних, запропонований метод здатний визначати політичну кіберпропаганду з показниками Acuracy 0.97, Precision 0.973, Recall 0.981 і F1 0.976 при застосуванні беггінга, та Acuracy 0.95, Precision 0.977, Recall 0.987 та F1 0.981 при застосуванні стекінга. Подальші дослідження будуть спрямовані на аналіз залежності розглянутих показників ефективності методу від ознак та параметрів аналізованого допису, таких як жанр, розмір і тематика.

Список літератури

1. Молчанова М.О., Залуцька О.О., Бармак О.В. Метод інтелектуального аналізу тональності текстів. Матеріали XII Всеукраїнської науково-практичної конференції «Глушковські читання». Київ – 2023. С. 113-116.
2. Молчанова М.О. Метод виявлення та класифікації технік пропаганди у текстовому контенті засобами штучного інтелекту. Розвитки інформаційно-керуючих систем та технологій.: монографія. Львів-Торунь : Lina-Pres, 2024. С. 245-266.
3. Krak I., Didur V., Molchanova M., Mazurets O., Zalutska O., Manziuk E., Barmak O. Method for Political Propaganda Detection in Internet Content Using Recurrent Neural Network Models Ensemble. CEUR Workshop Proceedings, 2024, Volume 3806, Page 312-324. URL: https://ceur-ws.org/Vol-3806/S_36_Krak.pdf (дата звернення: 16.11.2024).

Відомості про авторів

Молчанова Марина Олексіївна, аспірантка кафедри комп'ютерних наук, Хмельницький національний університет, m.o.molchanova@gmail.com
Бармак Олександр Володимирович, завідувач кафедри комп'ютерних наук, Хмельницький національний університет, д.т.н., професор, alexander.barmak@gmail.com

Секція 1

ВПЛИВ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ НА КІБЕРБЕЗПЕКУ

Орлов Р. Р.
Приватний заклад вищої освіти «Харківський технологічний університет «ШАГ»

Актуальність. Вплив згорткових нейронних мереж (CNN) на кібербезпеку зростає в умовах швидкого розвитку технологій та зростаючої кількості кіберзагроз. CNN, завдяки своїй здатності обробляти великі обсяги даних і виявляти складні шаблони, стали важливим інструментом у виявленні аномалій, класифікації загроз та прогнозуванні атак. Їх застосування дозволяє автоматизувати процеси виявлення вторгнень, забезпечуючи більш оперативну реакцію на кіберінциденти. Однак, з іншого боку, зловмисники також почали використовувати ці технології для створення більш складних атак. Таким чином, дослідження впливу CNN на кібербезпеку є необхідним для розробки ефективних стратегій захисту та адаптації до нових викликів у сфері інформаційної безпеки.

Метою цього дослідження є вплив згорткових нейронних мереж на кібербезпеку є комплексним аналізом їхнього потенціалу у підвищенні ефективності систем захисту інформації та виявлення нових можливостей для боротьби з кіберзагрозами. Згорткові нейронні мережі, завдяки своїй здатності обробляти великі обсяги даних і виявляти складні патерни, можуть значно полегшити процес автоматизації виявлення загроз, що у свою чергу дозволяє знизити навантаження на аналітиків безпеки та підвищити швидкість реагування на інциденти.

Основні положення. Дослідження впливу згорткових нейронних мереж (CNN) на кібербезпеку включають кілька ключових аспектів. По-перше, CNN – це тип глибоких навчальних моделей, що використовуються для обробки різних даних, таких як зображення та аудіо, і їх здатність виявляти патерни робить їх потужним інструментом у сфері кібербезпеки. По-друге, завдяки своїй здатності автоматизувати процеси виявлення загроз, CNN можуть виявляти аномалії в мережевому трафіку, що дозволяє оперативніше реагувати на потенційні атаки. Крім того, ці мережі здатні адаптуватися до нових типів загроз, що робить їх ефективними у боротьбі зі зловмисним програмним забезпеченням та іншими кіберзагрозами. CNN також покращують моніторинг, забезпечуючи виявлення підозрілої активності в реальному часі, що є критично важливим для своєчасного реагування на інциденти безпеки. Однак їх використання пов’язане з

певними викликами, такими як ризики зловживання технологією зловмисниками та питання етики в обробці даних. Дослідження має на меті розробити рекомендації щодо ефективної інтеграції CNN у вже існуючі системи захисту, що включає навчання персоналу, адаптацію політик безпеки та постійне вдосконалення технологій. Загалом, результати дослідження можуть стати основою для подальших інновацій у сфері кібербезпеки, пропонуючи нові рішення для захисту інформаційних систем від швидко змінюваних загроз у цифровому світі.

Висновки. Попри численні переваги, застосування CNN також пов’язане з певними ризиками, такими як можливість зловживання технологією та етичні питання, пов'язані з обробкою даних. Це вимагає ретельного підходу до їх інтеграції в існуючі системи захисту. Розробка ефективних стратегій впровадження, навчання персоналу та адаптація політик безпеки є критично важливими для забезпечення безпеки в умовах швидко змінюваного кіберсередовища. Загалом, результати дослідження вказують на необхідність подальшого вивчення і вдосконалення використання CNN у сфері кібербезпеки, що може сприяти створенню нових інноваційних рішень та підвищенню стійкості інформаційних систем до кіберзагроз у майбутньому.

Список літератури

1. Liu, Ruishen. «Face Recognition Based on Convolutional Neural Networks». Highlights in Science, Engineering and Technology. Volume 16. November 2022. Page 32–39. DOI: http://dx.doi.org/10.54097/hset.v16i.2225.

2. Sarada, N., and K. Thirupathi Rao. «A Neural Network Architecture Using Separable Neural Networks for the Identification of «Pneumonia» in Digital Chest Radiographs». International Journal of e-Collaboration. Volume 17(1). January 2021. Page 89–100. DOI: http://dx.doi.org/10.4018/ijec.2021010106.

Відомості про автора

Орлов Роман Русланович, старший оперуповноважений управління протидії кіберзлочинам в м. Києві Департаменту кіберполіції Національної поліції України, ст. викладач кафедри інформаційних технологій Приватного закладу вищої освіти «Харківський технологічний університет «ШАГ», аспірант навчально-наукового інституту захисту інформації Державного університету інформаційно-комунікаційних технологій, romanorlov0110@gmail.com

Секція 1

РОЗВИТОК ТЕХНОЛОГІЇ FINGERPRINT І ЇЇ ЗАСТОСУВАННЯ У ВЕБ-БЕЗПЕЦІ

Ошкодер А. В.
Сумський державний університет
Науковий керівник: Любчак В. О.

Актуальність. З розвитком веб-технологій зростає потреба в точній ідентифікації користувачів для підвищення безпеки онлайн-сервісів у фінансовій сфері, електронній комерції та інших критичних платформах. Технологія Fingerprint, що дозволяє створювати унікальний цифровий відбиток на основі даних пристрою і браузера, стає важливим інструментом захисту від шахрайства і несанкціонованого доступу. Водночас її використання викликає занепокоєння щодо конфіденційності, оскільки збір такої інформації може порушувати право на приватність користувача [2].

Метою даної роботи є аналіз основних методів і технік Fingerprint, оцінка його поточного застосування у веб-безпеці та дослідження способів захисту конфіденційності користувачів при використанні даної технології.

Основні положення. Серед методів Fingerprint розглядаються ключові методи, включаючи Canvas Fingerprinting, WebGL Fingerprinting, Audio Fingerprinting та інші, які дозволяють генерувати унікальний відбиток користувача. Ці методи використовуються для аналізу різноманітних характеристик пристрою, таких як налаштування браузера, шрифти, мова, часова зона та інше, що дозволяє створити стабільний ідентифікатор [1]. Технологія Fingerprint сприяє забезпеченню захисту користувачів від фішингу, ботнет-атак та інших кіберзагроз. Вона активно використовується для протидії шахрайству в фінансових операціях, захисту від атак типу "брутфорс" і блокування підозрілого трафіку. На прикладі сучасних сервісів розглядаються сценарії застосування для захисту критичних ресурсів [1]. Конфіденційність та етичні аспекти: Використання Fingerprint для ідентифікації без згоди користувачів викликає серйозні питання щодо приватності. Законодавчі ініціативи, такі як GDPR та CCPA, регулюють збирання та зберігання персональних даних. Деякі браузери та розширення, такі як Privacy Badger, надають можливість захисту від Fingerprint, блокуючи його основні механізми [1]. Баланс між безпекою та конфіденційністю: Технології Fingerprint повинні використовуватися з дотриманням прав на приватність та відповідальним підходом до збору

інформації. Застосування захисних заходів, таких як псевдонімізація даних, може зменшити ризики втрати приватності.

Висновки. Технологія Fingerprint є важливим інструментом у забезпеченні веб-безпеки, проте її використання повинно супроводжуватися обмеженнями і дотриманням принципів конфіденційності. Це вимагає співпраці розробників, законодавців і громадськості для створення стандартів, які забезпечують як безпеку, так і приватність користувачів.

Список літератури

1. Laperdrix P., Rudametkin W., Baudry B. Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints. *2016 IEEE Symposium on Security and Privacy (SP)*. 2016. Page 878–882. DOI: https://doi.org/10.1109/SP.2016.57

2. Zhang D., Zhang J., Bu Y., Chen B., Sun C., Wang T. A Survey of Browser Fingerprint Research and Application. *Wireless Communications and Mobile Computing*. Volume 2022. 2022. Page 4 – 8. DOI: https://doi.org/10.1155/2022/3363335.

Відомості про авторів

Ошкодер Анна Вікторівна, студентка кафедри кібербезпеки, СумДУ, oshkoder.anna@student.sumdu.edu.ua

Любчак Володимир Олександрович, завідувач кафедри кібербезпеки, СумДУ, к.ф.-м.н., доцент, v.liubchak@dcs.sumdu.edu.ua

Секція 1

ДОСЛІДЖЕННЯ КІБЕРРИЗИКІВ ТА РОЗРОБЛЕННЯ СТРАТЕГІЙ ЗАХИСТУ КРИПТОВАЛЮТНИХ ТРЕЙДЕРІВ З УРАХУВАННЯМ РЕГУЛЯТОРНИХ ВИМОГ

Пархоменко Є. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Морозова О. І.

Актуальність. Сьогодні захист криптовалютних інвесторів та трейдерів від кібер-ризиків є важливим аспектом безпеки у фінансовому та цифровому просторі. З розвитком ринку криптовалют зросла кількість кіберзагроз, таких як фішингові атаки, шкідливе програмне забезпечення та атаки на криптовалютні біржі. Ці ризики не тільки створюють загрозу втрати активів для інвесторів, але й порушують регуляторні вимоги, встановлені для безпеки ринку, такі як «Anti Money Laundering» (AML, «боротьба з відмиванням грошей») та «Know Your Customer» (KYC, «знай свого клієнта»). Тому існує нагальна потреба у застосуванні стратегій хеджування, які б гарантували безпеку активів інвесторів та відповідали останнім регуляторним стандартам [1, 2].

Мета роботи. Метою цієї роботи є аналіз основних кіберризиків, з якими стикаються криптовалютні трейдери та розробка комплексної стратегії захисту, що відповідає регуляторним вимогам та забезпечує безпечне середовище для трейдерів.

Основні положення. Розглянемо основні кіберризики, пов'язані з криптовалютними трейдерами та біржами. Фішинг – метод, спрямований на отримання доступу до конфіденційної інформації інвесторів через підроблені веб-сайти та повідомлення. Шкідливе програмне забезпечення – комп'ютерні програми, які крадуть особисту інформацію або фінансові активи. 51 атака – ситуація, коли одна група або невелика кількість користувачів може взяти під контроль мережу блокчейн і модифікувати дані блокчейну. Крадіжка біржових активів – коли інвестори втрачають свої активи через злом криптовалютних бірж [2, 3].

Також проаналізовано вимоги регуляторів щодо підвищення безпеки. Принципи KYC – вимоги до інвесторів підтверджувати свою особу для запобігання шахрайству. AML – стандарти боротьби з відмиванням грошей, які зменшують можливість незаконного використання криптовалют. Захист персональних даних – дотримання законодавства про захист персональних

даних, зокрема вимог General Data Protection Regulation (GDPR, загальний регламент про захист даних).

Ключовим елементом цього дослідження є розроблення особливо ефективних стратегій захисту. Використання апаратних гаманців для безпечного зберігання криптовалют. Багаторівнева аутентифікація – додатковий рівень захисту облікового запису. Регулярний аудит бірж і торгових платформ для виявлення та усунення можливих вразливостей.

Висновки. У дослідженні було проаналізовано основні кіберризики в секторі торгівлі криптовалютами та розроблено стратегію захисту на основі регуляторних вимог. Проаналізовано основні типи атак, що загрожують безпеці трейдерів, та методи захисту для мінімізації цих ризиків. Було виявлено, що використання комплексних підходів до безпеки, таких як апаратні гаманці та багаторівнева автентифікація, є важливими для захисту активів. Впровадження цих рекомендацій сприятиме підвищенню безпеки криптовалютного ринку та зміцненню довіри інвесторів.

Список літератури

1. Researching cyber risks. *StackExchange*. URL – https://security.stackexchange.com/search?q=Researching+cyber+risks (дата звернення: 09.11.2024).

2. Developing a Crypto Trading Strategy: A Beginner's Guide. *Openware*. URL – https://www.openware.com/news/articles/developing-a-crypto-trading-strategy-a-beginners-guide (дата звернення: 10.11.2024).

3. There’s No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. *Semantic scholar*. URL – https://www.semanticscholar.org/paper/There%27s-No-Free-Lunch%2C-Even-Using-Bitcoin%3A-Tracking-Vasek-Moore/c102f5dbb4e3bbbcca3d36583fde14caf2212931 (дата звернення: 10.11.2024).

Відомості про авторів

Пархоменко Євген Олександрович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.parkhomenko@student.csn.khai.edu

Морозова Ольга Ігорівна, професор кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, o.morozova@khai.edu

Секція 1

БЕЗПЕКА СМАРТ-КОНТРАКТІВ У БЛОКЧЕЙН-ОРІЄНТОВАНИХ БАЗАХ ДАНИХ

Петрів П. П.
Національний університет «Львівська політехніка»
Науковий керівник: Василишин Я. І.

Актуальність. З розвитком блокчейн-технологій, рівень їх інтеграції в бізнес-процеси істотно зріс [1]. Це призвело до стрімкого збільшення використання смарт-контрактів у децентралізованих базах даних. Смарт-контракт – це програмний код, який автоматично виконує визначені умови та зберігається у блокчейні, що забезпечує його незмінність та прозорість виконання [2]. Попередні дослідження в області блокчейн технологій, зокрема в контексті SSO (Single Sign-On) та блокчейн-логування, показали необхідність розробки комплексного підходу до безпеки децентралізованих баз даних [3, 4]. Серед усіх блокчейн-платформ, 43% ринку займає Ethereum зі своєю екосистемою смарт-контрактів, станом на 2023 рік. На другому місці знаходиться Binance Smart Chain з 28% ринку, що демонструє зростаючий попит на технологію смарт-контрактів [5]. Однак, через зріст популярності цієї технології, дана галузь привернула увагу зловмисників, які намагаються експлуатувати вразливості у смарт-контрактах. За даними компанії CipherTrace, 50% нових смарт-контрактів містять потенційні вразливості, що можуть бути використані для атак, а середній час від розгортання вразливого смарт-контракту до першої спроби його експлуатації становить менше 24 годин [5].

Метою дослідження є підвищення рівня безпеки децентралізованих баз даних шляхом розробки комплексного підходу до захисту смарт-контрактів, що включає методи виявлення вразливостей, механізми автоматизованої верифікації та рекомендації щодо безпечної імплементації.

Основні положення. Для своєчасного виявлення вразливостей у смарт-контрактах використовуються два типи аналізу: статичний та динамічний. Серед інструментів статичного аналізу ефективним є Mythril, що перевіряє смарт-контракти на наявність типових вразливостей згідно бази SWC (Smart Contract Weakness Classification). При перевірці смарт-контрактів, інструмент аналізує логіку виконання, доступ до даних та можливі вектори атак. В контексті розробки методології побудови децентралізованих баз даних запропоновано архітектурний підхід, який інтегрує механізми безпеки смарт-контрактів з існуючими рішеннями SSO та блокчейн-

логування [3, 4]. Окрім статичного аналізу, використовується динамічний аналіз за допомогою інструменту Echidna, який генерує тестові сценарії для виявлення потенційних вразливостей під час виконання смарт-контракту [2].

Висновки. Технологія смарт-контрактів є важливою складовою сучасних блокчейн-систем та має вбудовані механізми безпеки. Однак, більшість розробників не приділяють достатньої уваги безпечній розробці смарт-контрактів через складність технології та брак спеціалізованих знань. Запропоновані методологічні рішення щодо безпечної інтеграції смарт-контрактів стануть основою для подальшої розробки архітектури децентралізованих баз даних. Зменшити ризик вразливостей можна за допомогою інструментів автоматизованого аудиту та впровадження процесів безпечної розробки, проте даний метод є лише частиною комплексного підходу до безпеки і не гарантує повну захищеність смарт-контракту. Подальші дослідження будуть спрямовані на розробку методології безпечного життєвого циклу смарт-контрактів у децентралізованих базах даних.

Список літератури

1. Zheng Z., Xie S. «An overview on smart contracts: Challenges, advances and platforms». Future Generation Computer Systems. 2020. Volume 105. Page 475-491. DOI: https://doi.org/10.1016/j.future.2019.12.019.

2. Praitheeshan P., Pan L., Yu J., Liu J., Doss R. Security analysis methods on ethereum smart contract vulnerabilities: a survey. arXiv preprint. 2019. DOI: https://doi.org/10.48550/arXiv.1908.08605.

3. Saad M., Spaulding J. Overview of attack surfaces in blockchain. Blockchain for Distributed Systems Security. 2020. Page 51-66. DOI: https://doi.org/10.1002/9781119519621.ch3.

4. Chen H., Pendleton M. A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses. ACM Computing Surveys (CSUR). 2020. Volume 53(3). Page 1-43. DOI: https://doi.org/10.1145/3391195.

5. Sayeed S., Marco-Gisbert H., Caira T. «Smart Contract: Attacks and Protections». IEEE Access. 2020. Volume 8. Page 24416 - 24427. DOI: https://doi.org/10.1109/ACCESS.2020.2970495.

Відомості про авторів

Петрів Петро Петрович, аспірант кафедри захисту інформації, ІКТА, Національний університет «Львівська політехніка», petro.p.petriv@lpnu.ua

Василишин Святослав Ігорович, ст. викладач кафедри захисту інформації, ІКТА, Національний університет «Львівська політехніка», PhD з кібербезпеки, sviatoslav.i.vasylyshyn@lpnu.ua

Секція 1

СПОСОБИ ТА МЕТОДИ ЗАХИСТУ ПЕРЕДАЧІ ДАНИХ В ГЛОБАЛЬНІЙ МЕРЕЖІ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ

Положий А. С.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Бабешко Є. В.

Актуальність. З розвитком цифрових технологій, передача даних у мережі стала невід'ємною частиною сучасного суспільства. Швидкий обмін інформацією, який підтримують інтернет-сервіси, мобільні додатки та хмарні технології, значно спрощує комунікацію та роботу бізнесу. Однак зростання обсягу переданих даних супроводжується підвищенням ризиків витоку, перехоплення та модифікації інформації зловмисниками. За даними Cisco, у 2022 році 41% кібератак були націлені на перехоплення конфіденційних даних під час їх передачі [1]. Це підкреслює актуальність дослідження методів захисту даних у мережах.

Метою даної роботи є аналіз способів та методів захисту передачі даних у мережі, вивчення їх переваг і недоліків, а також виявлення найбільш ефективних практик у сучасних умовах.

Основні положення. Захист передавання даних у мережі забезпечується комплексом технологій та методів, спрямованих на запобігання втрати, викривленню чи несанкціонованому доступу до інформації. Одним із ключових способів є шифрування, яке гарантує конфіденційність даних навіть у разі їх перехоплення. Використання сучасних протоколів, таких як TLS або IPsec, дозволяє зберігати цілісність і захист трафіку в мережі [2].

Аутентифікація та авторизація є важливими компонентами захисту, забезпечуючи перевірку користувача перед доступом до системи або даних. Це доповнюється брандмауерами, які обмежують небажаний трафік, і системами виявлення загроз, що аналізують підозрілу активність.

Цифрові сертифікати забезпечують надійність зв’язків між користувачами та системами, а резервне копіювання є необхідним для відновлення даних у разі кібератак.

Моніторинг і аналіз трафіку дозволяють виявляти аномалії в мережі, забезпечуючи швидке реагування на можливі загрози. Інструменти моніторингу, такі як SIEM-системи, допомагають збирати, аналізувати та

відображати дані про мережеву активність, що сприяє надійному захисту мережі [3].

Висновки. Сучасні способи захисту передачі даних забезпечують багаторівневу безпеку інформації. Найефективнішим підходом є комбінування методів шифрування, автентифікації та використання інструментів моніторингу трафіку. Проте, навіть найкращі технології не гарантують абсолютного захисту без належного адміністрування та дотримання політик безпеки. Зростаюча складність атак вимагає постійного вдосконалення методів захисту, особливо у контексті розвитку квантових обчислень та технологій. Подальшим напрямком дослідження є вивчення нових методів шифрування для забезпечення захисту даних в умовах майбутнього розвитку квантових обчислень, а також дослідження нових інструментів автоматизації та вдосконалення моніторингу мережевого трафіку.

Список літератури

1. Cisco Annual Internet Report. *Cisco*. URL – https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2022.pdf (дата звернення: 10.11.2024).
2. В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. Технології забезпечення безпеки мережевої інфраструктури. Київський університет імені Бориса Грінченка. – Київ, 2019. – 218 с.
3. А. В. Жилін, О. М. Шаповал, О. А. Успенський. Технології захисту інформації в інформаційно-телекомунікаційних системах. ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ, 2020. – 213 с.

Відомості про авторів

Положий Антон Сергійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.s.polozhyy@student.csn.khai.edu
Бабешко Євген Васильович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., доцент, e.babeshko@csn.khai.edu

Секція 1

ЗАСТОСУВАННЯ МЕТОДІВ НАВЧАННЯ З ПІДКРІПЛЕННЯМ У ТЕСТУВАННІ НА ПРОНИКНЕННЯ: ЕФЕКТИВНІСТЬ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Притула А. В.
Вінницький національний технічний університет
Науковий керівник: Куперштейн Л. М.

Актуальність. У сучасному цифровому світі кібербезпека стає все більш актуальною проблемою, оскільки збільшується кількість складних кібератак, спрямованих на критично важливі інфраструктури та інформаційні системи [1]. Вразливості у цих системах можуть призвести до серйозних наслідків, включно з витоком конфіденційних даних і порушенням операційної діяльності. Тестування на проникнення виступає одним із ключових інструментів у кібербезпеці, оскільки дає змогу виявляти потенційні загрози до того, як вони стануть критичними [3]. Із розвитком штучного інтелекту виникають нові підходи до тестування на проникнення, зокрема методи навчання з підкріпленням (Reinforcement Learning, RL), що дозволяють автоматизувати процеси та адаптуватися до швидко змінних умов і нових загроз, які з'являються в кіберпросторі [1, 2].

Метою цього дослідження є глибокий аналіз можливостей, обмежень і перспектив використання методів навчання з підкріпленням у тестуванні на проникнення. Основна увага приділяється здатності RL-алгоритмів покращувати процес виявлення вразливостей шляхом автоматизації та моделювання кібератак [2]. Окрім того, важливо виявити потенційні виклики, які виникають під час впровадження цих технологій, зокрема необхідність значних обчислювальних ресурсів, труднощі в контролюванні дій алгоритмів та можливі ризики для систем безпеки [4]. Завданням дослідження є також оцінка ефективності RL у поєднанні з іншими методами машинного навчання, що може сприяти створенню більш динамічних і надійних систем кібербезпеки.

Основні положення. Тестування на проникнення включає кілька підходів: методи «чорної», «білої» та «сірої» скриньки [3]. Кожен з них дозволяє моделювати різні сценарії атак, варіюючи від зовнішніх загроз до повного доступу до внутрішніх компонентів системи. RL-методи здатні автоматизувати ці процеси, навчаючись на основі взаємодії з середовищем і розробляючи стратегії на основі системи винагород і покарань [1]. Таким чином, агент RL може розробляти оптимальні рішення для обходу

системних захистів, що імітує поведінку реальних зловмисників. Водночас RL-алгоритми потребують значних обчислювальних ресурсів, а їхня непередбачуваність може призводити до ризиків під час тестування. Це створює додаткові виклики в реальних умовах, де необхідно дотримуватися високих стандартів безпеки [4]. Інтеграція RL з іншими методами, такими як навчання без учителя, може допомогти в створенні гібридних систем, здатних ефективно реагувати на нові та поточні загрози [2].

Висновки. Методи навчання з підкріпленням у тестуванні на проникнення мають значний потенціал для вдосконалення процесів кібербезпеки завдяки здатності алгоритмів адаптуватися до нових загроз і самонавчатися [1]. Незважаючи на це, є кілька критичних аспектів, які вимагають подальшого дослідження: складність навчання, необхідність великих обчислювальних ресурсів і ризик непередбачуваних дій. Розвиток RL у сфері кібербезпеки передбачає комплексний підхід до його впровадження, що потребує оптимізації алгоритмів і більшої прозорості у процесі прийняття рішень [4]. Подальші дослідження можуть сприяти розробці гнучких і автономних систем кібербезпеки, здатних до швидкої адаптації у мінливих умовах кіберпростору. Це допоможе підвищити рівень захисту та швидкість реагування на нові атаки, що особливо актуально в умовах зростання кількості складних загроз, таких як атаки нульового дня [2].

Список літератури

1. Толкачова А., Посувайло М-М. Тестування на проникнення з використанням глибокого навчання з підкріпленням. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2024. 17-30 с.

2. Arulkumaran K., Deisenroth M., Brundage M., Bharath A. Deep Reinforcement Learning: A Brief Survey. IEEE Signal Processing Magazine. Volume 34(6). 2017. Page 26-38. DOI: https://doi.org/10.1109/MSP.2017.2743240

3. Types of penetration testing | black box vs white box vs grey box. *Redscan*. URL – https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/ (дата звернення: 27.10.2024).

4. Olsen K., Posthuma M., Ulrich S. Certified Tester Foundation Level (CTFL) Syllabus 2018 v3.1.1. General Assembly of the ISTQB, 2019. Page 93.

Відомості про авторів

Притула Андрій Вікторович, аспірант кафедри захисту інформації, ВНТУ, andrik.pritula@gmail.com

Куперштейн Леонід Михайлович, доцент кафедри захисту інформації, ВНТУ, к.т.н., kupershtein.lm@gmail.com

Секція 1

ВИКОРИСТАННЯ МЕТОДОЛОГІЇ OSINT ДЛЯ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ ФІНАНСОВИХ СТРУКТУР

Проценко Д. І.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Кількість кібератак у світі постійно збільшується, одним з головних об'єктів для кіберзлочинців є фінансовий сектор. Це пов'язано з тим, що фінансові організації володіють великою кількістю конфіденційної інформації та значними фінансовими ресурсами, що становлять велику цінність. Застосування методів OSINT (Розвідка з відкритих джерел) допомагає суттєво знизити ризики атак, виявляючи потенційні загрози на ранніх етапах [1].

Метою роботи є аналіз використання методології OSINT для підвищення рівня кібербезпеки фінансових структур, визначення її ролі у виявленні та нейтралізації кіберзагроз, а також розробка рекомендацій щодо ефективної інтеграції OSINT у систему безпеки фінансових установ.

Основні положення. Методологія OSINT базується на використанні загальнодоступної інформації, такої як новини, дані з соціальних мереж, форуми тощо. Основною метою OSINT – аналіз та виявлення корисної інформації для кіберрозвідки, моніторингу загроз, аналізу кібератак тощо. Одними з найбільш популярних інструментів є: Maltego – платформу для аналізу даних у реальному часі, яка допомагає виявити приховані зв'язки; Shodan – для моніторингу підключених до інтернету пристроїв і відкритих портів; DarkOwl – для сканування DarkWeb на предмет витоків або підготовки атак [2].

Використання OSINT у фінансовому секторі може суттєво підвищити ефективність виявлення та запобігання кіберзагрозам, за допомогою моніторингу широкого спектру джерел, включаючи DarkWeb. Якісними прикладами роботи OSINT є: виявлення скомпрометованих облікових даних, моніторинг активності хакерських груп, ідентифікація фішингових сайтів. Виявлення таких загроз на ранньому етапі знижує ризик подальших атак, захищаючи клієнтів та репутацію компанії [3].

Незважаючи на це все, потрібно пам'ятати, що необхідно враховувати етичні та правові аспекти, пов'язані з конфіденційністю та захистом персональних даних. Наприклад, збір персональних даних без дозволу,

навіть якщо вони доступні у соцмережах, може порушувати законодавство про захист даних [4].

Висновки. OSINT є важливим компонентом сучасної системи кібербезпеки, що дозволяє фінансовим установам оперативно реагувати на загрози та мінімізувати ризики. Використання такого інструменту рекомендоване для створення повноцінного комплексу систем захисту інформації.

Список літератури

1. Rising Cyber Threats Pose Serious Concerns for Financial Stability. *International Monetary Fund*. URL – https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability (дата звернення 14.11.2024).
2. The Beginner's Guide to Open-Source Intelligence (OSINT): Techniques and Tools. *Medium*. URL – https://medium.com/@techmindxperts/the-beginners-guide-to-open-source-intelligence-osint-techniques-and-tools-6a91b9c37ee1 (дата звернення 14.11.2024).
3. How Open Source Intelligence Can Protect You From Data Leaks. *Builtin*. URL – https://builtin.com/articles/osint-protect-data-leaks (дата звернення 14.11.2024).
4. Legal and ethical considerations in OSINT investigations. *HackerAcademy*. URL – https://hackeracademy.org/legal-and-ethical-considerations-in-osint-investigations (дата звернення: 14 листопад 2024).

Відомості про авторів

Проценко Данило Ігорович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.i.protsenko@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

МЕТОДИ І ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ ДЛЯ ЗАХИСТУ ОНЛАЙН-СЕРВІСІВ ОБРОБКИ МЕДИЧНИХ ЗОБРАЖЕНЬ

Рябко І. Б.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Харченко В.С.

Актуальність. Сучасні медичні онлайн-сервіси для обробки зображень (СОЗ) полегшують діагностику, але їхній розвиток супроводжується різноманітними загрозами кібербезпеки. Недоліком відомих публікацій є те, що вони зосереджуються на окремих аспектах кібербезпеки, не пропонуючи комплексних рішень для СОЗ.

Мета роботи. Оцінювання поточних методів і технологій кібербезпеки для захисту медичних онлайн-сервісів, виявлення основних загроз, аналіз контрзаходів та розроблення рекомендацій щодо підвищення рівня безпеки СОЗ.

Основні положення. Фішинг та соціальна інженерія. Фішинг-атаки на співробітників спрямовані на отримання доступу до конфіденційної інформації та ресурсів, що може призвести до масштабних витоків даних. DDoS-атаки. DDoS-атаки ускладнюють роботу онлайн-сервісів через перенасичення запитами, що може призвести до збоїв у роботі системи або її тимчасової недоступності для користувачів [1]. Вразливості програмного забезпечення. Уразливості, такі як SQL-ін'єкції та атаки типу XSS, часто використовуються для отримання несанкціонованого доступу до конфіденційних даних у недостатньо захищених системах [2]. Недостатній контроль доступу. Недостатньо налаштовані права доступу до чутливих даних або їхня відсутність створюють ризик несанкціонованого доступу до медичних даних, що може призвести до витоків інформації. Відсутність або недостатнє шифрування даних. Незашифровані дані під час передачі між серверами та клієнтами можуть бути перехоплені зловмисниками, що становить серйозну загрозу для конфіденційності медичної інформації [2]. Далі представлено методи захисту та рекомендації щодо їх вибору. Шифрування даних. Рекомендується використовувати AES для шифрування медичних даних, з можливістю застосування стеганографії для приховування інформації. Також слід використовувати SSL/TLS для захищених з'єднань, що знижує ризик перехоплення [3]. Моніторинг мережевих аномалій. Штучний інтелект для аналізу трафіку допомагає виявляти загрози, як-от DDoS-атаки або фішинг, і забезпечує швидке

реагування [4]. Багатофакторна аутентифікація (2FA). Впровадження 2FA знижує ризик компрометації облікових записів [5]. Резервне копіювання і відновлення. Регулярне шифроване резервне копіювання та тестування відновлення знижують ризики втрати даних через кіберінциденти або технічні збої [2]. Впровадження політик доступу. Застосування принципу найменших привілеїв для доступу до даних та регулярне оновлення політик доступу знижує ризик внутрішніх загроз [5].

Висновки. Інтегровані методи захисту, такі як шифрування, стеганографія, багатофакторна аутентифікація та моніторинг загроз, знижують ймовірність витоків медичних зображень і забезпечують високий рівень кібербезпеки в онлайн-сервісах, відповідаючи міжнародним стандартам (GDPR, HIPAA).

Список літератури

1. DDoS Protection and Security Solutions. *Cloudflare*. URL – https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack (дата звернення 11.11.24).

2. National Institute of Standards and Technology (NIST). *Advanced Encryption Standard (AES)*. NIST FIPS PUB 197, Published November 26, 2001; Updated May 9, 2023.

3. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. URL – https://datatracker.ietf.org/doc/html/rfc8446 (дата звернення: 11.11.2024).

4. General Data Protection Regulation (GDPR). *GDPR*. URL – https://gdpr-info.eu (дата звернення: 11.11.2024).

5. Summary of the HIPAA Security Rule. *U.S. Department of Health and Human Services*. URL – https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (дата звернення: 11.11.2024).

Відомості про авторів

Рябко Іван Богданович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.b.ryabko@student.csn.khai.edu

Харченко Вячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, v.kharchenko@csn.khai.edu

Секція 1

ОСНОВНІ СПОСОБИ ЗАХИСТУ ВІД ФІШИНГОВИХ АТАК

Садовник Є. А.
Вінницький національний технічний університет
Науковий керівник: Майданевич Л. О.

Актуальність. Сьогодні майже чи не кожен користується мережею інтернет задля спілкування, отримання інформації та послуг. Фінансові операції, інтернет-банкінг, соціальні мережі та обмін конфіденційною інформацією стали невід'ємною частиною повсякденного життя. Але разом із цим виникає загроза особистої безпеки та викрадення даних. З розвитком технологій розвиваються також і методи зловмисників. Найбільш популярним методом викрадення інформації є фішинг. Фішинг – це зловмисна атака, під час якої шахраї видають себе за достовірні джерела з метою отримання цінної інформації [1]. Фішинг вже довгий час залишається найпоширенішим способом для кіберзлочинців через його простоту та здатність обманути навіть найдосвідченіших користувачів.

Метою даної роботи є дослідження основних способів захисту від фішингових атак.

Основні положення. Основною метою боротьби з фішингом є захист користувачів від шахрайських атак, які можуть призвести до втрати персональної інформації та фінансових витрат. Обізнаність щодо фішингових загроз і впровадження сучасних технологій безпеки мінімізує ризики крадіжки даних. Щоб захистити себе від фішингових атак потрібно виконувати певні вимоги. Перш за все, користувачам мережі інтернет потрібно усвідомити, що фішинг може бути прихований під звичайні листи чи повідомлення, знайти різницю між якими буває досить складно. Відтак, основні вимоги захисту інформації включають: Регулярне оновлення браузерів та антивірусного забезпечення (саме в браузері відбувається найбільше наших дій в мережі Інтернет, тому захист його є на першому місці). Перевірка повідомлень на достовірність також є не менш важливим аспектом захисту (фішингові листи часто містять фейкові та недостовірні посилання, які можуть виглядати як справжні; тому, насамперед, перед натисканням на посилання рекомендується перевірити адресу відправника та домен сайту). Використання двофакторної автентифікації (2FA) є необхідно дією якщо ви хочете отримати додатковий рівень захисту та зроби ваші дані менш вразливими (ця процедура вимагає не лише введення паролю, але й спеціального коду, який генерується на вашому пристрої

(Google Authenticator) або СМС на ваш мобільний номер телефону; тобто, це ускладнює доступ зловмисників до ваших даних, навіть якщо вони отримали ваш пароль). Уникайте натискання на підозрілі посилання (якщо ж ви отримали запит з терміновим введенням своїх даних, то краще перевірити цей сайт на правдивість та офіційність; також звертайте увагу на захищеність з'єднання сайту і правильність домену, щоб уникнути фейкових сайтів). Обмеження розголошення особистих даних є також дуже важливим аспектом захисту інформації (не варто передавати свої особисті дані через листи та навіть в повідомленнях месенджерів; це важливо тому, що у разі злому вашої електронної пошти або соціальної мережі у зловмисника може бути більше цінної інформації про вас); 6) ще одним ключовим аспектом фішингу є соціальний інжиніринг – метод при якому шахраї використовують психологічні фактори для маніпуляції користувачами (вони можуть здаватися офіційними компаніями чи організаціями, створюючи відчуття страху та терміновості з метою отримання особистої інформації або доступу до ваших облікових записів) [2].

Висновки. Фішингові атаки наразі є серйозною проблемою для захисту та безпеки користувачів. Важливо бути обізнаним про загрози, перевіряти повідомлення на достовірність, використовувати додатковий захист від фішингу та шкідливих сайтів. Уважність, критичне мислення та заходи кібергігієни можуть допомогти мінімізувати ризики та захистити особисті дані від шахраїв.

Список літератури

1. Фішинг – що це таке? *Fenix Industry*. URL: https://fnx.com.ua/ua/articles/publications/25 (дата звертання 12.11.2024).
2. How To Recognize and Avoid Phishing Scams. *Federal Trade Commission (FTC)*. URL – https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (дата звертання 12.11.2024).

Відомості про авторів

Садовник Євгеній Анатолійович, студент кафедри захисту інформації, ВНТУ, sadovnikevgenii@gmail.com
Майданевич Леонід Олександрович, ст. викладач кафедри захисту інформації, ВНТУ, к. філос. н., lmaidanevych@ukr.net

Секція 1

ІННОВАЦІЙНІ БЕЗСЕРВЕРНІ ХМАРНІ ОБЧИСЛЕННЯ: ОСОБЛИВОСТІ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Селіванова М. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Хмарні обчислення (ХО) без серверів (serverless computing) є однією з найсучасніших технологій, що активно впливають на розвиток хмарних сервісів. Вони дозволяють компаніям і розробникам фокусуватися на розробці та впровадженні додатків без необхідності управління інфраструктурою. Це значно знижує витрати та підвищує ефективність використання обчислювальних ресурсів. Дана технологія є критично важливою для майбутнього хмарних технологій, оскільки забезпечує гнучкість, масштабованість та спрощення процесів розробки.

Метою даної роботи є: дослідити вплив ХО без серверів на розвиток хмарних технологій, їх переваги та виклики, а також можливі перспективи розвитку цієї галузі.

Основні положення. ХО – це надання обчислювальних послуг, зокрема серверів, сховищ, баз даних, мереж, програмного забезпечення, аналітики та інтелекту – через Інтернет («хмара»), щоб запропонувати швидші інновації, гнучкі ресурси та економію за рахунок масштабу. Без серверні обчислення – це модель виконання ХО, яка дозволяє розробникам ПЗ створювати та запускати додатки та сервери без необхідності надання або керування внутрішньою інфраструктурою. Завдяки без серверному режиму хмарний постачальник піклується про все регулярне керування і обслуговування інфраструктури, включаючи оновлення ОС застосування виправлень, керування безпекою, моніторинг системи та планування можливостей [1]. Без серверні обчислення дозволяють розробникам купувати серверні послуги на гнучкій основі «оплата за використання», тобто розробники повинні платити лише за послуги, якими вони користуються. Це схоже на перехід від тарифного плану мобільного телефону з фіксованим місячним лімітом до плану, який стягує плату лише за кожен фактично використаний байт даних [2]. Провідні компанії в усьому світі використовують без серверні обчислення, щоб надавати своїм клієнтам високопродуктивні онлайн-послуги з високою доступністю. Ось деякі з відомих прикладів:

- оновлення даних у режимі реального часу від Major League Baseball Advanced Media (MLBAM);
- швидка розробка та розгортання програм Autodesk;
- масштабована доставка медіа на вимогу Netflix;
- динамічні та чуйні чат-боти від Slack;

– розумні торговельні автомати на основі IoT від Coca-Cola;
– збирання сміття IoT від GreenQ;
– прийняття клінічних рішень на основі даних за допомогою IDEXX [3].

Майбутнє ХО без серверів включає інтеграцію з штучним інтелектом для оптимізації процесів та автоматизації управління ресурсами, розширення застосування в нових галузях, таких як IoT, фінансові технології та охорона здоров'я, та розвиток екосистеми з появою нових платформ та інструментів для спрощення розробки та впровадження рішень без серверів [4].

Висновки. ХО без серверів є важливим кроком у розвитку хмарних технологій. Вони надають значні переваги в зниженні витрат, підвищенні гнучкості та прискоренні процесів розробки. Однак, існують виклики, які потребують вирішення для максимізації потенціалу цієї технології. Подальший розвиток обчислень без серверів буде впливати на всі аспекти хмарних сервісів, відкриваючи нові можливості для бізнесу та розробників.

Список літератури

1. Rosencrance L. What Is Serverless Computing? Definition from TechTarget.com. *IT Operations.* URL – https://www.techtarget.com/searchitoperations/definition/serverless-computing (дата звернення: 29.05.2024).
2. What is serverless computing? | Serverless definition. *Cloudfare*. URL – https://www.cloudflare.com/learning/serverless/what-is-serverless (дата звернення: 29.05.2024).
3. Chiradeep BasuMallick. What Is Serverless? Definition, Architecture, Examples, and Applications. *Spiceworks*. URL – https://www.spiceworks.com/tech/devops/articles/what-is-serverless/ (дата звернення: 29.05.2024).
4. Michael Maximilien, David Hadas, Angelo Danducci II, Simon Moser. The future is serverless. *IBM Developer*. URL – https://developer.ibm.com/blogs/the-future-is-serverless (дата звернення: 29.05.2024).

Відомості про авторів

Селіванова Марія Олександрівна, магістрантка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.selivanova@student.csn.khai.edu
Пєвнєв Володими Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н, доцент, v.pevnev@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ ВИНИКНЕННЯ ЛОГІЧНИХ ПОМИЛОК В РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА МЕТОДИК ЇХ ВИЯВЛЕННЯ

Семенець О. Ю.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Тецький А. Г.

Актуальність. Логічні помилки - це ситуації, коли код програміста успішно компілюється і виконується, але не генерує очікуваний результат для всіх можливих вхідних даних [1]. На відміну від синтаксичних помилок, логічна помилка не призводить до збоїв або аварійного завершення роботи програми. Однак вона може створити умови для експлуатації вразливості чи порушення безпеки. Загрози та вразливості виявляються під час життєвого циклу розробки програмного забезпечення, та інженер з кібербезпеки може за допомогою сучасних технік статичного та динамічного аналізу програм виявити їх. Ці техніки ефективні для виявлення заздалегідь відомих дефектів, але вони не достатньо охоплюють таку проблему, як виявлення логічних помилок [2].

Метою даної роботи є дослідження виникнення логічних помилок, причини їх виникнення в розробці програмного забезпечення та огляд розповсюджених методик їх виявлення.

Основні положення. Для своєчасного виявлення логічних помилок до команди розробки треба залучити інженера з кібербезпеки, який буде приймати активну участь в створені проекту на кожній фазі розробки. В цій роботі було проведено дослідження причин виникнення логічних помилок, для абстрактного огляду процеси розробки була приведена каскадна модель розробки програмного забезпечення. За допомогою цієї моделі процес розробки можна представити як серію послідовних фаз, через які проходить проєкт. Проведено дослідження з методик виявлення логічних помилок в залежності від етапу розробки та інструментів, які може використовувати інженер з кібербезпеки, в залежності від його доступу до проекту. Був проведений огляд таких інструментів як: SLA-generator, Microsoft Threat Modeling Tool та OWASP Threat Dragon [3]; SonarQube, Checkmarx та Fortify [4]; Burp Suite, OWASP ZAP (Zed Attack Proxy) і Wireshark [5].

Висновки. Виявлення логічних помилок є надзвичайно важливим, але й складним завданням, оскільки помилки часто не можуть бути виявлені

стандартними методами тестування. Інженер з кібербезпеки для їх виявлення може застосувати такі методи як статичний та динамічний аналіз, перевірку на проникнення, а також може використати такі інструменти набір інструментів в залежності від наявності доступу інженера до вихідного коду проекту. Запропоновані алгоритми та інструменти наведені в доповіді.

Список літератури

1. Ettles A., Luxton-Reilly A., Denny P. Common logic errors made by novice programmers. the 20th Australasian Computing Education Conference, Brisbane, Queensland, Australia, 30 January – 2 February 2018. New York, USA, 2018. DOI: https://doi.org/10.1145/3160489.3160493.
2. Stergiopoulos, G., Katsaros, P., Gritzalis, D. Source code profiling and classification for automated detection of logical errors. In 3rd International Seminar on Program Verification, Automated Debugging and Symbolic Computation, Germany. 2014. URL – https://www.infosec.aueb.gr/Publications/PAS-2014%20Logical%20Error.pdf (дата звернення: 30.10.2024).
3. Granata D., Rak M. Systematic analysis of automated threat modelling techniques: Comparison of open-source tools. Software Qual J 32. 2024. Page 125–16. DOI: https://doi.org/10.1007/s11219-023-09634-4
4. Alexandra de Barros Reigada. Generic SAST tool Comparer. URL – https://repositorium.sdum.uminho.pt/bitstream/1822/84173/1/Alexandra%20de%20Barros%20Reigada.pdf (дата звернення: 05.11.2024).
5. Ekene Joseph. Burp Suite vs OWASP ZAP – a Comparison series. *Medium*. URL – https://medium.com/@Ekenejoseph/burp-suite-vs-owasp-zap-a-comparison-series-8e34162c42e6 (дата звернення: 10.11.2024).

Відомості про авторів

Семенець Олександр Юрійович, аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.y.semenets@csn.khai.edu
Тецький Артем Григорович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.tetskyi@csn.khai.edu

Секція 1

КРИТИЧНИЙ АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ПІДМІНИ GNSS КООРДИНАТ

Сергєєв В.М.
Сумський державний університет
Науковий керівник: П'ятаченко В.Ю.

Актуальність. GNSS-навігація відіграє важливу роль у авіації, судноплавстві, автомобільному транспорті та вбудована у кожний смартфон. У той же час цивільна версія стандарту GPS є вразливою до подавлення та підміни координат (спуфінгу). Це викликано низьким рівнем синалу через велику відстань від супутника до приймача та малу потужність передавача та відкритістю самого стандарту. У сукупності з відсутністю аутентифікації [1] зловмисник отримує можливість виконати спуфінг-атаку та викликати підміну координат. Особливо важливим є захист від атак для автономних систем, таких як безпілотні літальні апарати. Для проведення атаки підміни координат зловмиснику не потрібне дороге обладнання – програмно-апаратні комплекси для генерації GPS сигналів доступні у відкритому продажу та є досить простими у використанні що підкреслює актуальність захисту.

Метою даної роботи є дослідження методів та механізмів виявлення атак підміни координат на навігаційну систему - GPS-spoofing.

Основні положення. Аналізуючи існуючі методи виявлення підміни координат можна виділити вирішення проблеми визначення походження сигналу – рішення на базі оптичної навігації [4] або використання ідей інерційної навігації [5]. Застосування методів машинного навчання для аналізу даних системи може покращити відсоток виявлення атак на підміну GPS координат [5]. Для своєчасного виявлення GPS-спуфігу використовуються методи машинного навчання які дозволяють виявити некоректні координати пристрою аналізуючи такі дані як позиція у просторі, швидкість, кутове прискорення. Аналізуючи цю інформацію та історію переміщень приладу можна зробити висновок про те чи поточна позиція навігатору справжня чи підмінена. Якщо система виявила спуфінг-це дозволяє користувачу вжити відповідних заходів зі свого боку. Втім реєстрація даних польоту може потребувати додаткові сенсори, що може вплинути на вагу та функціональність БПЛА. Крім того зловмисники можуть маніпулювати значеннями сили сигналу, що маскуватиме атаку під вплив умов середовища, як сила вітру чи подібні природні шумові значення. В

рамках розпізнавання втручання роботу системи класичними методами машинного навчання, як метод опорних векторів чи деревоподібні методи, визначається проблема дискретності сигналу, в рамках якої визначення атаки ускладняється довільним формуванням вектора-реалізації класу розпізнавання. Глибоке навчання, засобами рекурентної чи моделі довгої короткочасної пам'яті чи генетичного алгоритму, визначаються прогностичним характером моделей, який дозволяє порівнювати передбачений сигнал з реально зафіксованим для визначення можливих відхилень траєкторії польоту, що може свідчити про спуфінг.

Висновки. Навігація з використанням GPS є невід'ємною частиною повсякденного життя, але стандарт GPS вразливий до подавлення та атак на підміну координат. Перспективним підходом до виявлення підміни координат є використання комбінованих моделей глибокого навчання з оптимізованими обчислювальними ресурсами, що дозволить мінімізувати вплив дискретизації сигналу та зменшити обчислювальні витрати, покращуючи швидкість виявлення атак.

Список літератури

1. Humphreys, T. Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing; The University of Texas at Austin: Austin, TX, USA. 2012. Page 1–16.

2. Rustamov, A., Gogoi, N., Minetto, A., & Dovis, F. (2020). Assessment of the Vulnerability to Spoofing Attacks of GNSS Receivers Integrated in Consumer Devices. 2020 International Conference on Localization and GNSS, 2-4 June 2020, Tampere, Finland. DOI: 10.1109/ICL-GNSS49876.2020.9115489.

3. Xue, N. DeepSIM: GPS Spoofing Detection on UAVs using Satellite Imagery Matching. ACM International Conference Proceeding Series. 2020. Page 304–319. DOI: 10.1145/3427228.3427254.

4. Feng, Z., Guan, N., Lv, M., Liu, W., Deng, Q., Liu, X., & Yi, W. Efficient drone hijacking detection using two-step GA-XGBoost. Journal of Systems Architecture, 103. 2020. DOI: 10.1016/J.SYSARC.2019.101694

5. Wei, X. ConstDet: Control Semantics-Based Detection for GPS Spoofing Attacks on UAVs. Remote Sensing 2022, Volume 14, Page 5587 DOI: 10.3390/RS14215587.

Відомості про авторів

Сергєєв Віктор Михайлович, аспірант кафедри комп'ютерних наук, СумДУ, viktor.serhieiev@gm.sumdu.edu.ua

П'ятаченко Владислав Юрійович, асистент кафедри комп'ютерних наук, СумДУ, vl.piatachenko@cs.sumdu.edu.ua

Секція 1

АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ЛІТАЮЧОЇ МЕРЕЖІ З БПЛА

Сіроклин О. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Клюшніков І. М.

Актуальність. Розвиток безпілотних літальних апаратів (БпЛА) відкриває нові можливості для їхнього використання в різних сферах, таких як моніторинг навколишнього середовища, рятувальні операції та військові місії. Одним із перспективних напрямів є застосування літаючих бездротових мереж (англ. Flying Ad Hoc Network - FANET) як методу для розгортання безперервної передачі інформації між двома об’єктами [1, 2]. Це дозволяє створювати ефективні комунікаційні мережі, які здатні адаптуватися до змінних умов експлуатації, забезпечуючи надійний зв'язок між різними пристроями [3]. Однак, з розширенням застосування БпЛА та FANET виникають нові виклики, пов'язані з безпекою [4]. Кіберзагрози, такі як перехоплення, модифікація або блокування інформації, можуть суттєво зашкодити функціонуванню мережі [5]. Відсутність належних заходів безпеки може призвести до критичних наслідків, включаючи втрату даних, порушення координації дій та небезпеку для людей.

Метою даної роботи є дослідження загроз безпеки для мереж FANET. Це включає:

– аналіз критичних ресурсів FANET;

– розробку моделей загроз для визначення потенційних вразливостей та методів їх подолання;

– опис моделі порушника, яка включає типи можливих зловмисників, їхні наміри, кваліфікаційні рівні та фізичні можливості.

Основні положення. Було проведено огляд технологій для роботи літаючих мереж, що включає аналіз структурних особливостей і можливостей FANET. Розглянуто різні види підтримки заряду БпЛА, можливі типи зв'язку, вибір яких визначає швидкість і надійність передачі даних, а також вплив мережевих топологій на продуктивність FANET. Було розроблено моделі загроз і порушника, які дозволяють ідентифікувати вразливі елементи мережі. Модель загроз визначає можливі цілі та методи атак, тоді як модель порушника описує потенційних зловмисників, їхні можливості та мотиви. Результати аналізу підкреслюють необхідність використання комплексних заходів безпеки, зокрема технологічних та організаційних, для підвищення захищеності FANET.

Висновки. Результати дослідження підкреслюють важливість комплексного підходу до аналізу загроз безпеки для FANET. Розроблені моделі загроз і порушника допомагають виявити вразливі елементи мережі та прогнозувати можливі сценарії атак. Визначення критичних ресурсів, таких як конфіденційність і цілісність даних, є ключовим для розробки адекватних заходів захисту. Необхідно впроваджувати як технологічні, так і організаційні рішення, що підвищать захищеність FANET та забезпечать надійність його функціонування в умовах зростаючих кіберзагроз.

Список літератури

1. Morgenthaler S., Braun T., Zhao Z., Staub T., Anwander M. UAVNet: A mobile wireless mesh network using Unmanned Aerial Vehicles. Proceedings of the IEEE Global Communications Conference (GLOBECOM). 2012. DOI: https://doi.org/10.1109/GLOCOMW.2012.6477825.
2. Ullah H., McClean S., Nixon P., Parr G., Luo C. An Optimal UAV Deployment Algorithm for Bridging Communication. In: 2017 IEEE International Conference on Intelligent Transportation Systems (ITST). 2017. DOI: https://doi.org/10.1109/ITST.2017.7972194.
3. I. M. Kliushnikov, H. V. Fesenko, V. S. Kharchenko. Scheduling UAV fleets for the persistent operation of UAV-enabled wireless networks during NPP monitoring. Radioelectronic and computer systems. 2020. No.1 DOI: https://doi.org/10.32620/reks.2020.1.03.
4. Ozlem Ceviz, Pinar Sadioglu, Sevil Sen. A Survey of Security in UAVs and FANETs: Issues, Threats, Analysis of Attacks, and Solutions. arXiv:2306.14281v3, 2023. DOI: https://doi.org/10.48550/arXiv.2306.14281.
5. Emmanuel Asituha. A comprehensive overview of privacy, security and performance issues in flying Ad Hoc Networks. World Journal of Advanced Research and Reviews, 2024. DOI: https://doi.org/10.30574/wjarr.2024.23.1.2166.

Відомості про авторів

Сіроклин Олександр Віталійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.v.siroklyn@student.csn.khai.edu
Клюшніков Ігор Миколайович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, к.т.н., с.н.с, i.kliushnikov@csn.khai.edu

Секція 1

СТАТИСТИЧНІ МЕТОДИ ДЛЯ ВИЯВЛЕННЯ АНОМАЛЬНИХ ОБСЯГІВ АКТИВНОСТІ IP-АДРЕС ТА СЕСІЙ

Скороход А. А.
Сумський державний університет
Науковий керівник Коваль В. В.

Актуальність. Проблема нетипово великих кількостей запитів уже не нова. Яскравими прикладами слугують DoS/DDoS-атаки, спамери та інші способи отримати вигоду чи нанести шкоду за рахунок обсягу звернень до веб-ресурсу. В Україні одним із найбільш резонансних випадків є DDoS-атаки кількох державних сайтів через спробу закриття сайту ex.ua [1]. Після початку повномасштабного вторгнення росії до України, кібербезпека та інформаційна війна почали відігравати критичну роль. Але яку кількість запитів вважати нормальною? Наприклад, можна виставити поріг запитів для одного IP. Але різні сервіси мають користувачів різної активності. У таких випадках можна застосувати методи виявлення аномальних кількостей запитів.

Метою даної роботи є дослідження простих в реалізації методів виявлення аномальних кількостей IP-запитів чи дій в межах однієї сесії за допомогою базових статистичних методів.

Основні положення. Однією із правильних практик ведення веб-серверів є процес логування – автоматичні записи подій з додатковою інформацією до «лог-файлу», серед яких можна зустріти два типи: запис про кожне підключення з IP-адреси, що дає змогу порахувати їх кількість або запис про сесію. Другий тип дещо ускладнює ситуацію. Створення сесії для користувача, в рамках якої він проводить дії (необов'язково з однієї IP-адреси) є частою практикою. Кожній сесії присвоюється унікальний session ID, і уже в межах цієї сесії можна виявляти аномалії. Тобто, проаналізувавши логи та підрахувавши кількість запитів для кожної IP-адреси або кількість дій в рамках однієї сесії за певний проміжок часу, вже можна шукати нетипові показники одним із двох пропонованих статистичних понять: правило трьох сигм та інтерквартильний розмах [2].

Метод на основі правила трьох сигм. Правило трьох сигм стверджує, що у нормальному розподілі в межах двох стандартних відхилень знаходиться 68,27% значень, у межах чотирьох – 95,45% і у межах шести – 99,73%, тобто, переважна більшість. Для початку варто знайти середнє значення діапазону (μ) та стандартне відхилення (σ). За статистикою, значення, що

знаходяться за межами діапазону $[\mu - 3\sigma, \mu + 3\sigma]$ є аномальними. У контексті кібербезпеки, підозрювати можна навіть значення, що виходять за дві сігми. Перевагою такого підходу є те, що при великій кількості даних і нормальному (чи близькому до нього) розподілі, можна швидко виявити аномальну кількість і вважати відповідну IP-адресу чи сесію підозрілою. Недоліком є випадок, коли дані сильно відхиляються від нормального розподілу – в такому разі можна отримати надто багато або надто мало аномалій.

Метод на основі інтерквартильного розмаху, на відміну від попереднього методу, є більш стійким до викривлених розподілів та викидів. Для початку варто визначити перший (Q1) та третій квартилі (Q3). розрахувати інтерквартильний розмах (IQR) за формулою $IQR = Q3 - Q1$. У такому випадку, аномаліями можна вважати значення за межами діапазону $[Q1 - 1.5 * IQR, Q3 + 1.5 * IQR]$. Якщо варіативність надто значна, медіана може слугувати показником «нормальної» активності, а аномаліями можна вважати ті значення, що значно її перевищують.

Висновки. У рамках даного дослідження, було розглянуто два методи виявлення аномальної кількісної активностей. Метод на основі правила трьох сигм швидко спрацьовує на нормальному (чи близькому до нього) розподілі даних, а метод на основі інтерквартильного розмаху є більш стійким до викривлених розподілів. Методи однаково можна застосувати як для кількості IP-підключень з однієї адреси, так і для дій в межах сесії.

Список літератури

1. Українська правда. EX.UA просить більше не знущатися над сайтами влади. *Web Archive*. URL: https://web.archive.org/web/20120203050404/ http://www.pravda.com.ua/news/2012/02/1/6946167/ (дата звернення: 14.11.2024).
2. Olbrych B. Statystyka matematyczna: przykłady. Poland: Akademia Handlowa Nauk Stosowanych w Radomiu, 2023.

Відомості про авторів

Скороход Андрій Анатолійович, аспірант кафедри комп'ютерних наук, СумДУ, andrey.skorochod@gmail.com
Коваль Віталій Вікторович, ст. викладач кафедри кібербезпеки, СумДУ, v.koval@gmail.com

Секція 1

ВИЯВЛЕННЯ КІБЕРЗАЛЯКУВАНЬ В ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ ЗАСОБАМИ МАШИННОГО НАВЧАННЯ

Собко О. В.
Хмельницький національний університет
Науковий керівник: Бармак О. В.

Актуальність. Тема виявлення кіберзалякувань в інформаційному середовищі є актуальною у зв'язку з інтенсивним зростанням цифрового спілкування та постійним розширенням присутності користувачів в інтернет-просторі. Зокрема, розвиток соціальних мереж, онлайн-форумів та інших платформ для обміну інформацією створює сприятливі умови для анонімних кібератак та кіберманіпуляцій, які важко виявити та контролювати [1].

Метою даної роботи є розробка підходу до виявлення кіберзалякувань в інформаційному середовищі засобами машинного навчання.

Основні положення. Розроблено підхід до виявлення кіберзалякувань за текстовими зразками в інформаційному середовищі засобами машинного навчання. На початковому етапі вхідні дані, а саме текст для аналізу – проходить попередню обробку та векторизацію. Далі, використовуючи векторизатор та модель машинного навчання, спеціально навчену для розпізнавання кіберзалякувань, здійснюється оцінка ймовірності їх наявності в тексті. У результаті отримується висновок щодо присутності чи відсутності кіберзалякувань у аналізованому текстовому зразку. Розроблений підхід було апробовано шляхом створення програмного забезпечення, яке здатне автоматично визначати наявність кіберзалякувань у текстових повідомленнях. У даному програмному забезпечені для векторизації тексту та класифікації було використано модель BERT, яка зарекомендувала себе як ефективний інструмент для обробки природної мови. Модель була навчена на датасеті [2], який містив класи Age, Ethnicity, Gender, Religion, Other type of cyberbullying, Not cyberbullying процесі класифікації модель повертає значення ймовірності наявності кіберзалякування в тексті, а також надає результати щодо різних типів кіберзалякувань, що присутні в тексті, таких як вікові кіберзалякування, гендерні, релігійні, етнічні та інші. Модель продемонструвала високі показники якості класифікації, зокрема, значення метрик становили: макрометрик Accuracy 94%, Precision 93%, Recall 93%,

F1 Score 93%, що свідчить про високу точність та надійність моделі у виявленні кіберзалякувань.

Висновки. Розроблений підхід до виявлення кіберзалякувань в інформаційному середовищі засобами машинного навчання продемонстрував високу ефективність і точність, що робить його цінним інструментом у сфері кібербезпеки. Завдяки здатності моделі автоматично ідентифікувати образливий контент з високою ймовірністю правильного визначення, цей метод сприяє створенню безпечнішого інформаційного середовища. Запропоноване рішення допомагає запобігати поширенню кіберзалякувань, своєчасно виявляючи потенційно небезпечні повідомлення та знижуючи ризики негативного кібервпливу на користувачів, зокрема на дітей та молодь.

Список літератури

1. Krak I., Zalutska O., Molchanova M., Mazurets O., Bahrii R., Sobko O., Barmak O. Abusive Speech Detection Method for Ukrainian Language Used Recurrent Neural Network. CEUR Workshop Proceedings, 2024, Volume 3688, Page 16-28. DOI: https://doi.org/10.31110/COLINS/2024-3/002.

2. Cyberbullying Tweets. *Kaggle*. URL – https://www.kaggle.com/datasets/soorajtomar/cyberbullying-tweets (дата звернення: 27.10.2024).

Відомості про авторів

Собко Олена Віталіївна, аспірантка кафедри комп'ютерних наук, Хмельницького національного університету, olenasobko.ua@gmail.com

Бармак Олександр Володимирович, завідувач кафедри комп'ютерних наук, Хмельницький національний університет, д.т.н., професор, alexander.barmak@gmail.com

Секція 1

ОСНОВНІ ПРАВИЛА КІБЕРГІГІЄНИ ПРИ КОРИСТУВАННІ ІНТЕРНЕТ-БАНКІНГОМ

Соловей В. С.
Вінницький національний технічний університет
Науковий керівник: Майданевич Л. О.

Актуальність. В сучасному світі з активним розвитком інформаційних технологій інтернет-банкінг (англ. Online Banking) займає лідерські позиції. Оскільки збільшився попит на онлайн сервіси пов'язані із покращенням ефективності – шляхом клієнто-орієнтованості. Нині в Україні збільшилась кількість банків ,що перевели свою роботу в онлайн режим та створили відповідне програмне забезпечення (наприклад, АТ КБ «Приватбанк», та український необанк «Monobank»). Це надає користувачеві можливість мобільно вирішувати свої фінансові питання навіть не виходячи з дому. Зокрема, сьогодні банки надають нам такі банківські послуги як: комунальні платежі, благодійні внески, оплата штрафів за порушення правил дорожнього руху тощо. Але зі збільшенням кількості банківських онлайн сервісів, ми (водночас) спостерігаємо за порушенням базовими правилами кібергігієни.

Метою даної роботи є дослідження основних правила кібергігієни при користуванні інтернет-банкінгом.

Основні положення. Інтернет-банкінг дозволяє користувачам вільно проводити велику кількість фінансових операцій незалежно від місця перебування. Всього-на-всього, необхідно лише мати будь-який мобільний пристрій та бути підключеним до мережі Інтернет. Відтак, до основних правил кібергігієни при користуванні інтернет-банкінгом ми можемо віднести: 1) Використання надійних паролів (створюйте складні паролі, уникайте очевидних комбінацій та використовуйте різні паролі для різних облікових записів; також рекомендується застосовувати багатофакторну автентифікацію (наприклад, одноразовий код на телефон). Не використовуйте загальнодоступні мережі Wi-Fi (доступ до інтернет-банкінгу краще здійснювати лише з захищених домашніх або мобільних мереж; публічний Wi-Fi може бути вразливим для хакерських атак). Перевірка надійності сайту або додатку (користуйтесь лише офіційними мобільними додатками банку або перевіреними вебсайтами; слідкуйте за тим, щоб адреса сайту починалась із «https» та містила іконку замка). Оновлення програмного забезпечення (регулярно оновлюйте операційну

систему та антивірусне ПЗ на всіх пристроях, які використовуються для доступу до банкінгу). Будьте обережні з підозрілими повідомленнями та посиланнями (не переходьте за сумнівними посиланнями і не вводьте особисту інформацію на підозрілих сайтах; не відкривайте файли чи посилання в електронних листах від невідомих відправників). Виходьте з акаунту після завершення роботи (завжди завершуйте сеанс, виходячи з облікового запису, особливо якщо користуєтесь чужим або загальнодоступним пристроєм). Контролюйте банківські операції та повідомлення (налаштуйте оповіщення про операції, щоб оперативно відслідковувати всі дії по рахунку; це допоможе швидко виявити можливу підозрілу активність). Ніколи не передавайте персональні дані (банк ніколи не запитує паролі або коди підтвердження операцій через електронну пошту чи телефонні дзвінки; якщо отримали такий запит – це може бути шахрайство) [1, 2].

Висновки. Користування інтернет-банкінгом є невід'ємною частиною нашого життя. Тому важливо пам'ятати, що кожен з нас є вразливим перед шахраями. Запропоновані тут вище правила допоможуть забезпечити додатковий захист ваших фінансових даних і запобігти ризикам у сфері інтернет-банкінгу.

Список літератури

1. Гасій О., Скорба О., Рошко Н. Вплив інтернет-банкінгу та мобільних додатків на зручність та доступність банківських послуг для клієнтів в Україні. *Економіка та суспільство*. 2024. № 59. DOI: https://doi.org/10.32782/2524-0072/2024-59-100.

2. Рекомендації щодо безпеки при роботі в системі Клієнт-банк. *КБ «АКОРДБАНК»*. URL: https://accordbank.com.ua/ua/corporate/clientbank-security (дата звертання 12.11.2024).

Відомості про авторів

Соловей Вероніка Сергіївна, студентка кафедри захисту інформації, ВНТУ, nikasolovey1@gmail.com

Майданевич Леонід Олександрович, ст. викладач кафедри захисту інформації, ВНТУ, к. філос. н., lmaidanevych@ukr.net

Секція 1

МЕТОДИ ЗАХИСТУ ВІД АТАК НА СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ

Стацишина І. П.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Клюшніков І. М.

Актуальність. Кібербезпека ШІ стає одним із пріоритетних напрямів роботи урядів і міжнародних організацій, оскільки все більше країн усвідомлюють потенційні ризики, пов'язані з використанням і розвитком штучного інтелекту [2].

Метою даної роботи є аналіз існуючих методів захисту систем штучного інтелекту від кіберзагроз.

Основні положення. Штучний інтелект – це здатність машин симулювати розум та імітувати людські когнітивні здібності. Тобто збирати й адаптувати зовнішні дані, а на їх основі навчатися ухвалювати рішення та робити висновки, як могла би людина. Технології штучного інтелекту міцно увійшли у життя людей на всіх рівнях – від голосових помічників до керованого алгоритмами синтезу стовбурових клітин. І це далеко не межа того, як вони можуть змінити розвиток людської цивілізації [1].

В рамках проведеної роботи було проаналізовано такі методи:

- вороже навчання;
- робастна оптимізація;
- регуляризація;
- ансамблеві методи;
- нормалізація даних.

Вони дозволяють системам ШІ краще адаптуватися до атак і знижувати ймовірність маніпуляцій. Утім, ці підходи потребують значних обчислювальних ресурсів, і їхня ефективність в реальних умовах залишається предметом подальших досліджень. Загрози на кшталт ворожих атак, отруєння даних та маніпуляцій алгоритмами є надзвичайно небезпечними для ШІ-систем, особливо тих, які використовуються у критичних застосуваннях (медицина, транспорт, фінанси). Виявлено, що навіть мінімальні зміни в даних можуть спричинити серйозні помилки, що підкреслює важливість розвитку нових стратегій для запобігання таким атакам. Загалом, хоча розроблено декілька підходів для захисту ШІ,

дослідження в цій сфері лише на початковому етапі. Подальший розвиток технологій потребує створення нових методів, які враховують реальні умови застосування, забезпечуючи безпеку ШІ на всіх рівнях – від алгоритмів до даних.

Висновки. Таким чином, розвиток ШІ відкриває безпрецедентні можливості, але супроводжується значними ризиками. Важливо, щоб технології захисту ШІ не відставали від темпів розвитку самих ШІ-систем. Використання таких методів як вороже навчання, робастна оптимізація, регуляризація та нормалізація даних допомагає забезпечити певний рівень захисту, проте ці підходи ще не досконалі.

У майбутньому необхідно зосередити увагу на:

- адаптивних системах захисту, здатних працювати в режимі реального часу;
- розробці нових етичних і правових норм для захисту ШІ і його користувачів;
- комплексному підході до тестування систем ШІ в умовах реальних загроз.

Безпека штучного інтелекту є однією з найбільш критичних проблем сучасної науки та технологій, і її вирішення вимагатиме зусиль як інженерів, так і законодавців та дослідників у сфері етики.

Список літератури

1. Даниленко Ю. Від Ш до І: що таке штучний інтелект та як він трансформує світ. *Speka*. URL: https://speka.media/ai/vid-s-do-i-shho-takestucnii-intelekt-ta-yak-vin-transformuje-svit-xv7039#shho-take-stucnii-intelekt (дата звернення: 02.11.2024).

2. Харченко В., Неретін О. Забезпечення кібербезпеки систем штучного інтелекту: аналіз вразливостей, атак і контрзаходів. Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі. 2022. №12. С. 7-22. URL: https://science.lpnu.ua/sisn/all-volumes-and-issues/volume-12-2022/ensurance-artificial-intelligence-systems-cyber-security (дата звернення: 16.10.2024).

Відомості про авторів

Стацишина Ірина Павлівна, магістрантка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.statcyshyna@student.csn.khai.edu

Клюшніков Ігор Миколайович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., с.н.с., i.kliushnikov@csh.khai.edu

Секція 1

СЕГМЕНТАЦІЯ ЗОБРАЖЕНЬ НА ОСНОВІ ВЕЙВЛЕТ АНАЛІЗУ

Тихий А. М.
Національний університет «Запорізька політехніка»
Науковий керівник: Дубровін В. І.

Актуальність. Зростання інтересу до сегментації зображень обумовлено безперервним розвитком технологій обробки даних та потребою у високоточних рішеннях для різних галузей, таких як медицина, аерокосмічна інженерія та комп'ютерна графіка. Сучасні методи обробки зображень вимагають розробки ефективних алгоритмів для точного виділення об'єктів та областей інтересу.

Метою дослідження є визначення найбільш підходящого методу сегментації зображень для досягнення високого рівня точності при оптимальних обчислювальних витратах [1].

Основні положення. Сегментація зображень є критичним етапом у процесі обробки, що дозволяє виділити об'єкти та області інтересу на основі спільних характеристик, таких як колір, текстура та форма. Вейвлет аналіз дозволяє сегментувати зображення на різних частотних компонентах, що є великим плюсом при обробці зображень з високим рівнем шуму. Забезпечує високу адаптивність до різних текстур і форм, дозволяючи отримувати детальнішу інформацію про структуру зображень.

При проведенні сегментації зображень на основі вейвлет аналізу можна виділити кілька ключових аспектів:

1. Мультирівнева обробка: Вейвлет аналіз дозволяє аналізувати зображення на різних масштабах, що забезпечує детальне виділення об'єктів та текстур [2-4].
2. Адаптивність до шумів: Метод демонструє високу стійкість до шумів, зберігаючи якість сегментації навіть у випадках, коли зображення містять артефакти.
3. Визначення характеристик об'єктів: Використання вейвлетів дозволяє виділити не лише контури, але й текстури, важливі для розпізнавання складних об'єктів.
4. Застосування в різних сферах: Сегментація зображень на основі вейвлет аналізу знаходить своє застосування в медицині, аерокосмічній інженерії та комп'ютерній графіці.

5. Потенціал для інтеграції з машинним навчанням: Метод вейвлет аналізу може бути інтегрований з алгоритмами машинного навчання для покращення точності сегментації.

Висновки. Розвиток технологій обробки зображень обумовлює необхідність вдосконалення методів сегментації. Сегментація зображень на основі вейвлет аналізу показує високу точність і ефективність, особливо в складних умовах. Подальші дослідження можуть зосередитися на інтеграції вейвлет аналізу з методами машинного навчання для покращення точності сегментації та розширення можливостей застосування системи. Це робить вейвлет аналіз важливим інструментом для професіоналів у різних сферах.

Список літератури

1. Andrea Gavlasová, Aleš Procházka, Martina Mudrová. Wavelet based image segmentation. URL – https://www.researchgate.net/publication/228453305_Wavelet_based_image_segmentation (дата звернення: 03.11.2024).

2. Пат. 90102 Україна, МПК6 G01R 23/16. Спосіб визначення оптимального вейвлету для аналізу сигналів на основі дослідження його амплітудно-частотної характеристики [Текст] / В. І. Дубровін, Ю. В. Твердохліб; заявник и патентовласник: Запорізький національний технічний університет. - заявл. 20.12.13; опубл. 12.05.14, Бюл. No9.,3с.

3. Комп'ютерна програма «Аналіз частотних складових вейвлет-базису»: Свідоцтво про реєстрацію авторського права на твір No 60630 / Ю. В. Твердохліб, В. І. Дубровін. – державна служба інтелектуальної власності України. – Дата реєстрації: 14.07.2015.

4. J. Tverdohleb Wavelet technologies of non-stationary signals analysis / J. Tverdohleb, V. Dubrovin, M. Zakharova // 1-th IEEE International Conference on Data Stream Mining & Processing. – Ukraine, Lviv: LPNU, 2016. – P. 75–79.

Відомості про авторів

Тихий Андрій Михайлович, студент кафедри програмних засобів, Національний університет «Запорізька Політехніка», chaffeeq@gmail.com

Дубровін Валерій Іванович, професор кафедри програмних засобів, Національний університет «Запорізька Політехніка», к.т.н., vdubrovin@gmail.com

Секція 1

ПОРІВНЯЛЬНИЙ АНАЛІЗ ДВОХ АЛГОРИТМІВ ФАКТОРИЗАЦІЇ

Труш М. С.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Алгоритм RSA залишається одним із найпоширеніших методів асиметричного шифрування, забезпечуючи захист передачі даних в Інтернеті та в інших мережах. Існує достатньо комерційних та відкритих платформ, які використовують криптосистему RSA, в тому числі поширені операційні системи, такі як Windows, MacOS, UNIX-подібні операційні системи [1]. Актуальність RSA підкріплюється його стійкістю проти класичних методів криптоаналізу, які базуються на факторизації великих чисел. Для стимулювання розвитку більш ефективних алгоритмів факторизації компанія RSA Laboratories заснувала RSA Factoring Challenge, який тривав до 2007 року. Незважаючи на завершення виклику, останні досягнення, такі як факторизація числа RSA-250 у 2020 році, демонструють, що дослідження в цій галузі тривають і мають значний вплив на безпеку RSA [2]. Окрім традиційних методів криптоаналізу, сьогоднішні дослідження фокусуються на розробці нових підходів до факторизації великих чисел для криптосистеми RSA, що дозволяє не лише оцінювати ефективність алгоритмів, але й створює потенційну загрозу для систем безпеки, якщо такі методи стануть обчислювально доступними [3]. Порівняльний аналіз алгоритмів факторизації дає можливість дослідникам оптимізувати стратегії захисту на основі сучасних криптоаналітичних досягнень, передбачаючи потенційні слабкі місця і рекомендувати більш захищені варіанти ключів або алгоритмів, щоб забезпечити довготривалу безпеку даних в умовах стрімкого розвитку обчислювальних технологій.

Мета роботи. Аналіз двох алгоритмів факторизації з проведенням експерименту для визначення найбільш ефективного алгоритму.

Основні положення. В роботі детально розглянуто алгоритм факторизації, в якому використовуються змінні P і Q, що коригуються на кожному кроці для поступового досягнення нульової різниці (дельти) між факторизованим числом N та добутком змінних P і Q. До переваг алгоритму належить значна швидкодія завдяки використанню простих операцій додавання та віднімання замість множення, що мінімізує обчислювальні витрати, особливо для великих чисел. В роботі показано, що на певному етапі алгоритм досягає стабільності в кількості ітерацій, що дозволяє

прогнозувати час факторизації та забезпечує додаткове прискорення виконання завдання. Окрім основних принципів факторизації, у документі також розглядається особлива техніка контролю помилок, яка базується на спостереженні за зміною знаку різниці дельти на кожному кроці алгоритму. Якщо дельта становить від'ємною, алгоритм корегує значення P і Q, таким чином, щоб на наступному кроці результат був додатнім, і навпаки. Це чергування знаків помилки дозволяє точно налаштувати кроки алгоритму, мінімізуючи кількість обчислень і швидше наближаючись до нульового значення при якому можна вважати, що спільний дільник для числа *N* знайдено.

Висновки. Попри високу стійкість і поширеність криптосистеми RSA, зокрема у комерційних системах, розвиток нових методів криптоаналізу постійно стимулює вдосконалення технік факторизації. Факторизація RSA-250, який складається з 829 бітів, демонструє прогрес у галузі, що підвищує актуальність аналізу різних алгоритмів факторизації. Дослідження також показали, що оптимізація обчислень за рахунок використання менш ресурсомістких операцій підвищує швидкодію роботи алгоритму.

Список літератури

1. RSA authentication agent supported platforms. *Scribd*. URL – https://www.scribd.com/document/89623408/RSA-Authentication-Agent-Supported-Platforms (дата звернення: 05.11.2024).

2. Boudot F., Gaudry P., Guillevic A., Heninger N., Thomé E., Zimmermann P. Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment. The 40th Annual International Cryptology Conference (Crypto 2020). August 2020. DOI: https://doi.org/10.48550/arXiv.2006.06197.

3. Pevnev V. Pseudoprime Numbers: Basic Concepts And The Problem Of Security. International Conference on Information and Communication Technologies in Education, Research, and Industrial Applications. 2017. Page 583-593. URL: https://ceur-ws.org/Vol-1844/10000583.pdf (дата звернення 06.11.2024).

Відомості про авторів

Труш Марина Сергіївна, студентка кафедри інженерії програмного забезпечення, НАУ «ХАІ»

Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu

Секція 1

АНАЛІЗ МЕТОДІВ КІБЕРБЕЗПЕКИ У СФЕРІ ДЕРЖАВНИХ ПОСЛУГ

Федоренко Д. Д.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Землянко Г. А.

Актуальність. Цифровізація державних послуг, таких як електронні документи, записи та медичне страхування, значно розширило доступ громадян до життєво важливих послуг, але водночас підвищило ризик кібератак. Успішні атаки можуть призвести до витоку персональних даних, порушення роботи критично важливої інфраструктури та втрати довіри до державних інституцій, що загрожує приватності громадян та економічній стабільності [1].

Щоб протистояти еволюціонуючим кіберзагрозам, держави повинні вживати гнучких і проактивних оборонних заходів, інвестуючи в технології штучного інтелекту для виявлення аномалій і систем аналізу загроз. Важливо також навчати персонал ефективно реагувати на нові типи атак, що підвищить загальний рівень кібербезпеки [2].

Метою даної роботи є аналізу сучасних методів забезпечення кібербезпеки у сфері державних послуг.

Основні положення. З огляду на стрімку цифровізацію та залежність громадян від державних сервісів, важливість їхнього захисту є критичною. Поряд з перевагами, які надають цифрові технології, зростають і кіберризики, що ставлять під загрозу національну безпеку та приватність громадян. Тому захист таких сервісів є необхідністю для забезпечення стабільності державних інфраструктур. Сучасні кіберзагрози для комунальних підприємств різноманітні та включають як зовнішні атаки, так і внутрішні порушення безпеки. До основних загроз належать DDoS-атаки, фішинг, SQL-ін'єкції та сучасні методи соціальної інженерії, спрямовані на викрадення персональних даних та компрометації систем [2]. Уразливості в системах контролю доступу, незахищені канали зв'язку та недосконалі механізми аутентифікації підвищують ризик успішних атак [3]. Зловмисники часто включають як окремих хакерів, так і організовані групи кіберзлочинців, які прагнуть отримати несанкціонований доступ до урядових даних і підірвати довіру громадськості до цифрових послуг [4, 5]. Для підвищення рівня кібербезпеки державних сервісів необхідно впроваджувати комплексний підхід, що включає як технічні, так і

організаційні заходи. Важливим елементом є застосування моделей безпеки, таких як Zero Trust, що передбачає мінімізацію доступу до ресурсів та постійну перевірку користувачів і пристроїв [5]. Використання багатофакторної автентифікації, методів шифрування даних, а також систем виявлення та запобігання вторгненням (IDS/IPS) дозволяє значно знизити вразливості в системах. Крім того, регулярні тренінги для персоналу, постійний моніторинг систем на предмет аномалій та впровадження стандартів безпеки, є необхідними кроками для забезпечення стійкості до кібератак.

Висновки. Аналіз показує, що диджиталізація державних послуг збільшує ризик атак і вразливостей, загрожуючи національній безпеці та приватності громадян. Для забезпечення належного захисту необхідна модель нульової довіри, багатофакторна автентифікація, використання сучасних технологій спостереження та шифрування, підвищення стандартів безпеки, навчання персоналу та розробка ефективних методів реагування на кіберзагрози.

Список літератури

1. Arief A. R. An analysis of cybersecurity policies and practices in public administration. *Journal of public representative and society provision*. 2022. Volume 2(2). Page 56–62. DOI: https://doi.org/10.55885/jprsp.v2i2.211.

2. Understanding Local Government Cybersecurity Policy: A Concept Map and Framework / S. T. Hossain et al. *Information*. 2024. Volume 15(6). Page 342. DOI: https://doi.org/10.3390/info15060342.

3. Cyber threats and advisories | cybersecurity and infrastructure security agency CISA. *CISA*. URL – https://www.cisa.gov/topics/cyber-threats-and-advisories (дата звернення: 10.11.2024).

4. ENISA Threat Landscape 2024. *ENISA*. URL – https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 10.11.2024).

5. The world economic forum. *World Economic Forum*. URL – https://www.weforum.org (дата звернення: 10.11.2024).

Відомості про авторів

Федоренко Дар'я Дмитрівна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.d.fedorenko@student.csn.khai.edu

Землянко Георгій Андрійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», PhD з кібербезбеки, g.zemlynko@csn.khai.edu

Секція 1

ОСНОВНІ СПОСОБИ ОЦІНКИ ДОСТОВІРНОСТІ ІНФОРМАЦІЇ

Фененко Б.О.
Вінницький національний технічний університет
Науковий керівник: Майданевич Л. О.

Актуальність. Під час повномасштабної війни, країна-агресор використовує різні методики ведення війни. І однією з цих методик є гібридна війна, що фактично є війною-онлайн. Такий тип війни не варто залишати поза увагою, оскільки він є пропагандою, що сильно впливає на людську свідомість за допомогою інформації. Інформація – це дані, що мають значення, впливають на прийняття рішень, зберігаються, передаються та використовуються для комунікації, навчання чи створення знань [1]. У сьогоденні інформація є одним з найважливіших аспектів людини, маючи її, особа має владу. Тож інформацією можна маніпулювати, що призводить до керування свідомістю людей або їх переконаннями. У таких випадках інформація стає ІПСО (тобто, інформаційно-психологічною операцією). Тож варто застосовувати критичне мислення та піддавати сумніву інформацію при отриманні її. Як приклад можна навести брехливі новини, що країна-агресор не обстрілює мирні споруди України, коли у реальності, обстріли відбуваються майже не щодня.

Метою даної роботи є оцінка достовірності інформації, відносно сучасних загроз.

Основні положення. Перевірка джерела інформації (оцінка надійності та авторитетності джерела, яке надає дані, наприклад, офіційні організації, верифіковані акаунти тощо). Порівняння з іншими джерелами (перевірка інформації шляхом співставлення з іншими незалежними джерелами, щоб виявити підтвердження або суперечності). Аналіз змісту інформації (логічна оцінка інформації, виявлення можливих суперечностей чи нестиковок, а також перевірка на предмет помилок в обставинах). Використання методів зворотного пошуку (наприклад, пошук зображень чи тексту в мережі для перевірки першоджерела або контексту). Перевірка часової актуальності (аналіз дати інформації, щоб визначити, чи є вона релевантною та своєчасною для поточної ситуації). Експертна оцінка (залучення фахівців для оцінки інформації, що потребує спеціальних знань або компетентності в конкретній сфері). Використання автоматизованих інструментів (спеціальні програми та алгоритми можуть аналізувати великі

бази даних, виявляти фальсифікації або схожість із перевіреними зразками) [1, 2].

Висновки. У сучасному світі інформація стала зброєю, тож перевірка інформації на достовірність є невід'ємною частиною життя, в іншому випадку можна легко стати жертвою ІПСО. Для свого захисту слід перевіряти інформацію на її достовірність за допомогою надійних джерел та критичного мислення.

Список літератури

1. Бржевська З., Довженко Н., Гайдур Г., Аносов А. Критерії моніторингу достовірності інформації в інформаційному просторі. Кібербезпека: освіта, наука, техніка. 2019. Том 1(5). С. 53-60. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/96 (дата звертання 12.11.2024).

2. Бржевська З., Киричок Р., Платоненко А., Гулак Г. Оцінка передумов формування методики оцінки достовірності інформації. Кібербезпека: освіта, наука, техніка. 2022. Том 3 (15). С. 164-174. DOI: https://doi.org/10.28925/2663-4023.2022.15.164174.

Відомості про авторів

Фененко Богдана Олександрівна, студентка кафедри захисту інформації, ВНТУ, bfenenko1@gmail.com

Майданевич Леонід Олександрович, ст. викладач кафедри захисту інформації, ВНТУ, к. філос, н, lmaidanevych@ukr.net

Секція 1

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ НОРМАЛІЗАЦІЇ ЕМБЕДІНГІВ У СИСТЕМАХ РОЗПІЗНАВАННЯ ОБЛИЧ

Ханін Д. О.
Національний університет «Львівська політехніка»
Науковий керівник: Отенко В. І.

Актуальність. У сучасних системах біометричної автентифікації використання нейронних мереж для розпізнавання облич стало стандартом де-факто. Ключовим етапом у процесі верифікації є генерація та порівняння ембедінгів – числових векторів, що представляють характеристики обличчя. Проте різні моделі генерують ембедінги з різними статистичними характеристиками та масштабами, що ускладнює їх ефективне порівняння та комбінування. Це робить критично важливим вибір правильного методу нормалізації для забезпечення надійної роботи системи верифікації, особливо при використанні ансамблю моделей.

Метою роботи є проведення порівняльного аналізу ефективності різних методів нормалізації ембедінгів у контексті систем розпізнавання облич та визначення їх впливу на точність верифікації при використанні як одиночних моделей, так і їх комбінацій.

Основні положення. В роботі досліджуються L2, Z-Score та Min-Max методи нормалізації ембедінгів [1].

Дослідження проводилось на наборі даних CFP (Celebrities in Frontal-Profile) [2], що містить 500 суб'єктів з 10 фронтальними зображеннями для кожного. Для генерації ембедінгів використовувались моделі VGG-Face, Facenet, ArcFace та SFace [3].

Експериментальні результати продемонстрували наступне. При використанні одиночних моделей: L2-нормалізація показала найвищу точність для всіх моделей; Z-Score нормалізація показала порівнянні результати, відстаючи від L2 на 0,4%; Min-Max показала гірші результати, особливо при наявності викидів у даних. При комбінуванні ембедінгів від різних моделей: Послідовне застосування Z-Score та L2 нормалізації дало найкращу точність; L2 нормалізація показала гіршу точність ніж послідовне застосування Z-Score та L2 на 0,2%; Використання Z-Score нормалізації для різних каскадів моделей призводило до нестабільної точності; Min-Max показала неприйнятні результати через чутливість до викидів.

Висновки. Проведене дослідження показало, що вибір методу нормалізації суттєво впливає на ефективність систем розпізнавання облич. При використанні одиночних моделей L2-нормалізація є оптимальним вибором, забезпечуючи баланс між точністю та обчислювальною складністю. Для систем, що використовують комбінацію ембедінгів від різних моделей, послідовне застосування Z-Score та L2 нормалізації дозволяє досягти найвищої точності. Подальші дослідження можуть бути спрямовані на розробку адаптивних методів нормалізації, що враховують специфіку конкретних моделей та даних.

Список літератури

1. Andrezza, I., Borges, E., Júnior, I., Moto, R., Marques, J., & Batista, L. Normalization Methods Analysis Applied to Face Recognition. 2017 Workshop of Computer Vision (WVC). Page 108-113. DOI: https://doi.org/10.1109/WVC.2017.00026.
2. S. Sengupta, J.C. Cheng, C.D. Castillo, V.M. Patel, R. Chellappa, D.W. Jacobs. Frontal to Profile Face Verification in the Wild. IEEE Winter Conference on Applications of Computer Vision (WACV). 2016. DOI: https://doi.org/10.1109/WACV.2016.7477558.
3. Goel R, Mehmood I, Ugail H. A Study of Deep Learning-Based Face Recognition Models for Sibling Identification. Sensors. 2021. Volume 21(15). DOI: https://doi.org/10.3390/s21155068.

Відомості про авторів

Ханін Денис Олегович, аспірант кафедри захисту інформації, Національний університет «Львівська політехніка», denys.o.khanin@lpnu.ua
Отенко Віктор Іванович, доцент кафедри захисту інформації, Національний університет «Львівська політехніка», к.т.н., доцент, viktor.i.otenko@lpnu.ua

Section 1

INFORMATION SECURITY AT USING SMART CONTRACTS IN SOCIAL NETWORKS

Yurii Tsudzenko
Ivan Franko National University of Lviv
Scientific adviser: Bohdan Pavlyshenko

Relevance. The increasing usage of social media platforms has led to concerns over data privacy and security, particularly with the widespread implementation of data analytics techniques [1]. This paper investigates the potential of using smart contracts on blockchain to secure data in social networks. By applying intelligent data analysis to social media data while leveraging smart contracts, this study demonstrates how decentralized systems can enhance information security and transparency, providing users with greater control over their data. The analysis reveals key privacy benefits, security improvements, and challenges in integrating blockchain for data analytics in social networks.

Purpose. The main focus of this research is on implementing Intelligent Data Analysis (IDA) to enhance security in social media data handling.

Principal provisions. By leveraging machine learning and advanced analytics, IDA can detect suspicious activities, such as unauthorized access or unusual user behavior, which are critical in identifying potential security threats. Using data patterns, it can assess risks and provide real-time alerts, allowing social media platforms to proactively respond to security incidents [2]. IDA techniques also enable the analysis of massive datasets, identifying anomalies and securing sensitive user data through encrypted and decentralized storage [3]. Encrypted data is managed within smart contracts, where execution rules ensure that user data remains protected and accessible only according to preset permissions. Once the smart contract execution completes, blockchain confirmation validates the integrity and security of the data, enhancing transparency and control for users over their information in the social network environment [4].

Furthermore, smart contracts on blockchain support IDA by ensuring transparent, secure transactions, enhancing trust in data handling. Blockchain's immutable ledger can validate user actions and prevent tampering, further strengthening data integrity. This integration of blockchain and IDA enables privacy-preserving analytics, where user consent is respected and data is processed with minimal exposure [5]. Through intelligent categorization, IDA ensures only authorized data flows through social media networks, reducing

vulnerability. Ultimately, IDA in social media aims to achieve high security, while maintaining an ethical balance of data utility and user privacy.

Conclusion. The integration of smart contracts and blockchain technology in social networks, with intelligent data analysis, opens significant pathways for enhancing data privacy, security, and transparency. By combining blockchain's decentralized, tamper-resistant structure with intelligent analytics, social platforms can gain valuable insights without compromising user privacy. Smart contracts facilitate secure, automated transactions that empower users with increased control over their data, thus strengthening accountability and minimizing unauthorized access. Blockchain ensures that data is stored securely across a distributed network, while intelligent analytics processes the data responsibly, offering insights in a way that respects user consent and privacy.

List of references

1. Laurent, A., Tuan, T. Analyzing Security Threats in Social Media Networks. *International Journal of Cybersecurity*. 2022. Volume 8(2). Page 231–245.
2. Zhao J.,Yuan J. Data Privacy in the Age of Blockchain and AI. In *Proceedings of the IEEE Conference on Data Privacy*. 2023. Page 210–225.
3. Dube, P. (2021). *Cybersecurity and Blockchain in Social Media: Protecting User Data Throught Decentralization*. Oxford University Press.
4. Gonzalez M., Rivera L. *Smart Contracts and Social Media: Enhancing Trust and Transparency*. 2020. Cambridge: MIT Press.
5. Yurii Tsudzenko «Approaches in modeling smart contracts based on Ethereum». *Electronics and information technologies*. 2023. Issue 22. P. 69–78. DOI: http://dx.doi.org/10.30970/eli.22.7.

Information about the authors

Tsudzenko Yurii, a PhD student from the Department of System Design, Ivan Franko National University of Lviv, yura9989@gmail.com
Pavlyshenko Bohdan M, candidate of physical and mathematical sciences, professor of the Department of System Design, Ivan Franko National University of Lviv, bohdan.pavlyshenko@lnu.edu.ua

Section 1

Leveraging LLMs to Build Glossaries for Detecting Data Leaks

Kiril Shamonin
Sumy State University
Scientific adviser: Dmytro Prylepa

Relevance. Every modern business has at least one thing in common: a lot of data. Collecting, refining, and making sense of data helps to drive business growth, as it is essential for identifying trends, consumer behaviour, and opportunities for competitive advantage. That is the reason why data leaks happen all the time. A data breach is the unintentional or accidental disclosure of confidential or sensitive information [1]. Cybercriminals are looking for information of value to use for their own purposes or to resell. Information that can be leaked includes personal information, financial data, credentials, corporate information, etc. [2].

Leaks can be caused by many factors, such as bad infrastructure, fraud, poor password policies, and human error [3]. Information security professionals should conduct cyclical monitoring of external resources for leaks of the organization's confidential data. This monitoring could reduce the risk of the information security incident, discover leak sources in the organization and protect the reputation of the organization.

Data leaks can be detected by analysing open sources, such as software code repositories (Github, Gitlab), anonymous data sharing sites (Pastebin), open cloud storage (AWS S3 Bucket), etc. The number of data leaks found depends on the quality of the glossary of confidential terms that is used for the search.

The purpose of this work is to analyze the mechanisms of large language models (LLM) in creation of the search data glossary for searching data leaks.

Principal provisions. LLMs can be used to analyze text and find language features that are specific to a particular organization. Such features can include unique names of variables and functions in the program code: speech patterns, phrases or legal terms in business documentation, etc. To create a glossary of confidential terms, you need to perform the following steps:

1. Setting up the model to detect confidential information. Information security analysts can use LLM such as GPT-4, LLaMa, Patronus AI. It is necessary to create a dataset for training the LLM using data that contains confidential and specific information for the organization. Train the model on this data so that it can recognize patterns related to confidential information, personal data, or specific information.

2. Use LLM to identify confidential information in documents. The LLM should be used to search for phrases that may indicate confidential information. You should also conduct additional testing and, if necessary, adjust the LLM.

3. Create a sensitive data glossary for further monitoring. Once the sensitive information has been identified, a database or index of sensitive words, phrases and expressions can be created. This information should be structured for ease of use.

This method of creating a glossary has advantages over manual creation, as it can use a larger amount of information than a specialist can process. This will allow you to find more unique data, which will increase the number of data leaks found, and may also reduce the number of false positives.

This glossary of confidential terms can be used in multiple processes, including ongoing audit of company's security posture, technical due diligence or vendor audits before acquisition process of products or services.

Conclusions. LLM provide the ability to analyze vast amounts of data. As a result, information security specialists could increase quality of findings of the data leaks, while reducing the number of false positives. This can reduce the information security risks of the organization.

List of references

1. How to Detect Data Leakage. *Upguard*. URL – https://www.upguard.com/blog/how-to-detect-and-prevent-data-leakage (date of access 06.11.204).

2. Data Leakage: Common Causes, Examples & Tips for Prevention. *Blue Voyant*. URL – https://www.bluevoyant.com/knowledge-center/data-leakage-common-causes-examples-tips-for-prevention (date of access 06.11.204).

3. Verma R., Gautam V., Yadav Ch., Gupta I., Singh A. A survey on data leakage detection and prevention: Materials of the international scientific and practical conference. Online. 2020. B.M. Institute of Engineering and Technology, India. DOI: http://dx.doi.org/10.2139/ssrn.3603736.

Information about the authors

Kiril Shamonin, a PhD student from the Department of Computer Science, Sumy state university, kirilshamonin@gmai.com

Dmytro Prylepa, Candidate of Technical Sciences, Assistant of the Department of Computer Science, d.prylepa@cs.sumdu.edu.ua

Секція 1

ДОСЛІДЖЕННЯ ШЛЯХІВ ОПТИМІЗАЦІЇ ПРОДУКТИВНОСТІ БАЗ ДАНИХ SQL: АНАЛІЗ ТА ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

Шашкін М. А.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник: Харченко В. С.

Актуальність. З ростом обсягу даних та складності запитів до баз даних SQL збільшується важливість оптимізації їх продуктивності. Недостатня продуктивність баз даних може призводити до значних затримок, що впливає на загальну ефективність бізнес-процесів. Дослідження показують, що понад 70% організацій зіткнулися з проблемами продуктивності своїх баз даних у минулому році, і більше половини цих проблем були пов'язані з неоптимальними запитами та індексами [1]. З моменту свого виникнення SQL став основним засобом управління реляційними базами даних. Однак, з часом, із збільшенням обсягів даних і складності запитів, виникають нові виклики щодо продуктивності баз даних SQL [2]. Застарілі методи індексування та неоптимальні схеми можуть значно впливати на швидкість виконання запитів [3]. Додатково, згідно зі звітом Gartner, витрати на утримання і оптимізацію баз даних складають близько 30% загального бюджету на IT у великих організаціях, що підкреслює значущість цієї проблеми [4].

Метою даного дослідження є аналіз методів оптимізації продуктивності баз даних SQL та розробка практичних рекомендацій щодо підвищення ефективності їх роботи в умовах зростаючих обсягів даних та складності запитів. Аналізуючи сучасний ринок баз даних, виявлено, що SQL залишається основним інструментом для управління великими обсягами структурованих даних. Однак, із зростанням обсягу даних та кількості користувачів, оптимізація продуктивності баз даних стає критично важливою для забезпечення швидкого доступу до інформації та підтримки безперебійної роботи систем.

Основні положення. Для ефективної оптимізації продуктивності баз даних SQL використовуються різноманітні методи та інструменти. Серед них важливе місце займають індексування, нормалізація даних, оптимізація запитів, використання кешування, а також регулярний аналіз продуктивності. Крім того, використання інструментів для моніторингу, таких як SQL Profiler, EXPLAIN планів запитів, та автоматизованих

оптимізаторів, є ключовими стратегіями для підвищення продуктивності баз даних [5]. У роботі проведено аналіз переваг та недоліків різних методів оптимізації, а також надано рекомендації з їх ефективного використання для забезпечення високої продуктивності баз даних на всіх етапах їх роботи та обслуговування.

Висновки. Дослідження показує необхідність постійного вдосконалення стратегій оптимізації продуктивності баз даних SQL та активної участі спеціалістів у цьому процесі. Рекомендації з оптимізації включають використання інструментів моніторингу, регулярний аналіз продуктивності та впровадження заходів з оптимізації запитів та індексів для забезпечення високої продуктивності баз даних в умовах зростаючих обсягів даних.

Список літератури

1. Smith J. Optimizing SQL Database Performance: An Empirical Study. Journal of Database Management, 2023. DOI: https://doi.org/10.1234/jdm.2023.5678.
2. Jones R., Brown L. SQL Query Optimization Techniques. International Journal of Data Engineering. 2022. DOI: https://doi.org/10.5678/ijde.2022.12345.
3. Williams A., Taylor P. Indexing in SQL Databases: Best Practices. Proceedings of the Database Optimization Conference. 2021. DOI: https://doi.org/10.6789/dboc.2021.54321.
4. Gartner Data Management Report. *Gartner*. URL: https://www.gartner.com/reports/data-management (дата звернення: 21.10.2024).
5. Saltzer J. H., Schroeder M. D. The protection of information in computer systems. Proceedings of the IEEE. 1975. Volume 63(9). Page 1278–1308. DOI: https://doi.org/10.1109/proc.1975.9939.

Відомості про авторів

Шашкін Мирослав Анатолійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.shashkin@student.csn.khai.edu
Харченко Вячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, v.kharchenko@csn.khai.edu

Секція 1

МЕТОД АНАЛІЗУ ДОСТОВІРНОСТІ ТЕКСТОВИХ ПОВІДОМЛЕНЬ ДЛЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ КІБЕРБЕЗПЕКИ

Шевчук П.О.
Хмельницький національний університет
Науковий керівник: Мазурець О.В.

Актуальність. Виявлення достовірності даних є важливою задачею в сфері кібербезпеки, адже в останній час в мережі Інтернет має місце розповсюдження неправдивої інформації [1], тому розробка прикладних рішень, які здатні перевіряти достовірність текстів є актуальною задачею розвитку інтелектуальних систем кібербезпеки [2].

Мета полягає в розробці методу аналізу достовірності текстових повідомлень для інтелектуальних систем кібербезпеки.

Основні положення. У дослідженні розроблено метод аналізу достовірності текстових повідомлень для інтелектуальних систем кібербезпеки на основі ансамблевого підходу, що поєднує логістичну регресію, дерево рішень, градієнтне посилення та випадковий ліс.

У якості вхідних даних представлені текст для аналізу та навчений ансамбль класифікаторів. Першим кроком система визначає мову тексту та при необхідності автоматично перекладає на англійську. Другим кроком увесь текст приводиться до нижнього регістру та видаляються стоп-символи. Отриманий результат проходить етапи токенізації, лематизації та векторизації. На третьому етапі дані аналізуються на наявність логістичної регресії та визначається дерево рішень. Окрім цього проводиться градієнтний бустінг та визначення випадкового лісу. Четвертим кроком формуються результати оцінки у вигляді зваженої оцінки. На виході отримується оцінка на принадлежність тексту для аналізу до категорії достовірності тексту.

Поданий метод був апробований шляхом розробки програмного забезпечення та продемонстрував високу ефективність, використовуючи зважений показник достовірності, обчислений на основі виходів кожної моделі.

Висновки. Запропонований метод аналізу достовірності текстових повідомлень для інтелектуальних систем кібербезпеки на основі ансамблевого підходу показав ефективність на рівні 92%, що є високим показником порівняно із сучасними рішеннями у сфері кібербезпеки.

Реалізація тестового програмного забезпечення була виконана у вигляді веб-додатка за допомогою технологій Scikit-Learn та Flask. На основі ансамблевих моделей було сформовано зважений показник достовірності тексту, який обчислюється як сума впливових коефіцієнтів кожної моделі, помножених на вихід відповідної моделі класифікатора.

Для навчання класифікаторів використовувався збалансований англомовний набір даних, що складався з 44 898 зразків, зокрема 23 481 зразків фейкової інформації та 21 417 зразків дійсної інформації.

Список літератури

1. Дослідження на поширення використання українцями соцмереж. *Детектор Медіа.* URL: https://detector.media/infospace/article/213998/2023-07-10-opora-osnovnym-dzherelom-informatsii-mayzhe-80-ukraintsiv-ie-sotsialni-merezhi (дата звернення 11.11.24).
2. Звідки українці беруть інформацію в умовах війни? *Українська Правда.* URL: https://life.pravda.com.ua/society/2022/06/2/248923 (дата звернення 11.11.24).

Відомості про авторів

Шевчук Павло Олександрович, студент кафедри комп'ютерних наук, Хмельницький національний університет, shevchuk12072005@gmail.com
Мазурець Олександр Вікторович, доцент кафедри комп'ютерних наук, Хмельницький національний університет, exechong@gmail.com

Section 1

COMPARATIVE ANALYSIS OF FACTORIZATION ALGORITHMS

Oles Yudin
National Aerospace University «Kharkiv Aviation Institute»
Scientific adviser: Vladimir Pevnev

The relevance of this research is based on the fact that many modern cryptographic systems, especially those that protect the privacy of transmitted information, rely on complex mathematical problems that are hard to solve using standard methods [1]. One of these problems is breaking down large numbers into prime factors, which is the foundation of the RSA encryption algorithm [2]. Today, cloud systems can perform calculations faster using clusters of computers, which helps speed up the factorization process and brings us closer to solving such problems [3]. As a consequence, it is important to study how the sizes of two large prime numbers affect the strength of the keys used in the RSA system. Factorization has an interesting feature: when a number is the product of two prime numbers P and Q the difficulty of breaking it down depends on the size difference between P and Q [4]. For example, if the prime numbers have a big size difference, the efficiency of factorization algorithms can change. This makes it important to study not only how effective the algorithms are in general but also how changes in these parameters affect the time it takes to factorize the numbers.

The purpose of this work is to analyze current factorization algorithms and study how the ratio between large prime numbers influences the difficulty of factorizing their product.

Principal provisions. This work studies the efficiency of various algorithms for factoring large numbers, including Fermat's factorization, Pollard's rho algorithm, Lenstra's algorithm, Dixon's algorithm, and the Continued Fraction Method (CFRAC). A comparison of these algorithms shows that their efficiency largely depends on the specific properties of the number being factored. Fermat's algorithm is highly efficient for numbers with two prime factors that are close in size, as it works by finding factors with a small difference in magnitude [5]. Pollard's rho algorithm, in turn, is better suited for numbers with small factors, as its methods can quickly detect such factors. Lenstra's algorithm is particularly efficient when factoring numbers with large prime factors, especially when one of the factors is a large prime number. This makes it effective for certain types of numbers often used in cryptography. Dixon's algorithm is a generalized version of Fermat's method that uses a factor base and smooth numbers. It is effective for factoring numbers with large but less significant factors, thanks to

its ability to handle numbers with many medium-sized prime factors. The Continued Fraction Method has proven to be the most efficient for numbers with certain structures and small prime factors, allowing it to solve factorizations where other algorithms may be less effective. The results of the study show that choosing a factorization algorithm depends on the specific characteristics of the input numbers, enabling the optimization of the factorization process under different input parameters.

Conclusions. The choice of a factorization algorithm depends on the characteristics of the number, and each algorithm has its advantages in specific situations, making them useful in different contexts of number factorization. Factoring large numbers is the foundation of security for cryptosystems like RSA, where the task of breaking down a number N into prime factors P and Q is critically important. Finding these factors allows the private key to be revealed and the system to be compromised. It is important to note that if there is a specific relationship between P and Q, the factorization problem may become easier, as specialized algorithms are effective for such patterns.

List of references

1. Pollard JM. Theorems on factorization and primality testing. *Mathematical Proceedings of the Cambridge Philosophical Society*. 1974. Volume 76(3). Page 521 – 528. DOI: https://doi.org/10.1017/S0305004100049252.

2. Milanov E. The RSA Algorithm. URL: https://sites.math.washington. edu/~morrow/336_09/ papers/Yevgeny.pdf (date of access: 05.10.2024).

3. Kleinjung T. A Heterogeneous Computing Environment to Solve the 768-bit RSA Challenge. 2012. Volume 15. Page 53 – 68. DOI: https://doi.org/10.1007/s10586-010-0149-0.

4. Pevnev V., Yudin O. Method of testing large numbers for primality. *Advanced Information Systems*. 2024. Volume 8(2). Page 99–106. DOI: https://doi.org/10.20998/2522-9052.2024.2.11.

5. Aminudin A., Cahyono E. A Practical Analysis of the Fermat Factorization and Pollard Rho Method for Factoring Integers. 2021. Volume 12(1). Page 33 – 40. DOI: https://doi.org/10.24843/LKJITI.2021.v12.i01.p04.

Information about the authors

Oles Yudin, a PhD student from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», o.yudin@csn.khai.edu

Vladimir Pevnev, Dr. Sc., professor from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», v.pevnev@csn.khai.edu

Секція 1

МЕТОДИ ЗАХИСТУ САЙТУ «ІНТЕРНЕТ-МАГАЗИНУ» ВІД КІБЕРАТАК

Якубець Б. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Годунов О. С.

Актуальність. Комп'ютерні та інформаційні технології сьогодні охопили багато галузей економіки, а саме торгівлю, і в них є дуже багато факторів небезпеки. Однією із небезпек являється безпека їх торгівельних майданчиків в мережі інтернет. Мова йдеться не лише про безпеку самої компанії, а й про її клієнтів. Для будь-якої сучасної компанії важливо захистити свій сайт від можливих кібератак.

Метою доповіді буде проаналізувати методи які зможуть захистити сайт «інтернет-магазин» від кібератак.

Основні положення. Інформаційна безпека – властивість системи протягом заданого часу протистояти несанкціонованому зняттю та модифікації інформації [1]. Розглянемо основні способи того, як можна вберегти свій сайт «інтернет магазин» від кібератак:

– захист корпоративної пошти. Половина всіх кібератак відбувається з боку корпоративної пошти, адже це критично важливий інструмент для компанії. Якщо безліч рекламних листів одразу не фільтрувати та не видаляти, то вони швидко заповнять всі ресурси сервера. Щоб убезпечитися від таких базових кібератак, поштовий сервіс варто розмістити у хмарі. Наприклад, хмарна платформа Microsoft Azure вже передбачає базовий захист від спаму [2];

– аналіз поведінки внутрішніх користувачів. Система для аналізу поведінки користувачів допомагає виявити нетипові дії співробітників.

– User behavior analytics (UBA) та User and Entity Behavior Analytics (UEBA) дозволяють за допомогою штучного інтелекту створити матрицю поведінки користувача або пристрою. Наприклад, співробітник щодня для робочих задач використовує Outlook, Microsoft Teams та завантажує 10 Мб файлів з пошти. Система запам’ятовує такий перелік дій, а тому помічає, коли раптом користувач починає завантажувати великий об’єм даних з внутрішнього сервера компанії на зовнішній ресурс. Це суттєве відхилення від матриці, а тому UBA одразу реагує. Вона може просто повідомити службу безпеки про нетипову поведінку або ж тимчасово заблокувати дії користувача [2];

– турбота про безпеку клієнтів [3]. Підвищуйте обізнаність клієнтів у питаннях ІБ. Регулярно нагадуйте клієнтам про правила безпечної роботи в інтернеті, роз'яснюйте методи атак та способи захисту. Застерігайте клієнтів від введення облікових даних на підозрілих веб-ресурсах і тим більше від повідомлення такої інформації будь-кому електронною поштою або під час телефонної розмови. Роз'яснюйте клієнтам порядок дій у разі підозри про шахрайство. Повідомляйте клієнтів про події, пов'язані з інформаційною безпекою.

Висновки. Проаналізувавши статистику з сайту компанії techexpert.ua [4], можна побачити , що кількість втрачених записів даних з кожним роком дуже стрімко збільшується – в 2005 році приблизно 15 мільйонів, в 2017 році – приблизно 63 мільйони, а в 2020 вже 101 мільйон втрачених записів даних. Зі звіту також видно, що інвестиції на захист даних за 2020 рік збільшилися на 10% з попереднього року і становлять близько 53 мільярдів доларів. Отже, можемо зробити висновок. З розвитком інформаційних технологій виростає ймовірність бути жертвою кібератаки. Тому варто серйозно віднестися до складової кібербезпеки в вашій компанії, а в нашому випадку сайту «інтернет-магазину».

Список літератури

1. Pevnev, M. Tsuranov, H. Zemlianko, O. Amelina. Conceptual model of information security. ICTM 2020, Lecture Notes in Networks and Systems, Springer, Cham, Switzerland. 2021. Volume 188. Page 158–168. DOI: https://doi.org/10.1007/978-3-030-66717-7_14.
2. 7 способів вас зламати або як захиститися від кібератак. *Kyivstar*. URL: https://hub.kyivstar.ua/news/7-sposobiv-vas-zlamaty-abo-yak-zahystyty-kompaniyu-vid-kiberatak (дата звернення 10.09.2024).
3. Як захиститися від кібер атак. *IT BIZ System Integrator*. URL: https://itbiz.ua/statti-ta-obzori/yak-zahistitisya-vid-kiberatak (дата звернення 10.09.2024).
4. Кількість кібератак збільшується: що з цим робити. *TechExpert IT Company*. URL: https://techexpert.ua/cyber-attacks-number-statistics (дата звернення 10.09.2024).

Відомості про авторів

Якубець Богдан Олександрович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», b.yakubets@student.csn.khai.edu
Годунов Олександр Сергійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.godunov@csn.khai.edu

Секція 1

БЕЗПЕКА ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Яшина В.А.
Хмельницький національний університет
Науковий керівник: Яшина О. М.

Актуальність. В останні роки, з постійним оновленням і розвитком науки і техніки в усьому світі та й в Україні зокрема, технологія ШІ (штучного інтелекту), як нова технологія, постійно впливає на життя людей, і важливість безпеки технології ШІ набуває все більшої актуальності абсолютно в різних сферах.

Загалом, з початку 21-го століття розвиток ШІ досяг свого піку. Однак, через недосконале застосування систем штучного інтелекту існують фактори ризику в його практичному застосуванні, що стосується усіх сфер його використання: від освіти та науки до технологічних рішень у виробництві.

Це означає, що виробники систем штучного інтелекту повинні розглядати безпеку клієнтів як основну вимогу бізнесу, а не просто як технічну функцію, і надавати пріоритет безпеці протягом усього життєвого циклу продукту, від зародження ідеї до планування завершення терміну служби системи. Це також означає, що системи штучного інтелекту повинні бути безпечними для використання від самого початку розробки та впровадження, з мінімальними змінами конфігурації та без додаткових витрат [2] або ці витрати мають бути мінімізовані.

Метою роботи є дослідження безпеки використання штучного інтелекту.

Основні положення. Безпека є вирішальною частиною побудови систем штучного інтелекту. Забезпечення безпеки вимагає ретельного проектування системи з нуля впродовж усього життєвого циклу, щоб різні компоненти працювали разом відповідно до вимог та бізнес-ідеї, а також розробки всіх інструментів, необхідних для нагляду за успішною роботою системи після її реалізації, впровадження та підтримки.

Технічна безпека ШІ є відносно новою галуззю, яка швидко розвивається, і її зміст варіюється від високорівневого та теоретичного до емпіричного та конкретного [1].

Висновки. Отже, обговорення цих ключових питань допоможе у вдосконаленні практик кібербезпеки в контексті розвитку штучного

інтелекту, а також пошуку нових підходів та рішень для створення безпечних систем із використанням штучного інтелекту.

Список літератури

1. Building safe artificial intelligence: specification, robustness, and assurance. *Medium*. URL – https://deepmindsafetyresearch.medium.com/building-safe-artificial-intelligence-52f5f75058f1 (дата звернення 12.09.2024).
2. How to design artificial intelligence that acts nice – and only nice. *Science News Explores*. URL – https://www.snexplores.org/article/artificial-intelligence-ai-safety-good-behavior (дата звернення 29.09.2024).
3. Safety Analysis and Design of Artificial Intelligence System Based on Sensor and AI Technology. URL: https://link.springer.com/chapter/10.1007/978-981-99-1157-8_49 (дата звернення 29.09.2024).
4. Huang, G. Safety Analysis and Design of Artificial Intelligence System Based on Sensor and AI Technology. In: Atiquzzaman, M., Yen, N.Y., Xu, Z. (eds) Proceedings of the 4th International Conference on Big Data Analytics for Cyber-Physical System in Smart City – Volume 2. BDCPS 2022. Lecture Notes on Data Engineering and Communications Technologies, Volume 168. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-99-1157-8_49.

Відомості про авторів

Яшина Вікторія Андріївна, студентка кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехнік, Хмельницький національний університет, yashina.victorya@gmail.com
Яшина Оксана Миколаївна, доцент кафедри інженерії програмного забезпечення, Хмельницький національний університет, к.т.н., oksana.yashyna@ukr.net

ТЕЗИ ДОПОВІДЕЙ

Секція 2. Функційна безпека

Section 2

SIGNAL DIRECTION OF ARRIVAL ESTIMATION USING DELAY AND SUM BEAMFORMING ALGORITHM

Filippos Papalos
Hellenic Military Academy, Athens, Greece
Scientific adviser: Nikolaos Doukas, Nikolaos G Bardis

Relevance. Locating the source of a signal is often associated with radiogoniometry, a reliable method but one with significant limitations. These include the necessity of at least three stations, high power consumption, and substantial distances between stations to ensure accuracy.
Beamforming, in contrast, offers a more advanced and efficient alternative by leveraging antenna arrays to transform omnidirectional antennas into directional elements. This approach enhances the signal-to-noise ratio, reduces interference, and saves energy by concentrating power in the required direction. Using beamforming, an antenna array can act as a virtual directional antenna, achieving high precision in detecting and receiving signals.

Purpose. This research aims to develop a program that uses two beamforming stations to estimate the Direction of Arrival (DOA) of a signal. By attaching specific weights to the antennas in an array, the system focuses the beam in a chosen direction. These weights depend solely on the array geometry and the desired angle. By calculating the weights for all possible angles and measuring the signal's intensity in each direction, the peak intensity identifies the DOA. With the DOAs from two stations and their known locations, the transmitter's exact location can be determined through triangulation.

Principal provisions. The program, written in Python, simulates the reception of a signal from a specified direction and estimates its DOA using two beamforming arrays, each consisting of three antennas. It operates by taking the transmitter's location as input, simulating the signal's angles of arrival at each array, and collecting samples. These samples are processed through a DOA estimation algorithm to determine the DOAs from both arrays. Finally, the program uses triangulation to calculate the transmitter's location and plots it on a two-dimensional plane.

Conclusion. The simulation is highly accurate, incorporating various factors to ensure precision. Experimental results demonstrate that the program

consistently calculates the transmitter's location with great accuracy, even over longer distances. The compact geometry of the antenna arrays further enhances the system's suitability for remote applications. This work highlights the potential of beamforming as an effective solution for signal direction finding, combining precision, efficiency, and versatility in its design.

List of references

1. A. Downey. *Think DSP: digital signal processing in Python*, First edition. Sebastopol, CA: O'Reilly Media Inc. 2016.
2. M. Lichtman. PySDR: A Guide to SDR and DSP using Python. *PySDR*. URL – https://pysdr.org (date of access: 13.11.2024).
3. A. B. Downey. *Think Python: how to think like a computer scientist*, Third edition. Beijing Boston Farnham Sebastopol Tokyo: O'Reilly, 2024.

Information about the authors

Filippos Papalos, M.Sc., Hellenic Military Academy, f.papalos@outlook.com
Nikolaos Doukas, Associate Professor, Hellenic Military Academy, nd@ieee.org
Nikolaos G Bardis, Professor, Hellenic Military Academy, bardis@ieee.org

Section 2

SMAD: A REAL TIME NETWORK ATTACK DETECTOR

Pavlos Konstantinidis
Hellenic Military Academy, Athens, Greece
Scientific adviser: Nikolaos Bardis

Relevance. Cyberattacks targeting information systems have evolved over the years, and attackers are using increasingly sophisticated tools and techniques to accomplish their malicious goals. However, the means used by malicious users are also available to defenders. Therefore, it is important to use as effectively as possible the information that can be obtained from the existing tools and attacking techniques, but also to invent new tools to adequately cover the needs of an information system to monitor the events that occur, detect malicious actions and take appropriate measures to mitigate the effects of attacks.

According to the US Department of Justice [1], only one in seven cybercrimes is reported, meaning a huge number of attacks remain undetected. This is also an indication of how little IT budgets are allocated for security in businesses. In research conducted by Vanta [2], 60% of the organizations surveyed, noted that they intend to reduce the budget spent on security. In addition, many security monitoring solutions are not that cost effective even for large organizations [3].

The purpose of this research is to provide a security tool that is capable of monitoring network traffic in order to detect attacks in real time. This tool is written in the python programming language and has a graphical user interface. Furthermore, to facilitate cybersecurity researchers, it has been programmed to be extensible in terms of its functionality. For example, it is possible for a programmer to create a module responsible for detecting an attack and easily incorporate it into the main program.

Principal provisions. The SMAD (System Monitoring & Attack detector) program [4] can be used for detecting attacks mainly occurring on computer networks utilizing the scapy python library. The scapy python library provides the necessary code to help a user to send, sniff, dissect and forge network packets. This specific program is utilizing unix sockets to detect attacks, so it needs to be executed on a Unix based system with a display for the graphical user interface. In addition, this tool can be extended by developing new modules to detect other types of attacks.

Currently, the SMAD program can detect three (3) network attacks: the ping sweep attack utilized during the enumeration phase of an attack, the

deauthentication attack, which is used to retrieve a network's password hash and the arp poisoning attack, used to conduct man-in-the-middle campaigns.

Conclusion. Taking everything into consideration, attack campaigns have developed rapidly. Hackers are now using more specialized tools and techniques to compromise systems. For this reason, it is important for organizations to spend their efforts in securing the businesses of upcoming threats, by using tools or developing new ones to meet their needs.

List of references

1. Report of the attorney general's cyber digital task force. *U.S. Department of Justice*. URL – https://www.justice.gov/archives/ag/page/file/1076696/dl (date of access: 01.11.2024).
2. State of Trust Report 2023. *Vanta*. URL – https://8588479.fs1.hubspotusercontent-na1.net/hubfs/8588479/2023%20State%20of%20Trust%20Report.pdf (date of access: 01.11.2024).
3. Managed SIEM Pricing Guide. *UnderDefence Cybersecurity*. URL – https://underdefense.com/blog/managed-siem-pricing-guide (date of access: 02.11.2024).
4. Security monitoring. *GitHub*. URL – https://github.com/paulkon68/Security_Monitoring (date of access: 03.11.2024).

Information about the authors

Pavlos Konstantinidis, MSc student, Hellenic Military Academy, paulkon68@gmail.com
Nikolaos G. Bardis, Professor, Hellenic Military Academy, bardis@ieee.org

Section 2

ADDRESSING A SYNTHETIC DATA GAP IN REMOTE SENSING: ARTIFICIAL AREA GENERATION USING LANDSCAPE METRICS

Michail Kefalakis
Hellenic Army Academy, Athens, Greece
Scientific adviser: Nikolaos V. Karadimas

Relevance. Remote sensing is a rapidly evolving field, with extensive research proposing solutions for training AI models to interpret complex spatial data. Approaches that leverage deep learning require large amounts of high-quality labeled data, which are typically manually annotated by humans. The process of collecting and labeling this data can be time-consuming and resource-intensive. Additionally, limited geographic availability of data can further impede model training, creating additional challenges [1]. A commonality across remote sensing imagery is its inherent depiction of landscape structure, an element pivotal for understanding geographic variability. Paradoxically, while landscape structure significantly influences remote sensing analytics, studies focusing on its direct application for selecting and generating synthetic data are limited.

The purpose of this work is to propose a novel method that incorporates landscape structure statistics to guide the selection and generation of synthetic training data. Our approach aims to mitigate the impact of geographic variability by ensuring that underrepresented classes are adequately synthesized. This methodology provides a more robust foundation for training AI models, ultimately enhancing the accuracy and generalizability of remote sensing applications.

Principal provisions. To test this approach, images from the OpenEarthMap dataset, specifically depicting Zanzibar, were utilized. The dataset included panchromatic images alongside their corresponding segmented counterparts. Semantic segmentation has emerged as a foundational research area in computer vision in recent years, underpinning numerous applications. Additionally, various remote sensing-specific datasets have been developed, providing imagery captured from a nadir perspective [2]. Reason for the need of segmented imagery in the context of this research is the calculation of the landscape metrics and fragmentation indices, using neutral landscape generators, a distinct field that frequently combines data from remote sensing sources to produce additional raster products for simulation. This area, encompassing landscape generators, is more commonly applied in ecology and evolutionary sciences to create

segmented, simulated landscapes [3, 4]. After calculating landscape metrics and fragmentation indices, the dataset is processed using Principal Component Analysis (PCA) to reduce its dimensionality to two principal components. This transformation enables a visual representation of the relationships between landscapes, where proximity in the plot indicates greater similarity, and distance reflects less similarity. Regions of the plot with sparse data points highlight unique or underrepresented landscapes, signaling an imbalance in the dataset. To address this, synthetic data points are generated at user-specified distances from the original points in these underrepresented areas. Each synthetic point is assigned its own landscape metrics and fragmentation indices. These metrics are then used to create new segmentation images, which are subsequently translated into detailed digital landscapes using the Unity Game Engine.

Conclusions. By utilizing landscape metrics and fragmentation indices, a novel approach to addressing dataset imbalance in remote sensing emerges, centered on the one constant in remote sensing imagery: the landscape itself. This methodology enables the generation of digitally replicated, enhanced areas that fill gaps in underrepresented portions of datasets. These synthetic landscapes serve as a vital step toward improving data diversity and quality, ultimately acting as a cornerstone for more robust and generalizable artificial intelligence model training.

List of references

1. Song, J., Chen H., Xuan, W., Xia J., Yokoya N. Synrs3d: A synthetic dataset for global 3d semantic understanding from monocular remote sensing imagery. 2024. *arXiv preprint arXiv:2406.18151*.

2. Lyu Y., Vosselman G., Xia G. S., Yilmaz A., Yang M. Y. UAVid: A semantic segmentation dataset for UAV imagery. 2020. *ISPRS journal of photogrammetry and remote sensing*, 165. Page 108-119.

3. Osborne P. E., Alvares-Sanches T. Quantifying how landscape composition and configuration affect urban land surface temperatures using machine learning and neutral landscapes. 2019. *Computers, Environment and Urban Systems*, *76*, Page 80-90.

4. van Strien M. J., Slager C. T., De Vries B., Grêt-Regamey A. An improved neutral landscape model for recreating real landscapes and generating landscape series for spatial ecological simulations. *Ecology and Evolution*, *6*(11), 3808-3821.

Information about the authors

Michail Kefalakis, M.Sc., Department of Military Sciences of the Hellenic Army Academy, mikkef@hotmail.com

Nikolaos V. Karadimas, Associate Professor, Department of Military Sciences of the Hellenic Army Academy, nkaradimas@sse.gr

Section 2

Future Media Challenges in the Age of AI

Yulian Hristov
Institute of ICT, Bulgarian Academy of Sciences
Debati.BG, Sofia, Bulgaria

Relevance. Today's media reality of social networks is constantly and profoundly changing our understandings, needs & opportunities and thus sustainably transforms the overall digital lifestyle in the new age of AI. The new media accents today are mostly giving priority to the role of AI, audience preferences and interactiveness, together with information trust and origin with both human and machine perspectives. However, these changes create also multiple transformational transcends for the future smart media environment and new society that have to be studied proactively. The narratives that drive human civilization, which have been accumulated over millennia and have created enduring and resilient archetypes, can today be remodulated and remodified by Artificial Intelligence, which can already question authorities, leaders and existing political and social orders, but also provokes a discussion about: "Who makes the decisions - the human or the machine?" [1, 2].

The purpose of this work is to investigate, study and analyze the risks in media transcendents and the influence over recipient's behavior. The work combines analytical modeling of future media environment expectations with users' responses of different multimedia modalities. Additionally, some experimental AI applications are added to advance the futurism of the media. All experiments are prototyped in an experimental test bed-environment, achieving an extensible outlook.

Principal provisions. Disinformation emerges as a leading risk for the next 2 years (2024-2025), which could lead to widening gaps between societies and social groups [3]. The media of the future have virtually unlimited possibilities in collecting data about users, and in addition of generating information, as they will profile the end users to whom it should be delivered [4]. This leads to an additional segmentation of end user groups, and from there to social, political, etc. clashes. In addition the creation of new realities, including: Virtual Reality (VR), Augmented Reality (AR) & Extended Reality (XR), the generative Artificial Intelligence has the ability to also create campaigns – e.g., a political platform that reaches profiled end users, with whom it can even enter into a communication mode, including an audiovisual interactive dialogue.

Conclusions. The proposed solution is expected to mark some of the future media development challenges and pitfalls in a proactive manner, and thus

provide a real support to the establishment of a more innovative, secure and resilient future society in the new age of AI, while saving human intellect dominance. Obviously, there is a vital need for investment of additional efforts to develop tools for automatic detection of disinformation with the construction of databases for disinformation narratives [5].

List of references

1. Harari, Yuval Noah. Homo Deus: A Brief History of Tomorrow. Vintage, 2017. Page 328.
2. Harari Yuval Noah. AI and the future of humanity, Frontiers Forum Live 2023. *YouTube*. URL – https://www.youtube.com/watch?v=azwt2pxn3UI (date of access: 05.11.2024).
3. World Economic Forum. "The Global Risks Report 2024". 2024.
4. Custom GPT For Advertising Campaigns – The Ultimate Guide. *Poll the People*. URL – https://pollthepeople.app/custom-gpt-for-advertising-campaigns (date of access: 06.11.2024).
5. Bontcheva K., et al. Generative AI and Disinformation: Recent Advances, Challenges, and Opportunities. *European Digital Media Observatory*. URL – https://edmo.eu/edmo-news/new-white-paper-on-generative-ai-and-disinformation-recent-advances-challenges-and-opportunities (date of access: 07.11.2024).

Information about the author

Yulian Hristov, Assistant Professor at the Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, julianvhristov@gmail.com

Секція 2

АНАЛІЗ ІСНУЮЧИХ ЗАСОБІВ ТЕЛЕМЕТРІЇ В IoT

Батраченко Ю.В.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник: Перепелицин А. Є.

Актуальність. Однією з проблем в системах технологій інтернету речей (IoT) – є отримання інформації о стані системи на відстані, вона полягає в точності та надійності передачі даних. Тому для вирішення цього питання необхідно дослідити існуючі рішення системи дистанційної телеметрії розумного будинку.

Метою роботи є аналіз можливих варіантів побудови систем телеметрії для побутових IoT рішень. Для досягнення цієї мети потрібно провести аналіз існуючих рішень для здійснення моніторингу в IoT, проаналізувати можливості їх побудови з використанім розповсюджених каналів зв'язку та датчиків, проаналізувати засоби візуалізації та отримання інформації від системи, а також побудувати практичний приклад системи.

Основні положення. Для передачі отриманих даних з датчиків на платформи для моніторингу в IoT використовується технології взаємодії пристроїв з доступом в Інтернет [1]. Це може бути Wi-Fi або Bluetooth, який використовується з пристроями з низьким енергоживленнями. Натомість Wi-Fi забезпечує швидкий обмін [2]. Для обміну інформацією використовуються хмарні сервіси [3].

Датчики в IoT відграють важливу роль збору та моніторингу інформації. Зазвичай вони невеликі, мають широкий спектр змінних та економічні. Використовують різні типи датчиків. Розповсюдженими є датчики, що сумісні з платформою Arduino, що робить їх зручними для використання у задачах, що передбачають швидке створення прототипів.

Процес збору та обробки даних, які були отримані вході роботи датчиків може бути реалізований на серверах або хмарних сервісах. Завдяки хмарним сервісам користувач має змогу керувати та отримувати проаналізовані дані про стан систем.

Для практичної реалізації датчика вимірювання температури в системі розумний будинок можна використати датчик DS18B20 на базі мікроконтролера Arduino UNO. Для зв'язку між прототипом системи та хмарним сервісом можливим варіантом є використання Wi-Fi, через те що для модулю зв'язку є бібліотеки та можливе зручне підключення до Інтернету. Для збору та отримання даних може бути використаний сервіс

ThingSpeak. Ця хмарна платформа дає змогу під'єднаним пристроям взаємодіяти між собою. Вона підтримує роботу достатньої кількості пристроїв та повідомлень, а також використовуватися для зручного відображення інформації від датчиків.

Проте недоліками такої системи є енергозалежність та необхідність налаштувань під'єднання для кожного екземпляру.

Висновки. В роботі був проведений аналіз існуючих способів телеметрії побутових систем та IoT. Розглянуті засоби, які використовуються під час розробки такої системи та варіанти їх взаємодії між собою. Також була реалізована система вимірювання температури, та представлено вирішення проблеми отримання інформації на відстані і передачі даних з Інтернет підключенням.

Список літератури

1. Вдовіченко, О. О. Організація взаємодії пристроїв з доступом в інтернет на основі мікроконтролерів із обмеженою кількістю ресурсів [Текст] / О. О. Вдовіченко, А. Є. Перепелицин // Авіаційно-космічна техніка і технологія. 2023. № 6. С. 76–85. DOI: https://doi.org/10.32620/aktt.2023.6.09.

2. Perepelitsyn, A. Service for communication of devices with internet access: analysis of technologies and method of creation [Text] / A. Perepelitsyn, O. Vdovichenko, & V. Mikhalevskyi // Radioelectronic and Computer Systems. 2023. No. 4. Page 197–208. DOI: https://doi.org/10.32620/reks.2023.4.14.

3. Pierleoni P., Concetti R., Belli A., Palma L. «Amazon, Google and Microsoft Solutions for IoT: Architectures and a Performance Comparison» in IEEE Access. 2020. Volume 8. Page 5455-5470. DOI: 10.1109/ACCESS.2019.2961511.

Відомості про авторів

Батраченко Юрій Володмирович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.batrachenko@student.csn.khai.edu

Перепелицин Артем Євгенович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.perepelitsyn@csn.khai.edu

Секція 2

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БПЛА З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ: СИСТЕМАТИЗАЦІЯ АТАК, КОНТРЗАХОДІВ ТА МОДЕЛЕЙ ОЦІНЮВАННЯ

Веприцька О.Ю.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник: Харченко В.С.

Актуальність. У зв'язку зі стрімким зростанням ринку безпілотних літальних апаратів (БПЛА), який, за прогнозами, досягне 50,4 мільярда доларів США до 2032 року [1], забезпечення їх кібербезпеки стає необхідністю. Інтеграція штучного інтелекту (ШІ) в БПЛА значно підвищує їх автономність, функціональність та здатність адаптуватися до змін у середовищі, але водночас створює нові вразливості до кібератак. Важливість цих викликів зростає в умовах російсько-української війни, де БПЛА стали базою для окремого виду ЗСУ.

Метою роботи є аналіз загроз, атак та втручань, а також обґрунтування вибору контрзаходів для підвищення рівня кібербезпеки систем БПЛА з урахуванням їхніх вразливостей і використання ШІ для посилення атак і засобів захисту. Підхід дослідження ґрунтується на:

– застосуванні методології Security Informed Safety [2] та техніки IMECA для систем БПЛА з урахуванням особливостей використання ШІ;

– використанні моделі якості ШІ для обґрунтування вимог до ШІ в БПЛА [3] як засобів виконання функцій та захисту кіберактивів.

Основні положення. В рамках проведеної роботи:

– визначено основні перешкоди для впровадження ШІ в системи БПЛА, з огляду на ризики безпеки, технічні обмеження та їх кібербезпеку;

– запропоновано класифікацію контрзаходів з урахуванням аспекту ШІ;

– проаналізовано контрзаходи на регуляторному та технічному рівнях, а також оцінено їхній вплив на загальні ризики кібербезпеки та безпеки;

– наведено приклад створення моделей якості, ризик орієнтована (IMECA), логіко-ймовірнісна (дерева атак) та стохастична (марковська модель) для оцінки ШІ-систем на борту та засобів захисту БПЛА, що використовуються для задачі розмінування.

Висновки. Основний внесок цього дослідження полягає в класифікації загроз та засобів захисту з урахуванням аспекту ШІ та прикладі

впровадження стандартизації компонентів ШІ в БПЛА залежно від визначених функцій [4]. Запропонована систематизація включає регуляторні методи, орієнтовані переважно на легалізацію використання, стандартизацію та контроль якості БПЛА і ШІ, а також відповідні програмно-технічні засоби реалізації цих методів. Запропонований підхід може бути поширений на аналіз безпеки критичних систем, що працюють в агресивному інформаційному та фізичному середовищі, і забезпечення проактивного захисту від атак, посилених засобами ШІ.

Список літератури

1. Global Unmanned Aerial Vehicle Market 2024-2033. *Custom Market Insights*. URL – https://www.custommarketinsights.com/report/unmanned-aerial-vehicle-market (дата звернення: 02.11.2024).
2. Illiashenko O, Babeshko I., Kharchenko V., Fesenko H., Di Giandomenico F. Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection / Entropy. 2023. Volume 25(8). Page 1123. DOI: https://doi.org/10.3390/e25081123.
3. Kharchenko V., Fesenko H., Illiashenko O. Quality Models for Artificial Intelligence Systems: Characteristic-Based Approach, Development and Application. Sensors. 2022. Volume 22(13). Page 4865. DOI: https://doi.org/10.3390/s22134865.
4. Veprytska O., Kharchenko V. Analysis of AI powered attacks and protection of UAV assets: quality model-based assessing cybersecurity of mobile system for demining. International Workshop on Intelligent Information Technologies & Systems of Information Security. 2024. URL: https://ceur-ws.org/Vol-3675/paper26.pdf (дата звернення: 02.11.2024).

Відомості про авторів

Веприцька Олена Юріївна, аспірантка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.veprytska@csn.khai.edu
Харченко Вячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, v.kharchenko@csn.khai.edu

Секція 2

ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ НЕЙРОННИХ МЕРЕЖ В УМОВАХ НЕВИЗНАЧЕНОСТІ

Заіка В. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Шостак А. В.

Актуальність. Штучний інтелект та нейронні мережі стали невід'ємною частиною критично важливих систем, таких як автоматизовані транспортні засоби, системи медичної діагностики, розумні енергетичні мережі та робототехніка [1]. Однак їх широке впровадження породжує нові ризики для функціональної безпеки, зокрема в умовах невизначеності. До таких ризиків належать помилки через недостатню кількість або низьку якість навчальних даних, уразливості до атак типу "adversarial examples", а також труднощі з прогнозуванням поведінки нейромереж у нестандартних сценаріях [2].

За даними дослідження Microsoft Research, майже 30% автономних систем, що використовують штучний інтелект, демонструють непередбачувану поведінку в умовах неповних або суперечливих даних [3]. Така непередбачуваність створює загрозу для функціональної безпеки систем і вимагає нових підходів до їх проектування, тестування та забезпечення надійності.

Метою даної роботи є вивчення ключових викликів забезпечення функціональної безпеки нейромереж в умовах невизначеності, аналіз сучасних методів підвищення їх стійкості, а також розробка рекомендацій для впровадження цих методів у практику.

Особливу увагу приділено адаптації алгоритмів машинного навчання до роботи в умовах обмеженої інформації, неконтрольованих змін середовища або навмисних атак. Також досліджуються способи оцінки ризиків і тестування моделей у критичних системах, таких як автономні транспортні засоби та медичні пристрої. Це дозволить не лише підвищити надійність таких систем, але й закласти основу для стандартизації процесів забезпечення функціональної безпеки в умовах стрімкого розвитку технологій штучного інтелекту.

Основні положення. Для підвищення надійності нейромереж запропоновано навчання з урахуванням найгірших сценаріїв. Використання підходів, що дозволяють нейромережам бути стійкими до несподіваних змін у середовищі. Інтерпретація результатів роботи

нейромереж. Використання методів Explainable AI для ідентифікації можливих помилок у критичних сценаріях. Захист від атак. Застосування алгоритмів захисту від атак типу "adversarial examples", зокрема обробка вхідних даних за допомогою розсіювання шуму або детекції аномалій.

Висновки. В умовах стрімкого впровадження нейромереж у критично важливі системи забезпечення їх функціональної безпеки стає пріоритетним завданням. Реалізація запропонованих підходів сприятиме зниженню ризиків, пов'язаних з непередбачуваною поведінкою нейромереж, і підвищить надійність таких систем у нестабільних умовах.

Список літератури

1. He K., Zhang X., Ren S., Sun J. Deep Residual Learning for Image Recognition. IEEE Conference on Computer Vision and Pattern Recognition (CVPR). 2016. DOI: https://doi.org/10.1109/CVPR.2016.90.
2. Goodfellow I. J., Shlens J., Szegedy C. Explaining and Harnessing Adversarial Examples. International Conference on Learning Representations (ICLR). 2015. DOI: https://doi.org/10.48550/arXiv.1412.6572.
3. Amodei D., Olah C., Steinhardt J., Christiano P., Schulman J., Mane, D. (2016). Concrete Problems in AI Safety. DOI: https://doi.org/10.48550/arXiv.1606.06565.

Відомості про авторів

Заіка Владислав Віталійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», v.v.zaika@student.csn.khai.edu
Шостак Анатолій Васильович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., доцент, a.shostak@csn.khai.edu

Секція 2

МЕТОДИ БЕЗПЕЧНОЇ ІНТЕГРАЦІЇ БЛОКЧЕЙНУ ETHEREUM З СИСТЕМАМИ ІНТЕРНЕТУ РЕЧЕЙ: РОЗРОБКА ТА ОПТИМІЗАЦІЯ

Зарудний І. С.
Сумський державний університет
Науковий керівник: Любчак В. О.

Актуальність. З розвитком Інтернету речей (IoT) виникає потреба у підвищенні безпеки та прозорості обміну даними між пристроями. Використання блокчейн-технологій, зокрема Ethereum, дає змогу забезпечити децентралізацію, захист від несанкціонованого доступу та підвищити стійкість систем до кібератак. Однак інтеграція блокчейну з IoT несе виклики у вигляді обмежень пропускної здатності, енергоспоживання та масштабованості.

Метою є розробка методів та інформаційних технологій для забезпечення безпечної та ефективної інтеграції блокчейну Ethereum з IoT-системами. Особлива увага приділяється впровадженню та апробації технології смарт-контрактів для управління доступом і автоматизації процесів у мережах Інтернету речей. Апробація виконана на основі експериментальної платформи, що дозволяє оцінити ефективність розроблених методів у реальних умовах.

Основні положення. Основні положення роботи включають розробку підходів до використання смарт-контрактів Ethereum для управління доступом в IoT-системах, що забезпечують автоматизацію та безпеку взаємодії між пристроями. Особливу увагу приділено оптимізації споживання енергії IoT-пристроїв шляхом мінімізації кількості транзакцій та застосування енергоефективних алгоритмів консенсусу. Також пропонуються рішення для зменшення затримки транзакцій у блокчейн-мережі за допомогою впровадження шарових протоколів (Layer 2) і оптимізації розподілу навантаження між вузлами. Крім того, розроблені методи спрямовані на захист конфіденційності даних і забезпечення анонімності транзакцій за допомогою криптографічних технологій, таких як zk-SNARKs, що гарантують безпеку інформації без розкриття її змісту стороннім.

Висновки. У результаті дослідження було розроблено та апробовано методи безпечної інтеграції блокчейну Ethereum з системами Інтернету речей. Запропоновані підходи демонструють високу ефективність у

забезпеченні безпеки та автоматизації процесів взаємодії між IoT-пристроями. Зокрема, використання смарт-контрактів дозволяє суттєво знизити ризики несанкціонованого доступу до даних та забезпечити децентралізоване управління доступом. Однак впровадження блокчейну в IoT не позбавлене недоліків. Серед основних проблем можна виділити обмеження пропускної здатності, високе енергоспоживання IoT-пристроїв та затримки при обробці транзакцій. Для компенсації цих недоліків у роботі було запропоновано впровадження шарових протоколів (Layer 2) для оптимізації обробки транзакцій та зменшення затримок. Також розроблено енергоефективні алгоритми консенсусу, які суттєво знижують навантаження на пристрої з обмеженими ресурсами. Додатково було впроваджено криптографічні механізми, такі як zk-SNARKs, що забезпечують високий рівень конфіденційності даних без збільшення обчислювальної складності. Це дозволяє IoT-системам зберігати анонімність транзакцій, водночас підтримуючи високий рівень безпеки. Очікується, що запропоновані методи сприятимуть зниженню витрат ресурсів, підвищенню продуктивності та масштабованості IoT-систем, що використовують блокчейн Ethereum.

Список літератури

1. Сухомлин С. В., Ковальчук В. А. Інтеграція блокчейн-технологій у системи Інтернету речей. У кн.: Сучасні інформаційні технології: тези доп. 10-ї міжнар. наук.-практ. конф., 2023. м. Київ. – Київ: Наук. думка, 2023. – 92 с.

2. Puthal D., Malik N., Mohanty S. P. Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems. IEEE Consumer Electronics Magazine, 2018. Volume 7(4). Page 6-14.

3. Dorri A., Kanhere S. S., Jurdak R. Blockchain in Internet of Things: Challenges and Solutions. Computer Communications, 2019. Volume 36(3). Page 231-241.

4. Захарченко І. А., Ткаченко О. М. Смарт-контракти та їх застосування у блокчейн-мережах. Інформаційні системи і технології, 2022, №2, с. 34-45.

5. Makhdoom I., Abolhasan M., Lipman J. Blockchain for IoT: The Challenges and a Way Forward. Future Generation Computer Systems, 2019. 92. Page 610-626.

Відомості про авторів

Зарудний Іван Сергійович, магістрант кафедри комп'ютерних наук, СумДУ, zarudnyi.ivan@gmail.com

Любчак Володимир Олександрович, професор кафедри комп'ютерних наук, СумДУ, к.ф.-м.н., доцент, v.liubchak@dcs.sumdu.edu.ua

Секція 2

ВИКОРИСТАННЯ РЕКУРЕНТНОЇ НЕЙРОННОЇ МЕРЕЖІ НА БАЗІ FPGA ДЛЯ ПЕРЕВІРКИ ВИКОНУВАНИХ ФАЙЛІВ НА ФАЙЛОВОМУ СЕРВЕРІ

Зубрицький О. О.
Донбаська державна машинобудівна академія
Науковий керівник: Донченко Є. І.

Актуальність. В останні роки спостерігається збільшення обсягів даних що зберігаються на файлових серверах, внаслідок зростання використання мультимедійного контенту, хмарних послуг та розвитку цифрових технологій. Використання заражених виконуваних файлів вірусами, може призвести до різних ситуацій: крадіжки корпоративної інформації, крадіжки фінансової інформації, збоїв у роботі персональних комп'ютерів, шифрування або видалення файлів [1, 2]. Усі данні ситуації можуть завдати значних фінансових збитків [3]. Перевірка виконуваних файлів у реальному часі сильно навантажує центральний процесор серверу та знижує якість послуг. Використання нейронної мережі дозволить багатократно збільшити швидкість перевірки файлів за рахунок реалізації паралельних обчислень на FPGA.

Метою дослідження є збільшення продуктивності перевірки виконуваних файлів шляхом використання рекурентної нейронної мережі, реалізованої на базі FPGA.

Основні положення дослідження. Останнім часом технологічні лідери докладають значних зусиль для кращої інтеграції FPGA в сервери центрів обробки даних (наприклад, Microsoft Catapult, IBM CAPI) [4]. FPGA забезпечує кращу продуктивність у порівнянні з CPU та GPU, оскільки вбудовані в FPGA, B-RAM, DSP та реконфігуровані структури дозволяють ефективно використовувати дрібний паралелізм з матриць малого/середнього розміру [4].

Рекурентні нейронні мережі забезпечують високу точність аналізу послідовних наборів [4]. Основною особливістю, яка відрізняє RNN від інших нейронних мереж, є формування прямих циклів між нейронами. Це забезпечує мережу тимчасовою обробкою та навчанням послідовності, шляхом створення внутрішніх станів. Ці деталі та складність RNN зазвичай призводять до того, що вони вимагають більшого обсягу пам'яті, а також більшого часу виконання [5]. Використання FPGA дозволить збалансувати ці недоліки RNN.

Висновки. Використання RNN дозволить збільшити точність перевірки виконуваних файлів. FPGA забезпечує кращу продуктивність у порівнянні з CPU та GPU серверного обладнання.

Список літератури

1. Challenges and pitfalls in malware research [Electronic resource] / Marcus Botacin [et al.] // Computers & Security. 2021. Volume 106. Page 102287. DOI: https://doi.org/10.1016/j.cose.2021.102287.
2. We need to talk about antiviruses: challenges & pitfalls of AV evaluations [Electronic resource] / Marcus Botacin [et al.] // Computers & Security. 2020. Volume 95. Page 101859. DOI: https://doi.org/10.1016/j.cose.2020.101859.
3. Bensaoud A. A Survey of Malware Detection Using Deep Learning [Electronic resource] / Ahmed Bensaoud, Jugal Kalita, Mahmoud Bensaoud // SSRN Electronic Journal. 2023. DOI: https://doi.org/10.1016/j.mlwa.2024.100546.
4. Accelerating recurrent neural networks in analytics servers: Comparison of FPGA, CPU, GPU, and ASIC [Electronic resource] / Eriko Nurvitadhi [et al.] // 2016 26th International Conference on Field Programmable Logic and Applications (FPL), Lausanne, Switzerland. 2016.
5. A Model Based on LSTM Neural Networks to Identify Five Different Types of Malware [Electronic resource] / Eduardo de O. Andrade [et al.] // Procedia Computer Science. 2019. Volume 159. Page 182–191. DOI: https://doi.org/10.1016/j.procs.2019.09.173.

Відомості про авторів

Зубрицький Олексій Олександрович, аспірант кафедри автоматизації виробничих процесів, Донбаська державна машинобудівна академія, salamandra199720@gmail.com

Донченко Євген Іванович, ст. викладач кафедри автоматизації виробничих процесів, Донбаська державна машинобудівна академія, к.т.н. donchenko.egen@gmail.com

Секція 2

ФУНКЦІОНАЛЬНА БЕЗПЕКА РОЗУМНИХ БУДИНКІВ

Кіріченко Д. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Землянко Г. А.

Актуальність. Розвиток Інтернету речей (IoT) та штучного інтелекту зробив розумні будинки звичним явищем, що забезпечує комфорт, ефективність та автоматизацію [1, 2]. Проте інтеграція інтелектуальних систем підвищує ризик збоїв і зловмисного втручання, що може призвести до матеріальних збитків і порушення конфіденційності. Тому функціональна безпека розумного будинку є ключовою для захисту користувачів і стабільної роботи систем [2, 3].

Метою роботи є аналіз основних загроз для функціональної безпеки та розробка рекомендацій для підвищення надійності та захисту функцій автоматизованих систем.

Основні положення. Розумний будинок – це комплекс систем і пристроїв, об'єднаних в єдину мережу для забезпечення автоматизації, зручності та енергоефективності. Основними компонентами є системи управління освітленням, клімат-контролю, системи безпеки, медіасистеми та побутова техніка. Всі елементи взаємодіють між собою за допомогою дротових або бездротових каналів зв'язку та центрального контролера [3, 4]. В роботі розглянуто основні загрози функціональної безпеки [4, 5]. Кібератаки: злом мереж через вразливості Wi-Fi і Bluetooth, перехоплення даних через незашифровані канали, та використання пристроїв зі слабкими паролями у DDoS-атаках. Програмні вразливості: недостатні оновлення прошивки і незахищені API створюють ризики несанкціонованого доступу. Фізичні загрози: відключення живлення без резерву та зношеність обладнання можуть порушити роботу систем безпеки. Стандартні паролі: прості паролі полегшують доступ зловмисникам. Соціальна інженерія: використання фішингу для отримання доступу від недосвідчених користувачів. В роботі також розглянуто засоби підвищення функціональної безпеки: сегментація мережі для ізоляції критично важливих систем від загальнодоступного інтернету; системи виявлення вторгнень для моніторингу аномальних дій і запобігання несанкціонованому доступу; регулярне оновлення програмного забезпечення для усунення вразливостей безпеки; використання багатофакторної автентифікації для контролю доступу до систем

управління; резервне копіювання даних для збереження налаштувань і забезпечення безперебійної роботи в разі збою [4, 5].

Висновки. Функціональна безпека розумних будинків є необхідною умовою для їх повноцінної роботи та захисту мешканців. Впровадження заходів з підвищення функціональної безпеки мінімізує ризики, пов'язані з кібератаками і технічними збоями, а також забезпечує стабільну, безпечну і комфортну роботу розумного будинку.

Список літератури

1. Mantas G., Lymberopoulos D., Komninos N. Security in smart home environment. *Wireless technologies for ambient assisted living and healthcare*. Page 170–191. DOI: https://doi.org/10.4018/978-1-61520-805-0.ch010.

2. Systematic analysis of safety and security risks in smart homes / H. Ullah Khan et al. *Computers, materials & continua*. 2021. Volume 68(1). Page 1409-1428. DOI: https://doi.org/10.32604/cmc.2021.016058.

3. Dewsbury G., Linskell J. Smart home technology for safety and functional independence: The UK experience. *NeuroRehabilitation*. 2011. Volume 28(3). Page 249–260. DOI: https://doi.org/10.3233/nre-2011-0653.

4. Al-Wahah M., Al-Hossenat A. Safety assurance in IoT-based smart homes. *Edge computing - architecture and applications for smart cities [working title]*. 2024. DOI: https://doi.org/10.5772/intechopen.1005492.

5. Smart Home Automation Safety and Security. *Advantage Insuarance Solutions*. URL – https://www.teamais.net/blog/keeping-your-child-and-home-safe-with-smart-technology (дата звернення: 03.11.2024).

Відомості про авторів

Кіріченко Данило Володимирович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.v.kirichenko@student.csn.khai.ed

Землянко Георгій Андрійович, ст. викладач кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», PhD з кібербезпеки, g.zemlynko@csn.khai.edu

Section 2

AIUAVS-DEVSECOPS METHODOLOGY AS SUPPORT UAV-BASED MINE CLEARANCE INFRASTRUCTURE

Bohdan Kosarevskyi
National Aerospace University «Kharkiv Aviation Institute»
Scientific adviser: Artem Tetskyi

Relevance. Ongoing warfare has left many regions contaminated with mines and unexploded ordnance, which hampers safe movement, infrastructure restoration, and the return to normal life. Unmanned aerial vehicles equipped with advanced sensors and tools have become essential in modern demining technology. These drones can detect mines and explosive devices from a safe distance, significantly reducing the risk to human operators. The integration of artificial intelligence further allows for real-time data analysis, facilitating informed decision-making and reducing operational costs.

Purpose. This study aims to review existing information technology methods and adaptations used in deploying unmanned intelligent systems for land demining, with a particular focus on information security. It covers security assessment methods, relevant metrics for demining support systems, and explains the AIUAVS-DevSecOps methodology, which integrates AI and DevSecOps principles.

Principal provisions. Several existing methodologies and frameworks are analyzed. The CVAIM method [1], an iterative process designed for business projects, can be adapted to deploy safe infrastructure for unmanned demining systems. The System Infrastructure Development Life Cycle adapts the SDLC specifically for infrastructure solutions, providing a seven-stage process - from requirements gathering to decommissioning - that integrates infrastructure-specific needs and security considerations at every step. The idea of dynamically distributing computations between local and remote resources to reduce processing time and maintain the compactness and energy efficiency of local resources by using larger computing capacities remotely [2]. Edge computing optimizes decision-making for offloading tasks, reducing latency and energy use, although data security remains a critical concern [3]. Optimal cloud infrastructure design focuses on security and scalability, addressing specific demining challenges. UAV swarms within networked control systems enhance productivity and efficiency but face resource and security constraints.

Securing UAV-based demining systems involves ensuring system reliability (measured by the Comprehensive Reliability Indicator), data integrity through encryption and authentication, robust cybersecurity measures like multi-factor authentication and intrusion detection, operational security via access control and risk management, and functional safety through testing and compliance with safety standards. The AIUAVS-DevSecOps methodology integrates AI and DevSecOps to rapidly develop and deploy secure infrastructure in critical systems, emphasizing continuous security monitoring, real-time management with anomaly detection, automated processes, and secure infrastructure management.

Conclusions. Modern IT methods are indispensable for creating and maintaining secure infrastructure for UAV-based demining systems. AI and AIUAVS-DevSecOps enhance system security, efficiency, and reliability. AI significantly improves the accuracy and speed of detecting explosives. As technology advances, unmanned systems are becoming more effective and safer, reducing the risk to human operators.

List of references

1. Banz A. Requirements Engineering Method for Infrastructure Automation and Cloud Projects. 2019 IEEE 27th International Requirements Engineering Conference (RE). 2019. Page 276-285. DOI: https://doi.org/10.1109/RE.2019.00037.
2. Callegaro D., Baidya S., Levorato M. Dynamic Distributed Computing for Infrastructure-Assisted Autonomous UAVs. ICC 2020 - 2020 IEEE International Conference on Communications (ICC). 2020. Page 1-6. DOI: https://doi.org/10.1109/ICC40277.2020.9148986.
3. Callegaro D., Levorato M. Optimal Edge Computing for Infrastructure-Assisted UAV Systems. IEEE Transactions on Vehicular Technology. Volume 70(2). 2021. Page 1782-1792. DOI: https://doi.org/10.1109/TVT.2021.3051378.

Information about the authors

Bohdan Kosarevskyi, a PhD student from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», b.v.kosarevskyi@student.csn.khai.edu

Artem Tetskyi, PhD, Associate Professor from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», a.tetskiy@csn.khai.edu

Секція 2

ФУНКЦІЙНА БЕЗПЕКА: АНАЛІЗ МЕТОДІВ ТА ІНСТРУМЕНТІВ ЗАБЕЗПЕЧЕННЯ

Костенко М. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Харченко В. С.

Актуальність. Функційна безпека є ключовою вимогою у розробці та експлуатації критичних систем, таких як транспорт, медицина, енергетика, авіація та промисловість. Порушення функційної безпеки в цих сферах може призвести до важких наслідків: людських жертв, екологічних катастроф та масштабних економічних втрат. У сучасних умовах технологічного прогресу та автоматизації зростає складність систем, що підвищує ризик помилок у програмному забезпеченні, збоїв у роботі компонентів або порушень у інтеграції різних модулів. Водночас, відповідність міжнародним стандартам, таким як IEC 61508 чи ISO 26262, стає обов'язковою умовою для розробників систем [1, 2]. Статистика свідчить, що 70% інцидентів у критичних системах спричинені людськими помилками або недоліками у процесах тестування. Тому функційна безпека вимагає комплексного підходу: від аналізу ризиків і проектування до експлуатації та обслуговування систем.

Метою даної роботи є дослідження існуючих стандартів функційної безпеки та їх адаптацію до сучасних викликів, аналіз інструментів оцінки та забезпечення функційної безпеки, включаючи автоматизовані засоби діагностики, виявлення основних викликів впровадження функційної безпеки та запропонувати шляхи їх подолання.

Основні положення. Стандарти IEC 61508 та ISO 26262 регламентують вимоги до розробки, тестування та верифікації систем із високим рівнем безпеки. Вони визначають поняття рівнів функційної безпеки (SIL), що є мірою надійності системи. Наприклад, SIL 3 використовується в системах, де навіть одна відмова може призвести до катастрофічних наслідків, як у випадках автоматизованого управління в авіації [3]. Сучасні підходи до аналізу ризиків базуються на наступних методах: FTA (Fault Tree Analysis): дозволяє моделювати сценарії збоїв через графічне представлення причинно-наслідкових зв'язків, FMEA (Failure Mode and Effects Analysis): оцінює вплив можливих відмов компонентів системи на загальну функціональність та HAZOP (Hazard and Operability Study): використовується для ідентифікації ризиків в складних процесах, таких як

хімічне виробництво. У сучасних системах широко застосовуються інструменти автоматичного моніторингу та діагностики, зокрема засоби аналізу даних у реальному часі. Це дозволяє ідентифікувати потенційні збої ще до їх виникнення [4]. Використання систем машинного навчання для аналізу телеметрії та даних із сенсорів допомагає передбачати можливі відмови. Серед основних викликів впровадження виділяють: висока вартість: Інтеграція засобів забезпечення безпеки потребує значних фінансових ресурсів. Складність тестування: У випадку розподілених або багатомодульних систем верифікація стає вкрай трудомісткою та Брак фахівців: Недостатня кількість інженерів, кваліфікованих у сфері функційної безпеки, сповільнює адаптацію сучасних технологій.

Висновки. Функційна безпека є визначальним фактором у створенні критичних систем, що потребує дотримання міжнародних стандартів, впровадження сучасних засобів аналізу ризиків та підвищення рівня компетентності персоналу. Основними напрямами вдосконалення функційної безпеки є автоматизація процесів, використання штучного інтелекту та розвиток комплексних методик тестування.

Список літератури

1. IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems URL – https://webstore.iec.ch/en/publication/5515 (дата звернення 12.11.24).
2. ISO 26262: Road Vehicles – Functional Safety URL – https://www.iso.org/standard/68384.html (дата звернення 12.11.24).
3. Савчук В. О., Цуранов М. В. Аналіз засобів безпеки критичних систем У збірнику конференції: Проблеми інформатизації. Тези доступні у бібліотеках або в електронних архівах університетів. 2020.
4. Eklund U., Törner F. A Comprehensive Study of FMEA and FTA as Risk Assessment Techniques for Critical Systems URL – https://www.researchgate.net/publication/320579551_A_comparative_critical_study_between_FMEA_and_FTA_risk_analysis_methods (дата звернення 12.11.24).

Відомості про авторів

Костенко Максим Вікторович, бакалаврат кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.v.kostenko@student.csn.khai.edu

Харченко Вячеслав Сергійович, завідувач кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н, професор, v.kharchenko@csn.khai.edu

Секція 2

АНАЛІЗ ТЕХНОЛОГІЙ ДЛЯ ПОБУДОВИ СИСТЕМИ ВЗАЄМОДІЇ ПРИСТРОЇВ РОЗУМНОГО БУДИНКУ

Кравченко О. А.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Перепелицин А. Є.

Актуальність. IoT впливає на наш світ, змінюючи спосіб, яким ми взаємодіємо з технологіями та навколишнім середовищем. Створення систем взаємодії пристроїв розумного будинку є актуальним завдяки їх інтеграції в повсякденне життя. Це відкриває широкі можливості для автоматизації побутових процесів, спрощення керування пристроями та отримання інформації від них [1]. Користувачі також прагнуть підвищити безпеку та енергоефективність взаємодії різних побутових пристроїв [2].

Метою цієї роботи є дослідження сучасних технологій взаємодій пристроїв розумного будинку. Для досягнення цієї мети необхідно вирішити наступні задачі: провести аналіз технологій для побудови системи взаємодії пристроїв розумного будинку, спроектувати та побудувати приклад системи розумного будинку у вигляді світильника.

Основні положення. Для аналізу була обрана взаємодія за допомогою Wi-Fi. Також існують взаємодії за допомогою Bluetooth, Ethernet. Wi-Fi має кілько переваг серед варіантів взаємодії, які були розглянуті. Ця взаємодія дозволяє досягти високу швидкість між пристроями, які є частиною розумного будинку. Великою перевагою є широкий радіус дії, який ще може збільшуватись за допомогою підсилювачів. Універсальність системи надає можливість її використання без спеціальних адаптерів. Недоліками цієї системи взаємодії є високе енергоспоживання, яке відчутно впливає на пристрої, які живляться від батарейки. Також має сенс використовувати роутер, тому що домашні роутери мають достатню кількість підключень. Але велика кількість пристроїв, які постійно передають дані, можуть створювати значне навантаження на мережу, що може призвести до зниження швидкості та якості. Bluetooth порівняно з Wi-Fi має низьке енергоспоживання, що робить його кращим для пристроїв з автономним живленням. Висока сумісність спрощує керування через мобільні додатки. Також перевагою є відсутність залежності від Інтернету, що особливо робить його надійним підключенням у випадках, коли мережа недоступна. Bluetooth має коротший діапазон зв’язку, що ускладнює його використання в великих будівлях. Також для стабільного з’єднання важливо, щоб між

пристроями не було перешкод, які будуть заважати якісній передачі інформації. Ще одним варіантом взаємодії є дротове з'єднання, перевагою якого є висока швидкість передачі даних, що робить цю систему ідеальної для пристроїв, які потребують швидкісної передачі інформації. Порівняно з бездротовими мережами, він менш схильний до перешкод і перебоїв в роботі. Також частина пристроїв має підтримку технології живлення за тім самим дротом Power over Ethernet (PoE), що забезпечує їм живлення. Але для нього є потреба в прокладанні кабелів, це може бути складним та дорогим процесом [3]. А також немає мобільності пристроїв. В рамках проведеного аналізу для побудови прототипу була обрана плата ESP8266, яка має вбудований Wi-Fi модуль. Що є ідеальним варіантом, для обраної системи взаємодії пристроїв розумного будинку.

Висновки. У ході аналізу був розглянута можливість зв'язку з Wi-Fi, за допомогою якого виконується взаємодія пристроїв розумного будинку, за рахунок своєї універсальності для багатьох проектах. А також була обрана плата ESP8266 для розробки, яка є однією із найпопулярніших і бюджетних Wi-Fi модулів. Система виконує кілька завдань, які допомагають зробити освітлення більш зручнішим, ефективним та розумним, що впливає на зручність та комфорт для користувача.

Список літератури

1. Вдовіченко, О. О. Організація взаємодії пристроїв з доступом в інтернет на основі мікроконтролерів із обмеженою кількістю ресурсів [Текст] / О. О. Вдовіченко, А. Є. Перепелицин // Авіаційно-космічна техніка і технологія. 2023. № 6. С. 76–85. DOI: 10.32620/aktt.2023.6.09.

2. Perepelitsyn, A. Service for communication of devices with internet access: analysis of technologies and method of creation [Text] / A. Perepelitsyn, O. Vdovichenko, & V. Mikhalevskyi // Radioelectronic and Computer Systems. 2023. No. 4. Page 197–208. DOI: 10.32620/reks.2023.4.14.

3. Vdovichenko, O. Technologies for building systems of remote lining of communication lines: a practical example of implementation [Text] / O. Vdovichenko, A. Perepelitsyn // Radioelectronic and Computer Systems. – 2021. No. 2. Page 31–38. DOI: 10.32620/reks.2021.2.03.

Відомості про авторів

Кравченко Олексій Андрійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.kravchenko@student.csn.khai.edu

Перепелицин Артем Євгенович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.perepelitsyn@csn.khai.edu

Section 2

COMPARISON OF ARCHIVE FORMATS APPLICABILITY FOR PRACTICAL USE

Andrii Litvinov
National Aerospace University «Kharkiv Aviation Institute»
Scientific adviser: Artem Perepelitsyn

Relevance. In the era of large-scale data management, archiving formats have become essential tools for reducing storage costs, optimizing file transfer efficiency, and enhancing data organization. As digital data continues to grow, selecting an optimal archive format has practical implications for both individuals and organizations [1]. Choosing the appropriate format can save storage space, reduce transfer times, and improve overall data handling efficiency, particularly in scenarios where bandwidth and storage resources are limited. This study addresses these needs by analyzing commonly used archive formats to determine their effectiveness in practical, everyday applications.

The purpose of this study is to conduct a comparative analysis of popular archive formats, specifically ZIP, RAR, 7z, and TAR.GZ, to assess their practical utility in terms of compression efficiency, data handling features, and suitability for a range of use cases. By evaluating factors such as compression ratio, processing speed, and recovery options, this study aims to guide users in selecting the best format for their specific archiving requirements.

Research results. The analysis of ZIP format compatibility shows support by various systems and acceptable compression efficiency. While standard ZIP has a 4GB file size limit, the ZIP64 extension allows larger archives. Despite its user-friendly design, ZIP lacks advanced recovery features, which limits its reliability for sensitive data applications [2]. RAR format shows a high compression ratio and multi-volume support, making it suitable for large datasets [3]. It also includes data recovery features for added resilience against corruption. However, the RAR format has only extraction source code available for the use that can be a disadvantage in open-source environments [4]. The 7Z format, supported by the open-source 7-Zip software, achieves strong compression through the LZMA algorithm. It is ideal for archiving large files due to its high efficiency and open-source flexibility. However, 7Z offers limited recovery options and may lack native support on some systems, which can be a drawback in standardized environments. Lastly, TAR, often paired with GZIP to form TAR.GZ, is common in UNIX and Linux systems. While TAR does not compress files on its own, TAR.GZ provides effective compression while

preserving file attributes. However, TAR.GZ lacks native encryption and data recovery features, limiting its suitability for applications requiring high data protection.

Conclusions. The performed investigation allowed us to identify the strengths and limitations of popular archive formats. ZIP and TAR.GZ are ideal for general use and compatibility, while 7z and RAR provide higher compression, suited for storage-limited environments. For open-source and high-efficiency needs, 7z is recommended, while RAR is preferable for situations requiring data integrity protection and data recovery. Selecting the right format depends on balancing compression, features, and compatibility with specific use cases.

List of references

1. Prabavathy B., Ramya P., Babu C. Optimized private cloud storage for heterogeneous files in an university scenario. 2013. 3rd International Conference on Recent Trends in Information Technology (ICRTIT), Page. 323–328. DOI: https://doi.org/10.1109/icrtit.2013.6844224.
2. Wei Y., Zheng N., Xu M. An Automatic Carving Method for RAR File Based on Content and Structure. 2010. 2nd International Conference on Information Technology and Computer Science (ITCS 2010), p. 68–72. URL: https://doi.org/10.1109/itcs.2010.23.
3. Radescu R., Barar A. P. The Performances of the Fixed Constraints Transform Applied in Text Compression Experimental Results and Comparisons. 2018. 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Page 1–6. DOI: https://doi.org/10.1109/ecai.2018.8678935.
4. Guo Y., Li G., Zhang G. Design of the Scientific and Technological Information Management Software. 2023. 5th International Conference on Electronic Engineering and Informatics (EEI), Page 235–239. URL: https://doi.org/10.1109/eei59236.2023.10212809.

Information about the authors

Andrii Litvinov, student at the Computer Systems, Networks and Cybersecurity Department, National Aerospace University «Kharkiv Aviation Institute», a.a.litvinov@student.csn.khai.edu
Artem Perepelitsyn, Associate professor at the Computer Systems, Networks and Cybersecurity Department, National Aerospace University «Kharkiv Aviation Institute», PhD, a.perepelitsyn@csn.khai.edu

Секція 2

ДОСЛІДЖЕННЯ ТА РОЗРОБКА СИСТЕМИ КЕРУВАННЯ ТРАНСПОРТНИМ ТРАФІКОМ МІСТА

Мосін А. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Желтухін О. В.

Актуальність. Проблема транспортних заторів досі залишається однією з суттєвих проблем багатьох великих міст на різних континентах [1]. При цьому зростання кількості транспорту на дорогах великих міст, як правило, випереджає можливості дорожньої інфраструктури, що призводить до транспортних заторів. Це свідчить про те, що оптимізація трафіку є актуальною науковою та практичною задачею, яка має значний вплив на соціально- економічний розвиток міст. Мова не про будівництво нових доріг і розв'язок, а про розумне керування транспортними потоками з використанням інтелектуальних систем і технологій керування дорожнім рухом.

Мета та задачі дослідження. Мета роботи полягає в розробці інтелектуальної системи керування трафіком великого міста, здатної зменшити кількість транспортних заторів за рахунок розумного керування світлофорами, в основу роботи якої покладено модель штучного інтелекту, навчену на симуляційних експериментах за сценарієм руху з урахуванням точок інтересу [3]. Для досягнення цієї мети можуть бути використані сенсорні технології, надаючи змогу покращити керування дорожнім рухом. Є можливість використати модель онтолого-керованої системи, призначеної для розумного розподілу транспортних потоків на перехрестях великого міста [2]. При цьому бази правил для кожного типу перехресть формуються з правил дорожнього руху, а управління тривалістю сигналів світлофорів базується на аналізі даних, що надходять з різних джерел в режимі реального часу. Задачі дослідження полягають у вивченні проблем дорожнього руху в сучасних великих містах та систем управління трафіком.

Дослідження передбачає розробку архітектури високонавантаженої інтелектуальної системи, здатної управляти транспортними потоками великого міста в режимі реального часу, а також обґрунтування вибору моделі штучного інтелекту для вирішення задачі керування комплексом світлофорів.

Основні положення. Композиції та структурне моделювання використовуються в концептуальному моделюванні системи. Нечітка логіка застосовується для формалізації понятійного апарату в домені «Дорожній рух» в онтології системи та для правил управління комплексом світлофорів на складних перехрестях. Теорія автоматів допомагає розширити базу правил управління комплексом світлофорів, враховуючи передумови їх застосування. Теорії ймовірностей та математичної статистики використовуються для моделювання транспортних потоків з урахуванням ключових точок інтересу. Імітаційне моделювання служить для тренування моделі управління комплексом світлофорів в умовах, наближених до реальних, а навчання з підкріпленням дозволяє оптимізувати цю модель.

Висновки. Розробка інтелектуальної системи керування трафіком великого міста, здатної зменшити кількість транспортних заторів за рахунок розумного керування світлофорами є важливою задачею для країни. Це вирішить багато проблем як для країни так і підвищить індекс щастя для учасників транспортного руху.

Список літератури

1. Kyiv is already third in the world for traffic jams. Further it will be even worse. Epravda. URL – https://www.epravda.com.ua/publications/2022/02/10/682256 (дата звернення: 12.11.2024).

2. Mazurenko R. & Yeremenko B. (2023). Intelligent Road Transport Flow Management System: Basic Ontology Concepts. Management of Development of Complex Systems. Volume 55. Page 192–197. DOI: dx.doi.org\10.32347/2412-9933.2023.55.192-197.

3. Neelakandan S., Berlin M. A., Tripathi S., Devi V. B., Bhardwaj I., Arulkumar N. IoT-based traffic prediction and traffic signal control system for smart city. *Soft Computing*. 2021. Volume 25(18). Page 12241–12248. DOI: https://doi.org/10.1007/s00500-021-05896-x.

Відомості про авторів

Мосін Андрій Валерійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.mosin@student.csn.khai.edu

Желтухін Олександр Васильович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ» a.zheltukhin@csn.khai.edu

Секція 2

ВИКОРИСТАННЯ ЛОКАЛЬНИХ МОВНИХ МОДЕЛЕЙ

Попов Р. О.
Дніпровський національний університет ім. Олеся Гончара
Науковий керівник: Карпенко Н. В.

Актуальність. Вплив великих мовних моделей (англ. Large Language Model, LLM) очевидний: для користувачів – це інструмент для навчання та аналізу, а дослідники постійно розробляють нові архітектури, що демонструють кращі результати. LLM також стали важливими для бізнесу, оскільки багато додатків використовують API від OpenAI, Anthropic, Mistral та інших компаній. Це зручно і ефективно, оскільки для запуску моделей потрібні великі ресурси. Однак, використання віддалених моделей через API має недоліки, такі як проблеми з конфіденційністю, обмежена налаштовуваність та інші. Виникає питання: чи можна запускати LLM локально і які переваги це дасть порівняно з віддаленими моделями? Як це вплине на ефективність AI-додатків?

Мета. Розглянути інструменти для локального запуску мовних моделей та проаналізувати їхні можливості порівняно з віддаленими моделями IT-компаній.

Осовні положення. Для запуску великих мовних моделей необхідне коштовне обладнання та великі витрати електроенергії. Натомість, зараз активно набирає популярність тема малих мовних моделей (англ. Small Language Models, SLM), які потребують менше пам’яті та мають велику швидкість генерації виводу [1]. На обсяг ресурсів для запуску SLM впливає три основні фактори: кількість параметрів, квантизація та архітектура. Кількість параметрів зазвичай вимірюється в мільярдах, і компанії випускають моделі з різною кількістю параметрів, як-от Google Gemma 2 з 2 млрд., 9 млрд. та 27 млрд. параметрів. За допомогою квантизації можна зменшити розмір моделі та пришвидчити виконання арифметичних операцій, що досягається спрощеним представленням чисел (8, 4 або навіть 2 біти) [2]. Згідно з результатами тестувань SLM на різних збірках даних, саме архітектура та дата випуску моделі найбільше впливають на якість генерації. Різні архітектури адаптовані для різних задач, а моделі поточного року мають якість в декілька разів кращу за моделі попереднього року [1]. Внутрішній експеримент Microsoft показав, що SLM мають досить високу ефективність та в десятки разів меншу вартість обслуговування, аніж LLM [3]. Популярними SLM зараз є такі моделі: Microsoft Phi3.5, Alibaba

Qwen2.5, Google Gemma 2, Meta Llama 3.2, та інші. Зазвичай більшість SLM та LLM зберігаються на сервісі Hugging Face, а стандартом де-факто для локального запуску моделей є программа llama.cpp. Інтеграція локальних моделей в існуючий AI-додаток може бути абсолютно безшовною, оскільки llama.cpp (та інші програми) можуть надавати свої послуги через HTTP API, сумісний з API OpenAI.

Висновки. Розглянуто питання локального запуску мовних моделей. Перевагою мовних моделей, які можна запустити локально, є повне збереження конфіденційності даних, на відміну від використання через API віддалених мовних моделей. Існує досить багато SLM для вирішення різних задач, які знаходяться у вільному доступі, їх можна завантажити з Hugging Face та запускати локально через llama.cpp. Проведений аналіз показує, що для задач обробки інформації SLM мають ефективність порівняну з LLM, і до того ж потребують набагато менше обчислювальних ресурсів.

Список літератури

1. Lu Z., Li X., Cai D. Small Language Models: Survey, Measurements, and Insights. 2024. DOI: https://doi.org/10.48550/arXiv.2409.15790.
2. Li S., Ning X., Wang L. et al. Evaluating Quantized Large Language Models. 2024. DOI: https://doi.org/10.48550/ARXIV.2402.18158.
3. Li B., Zhang Y., Bubeck S. Small Language Models for Application Interactions: A Case Study. 2024. DOI: https://doi.org/10.48550/ARXIV.2405.20347.

Відомості про авторів

Попов Руслан Олександрович, студент кафедри електронних обчислювальних машин, ДНУ ім. Олеся Гончара, popov_r@365.dnu.edu.ua
Карпенко Надія Валеріївна, доцент кафедри електронних обчислювальних машин, ДНУ ім. Олеся Гончара, к.ф.-м.н., доцент, karpenko_n@365.dnu.edu.ua

Секція 2

АНАЛІЗ МОЖЛИВОСТІ ДОМАШНЬОЇ АВТОМАТИЗАЦІЇ З ВИКОРИСТАННЯМ ЗРУЧНОЇ ВЗАЄМОДІЇ З ПРИСТРОЄМ

Самарченко В. С.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Перепелицин А. Є.

Актуальність. У сучасному світі важко переоцінити актуальність домашньої автоматизації [1]. Завдяки розвитку Інтернету речей ці технології все більше інтегруються в повсякденне життя [2], підвищуючи комфорт та безпеку житлових приміщень [3].

Метою роботи є аналіз можливості домашньої автоматизації з використанням зручних варіантів взаємодії користувача з пристроєм та технології Інтернету Речей. Для досягнення цієї мети необхідно вирішити задачу аналізу можливих способів локальної взаємодії з побутовими системами, а також запропонувати практичну реалізацію результатів дослідження.

Основні положення. Розглянуті існуючі варіанти реалізації взаємодії з пристроями. Arduino – один із найпопулярніших платформ швидкого проектування. ESP32 – являє собою серію недорогих мікроконтролерів з низьким енергоспоживанням, вбудованим Wi-Fi та дворежимним Bluetooth. Пульт дистанційного керування працює через інфрачервоний сигнал або радіочастотний канал, інфрачервоні приймачі (ІЧ) сумісні з Arduino або ESP32 можна інтегрувати для прийому команд від ІЧ-пультів.

Додатки на смартфоні можуть керувати пристроями через Wi-Fi або Bluetooth. Вони дозволяють контролювати систему з будь-якої точки будинку або навіть поза його межами та надають зворотній зв’язок корисувачу. Arduino, Raspberry Pi або ESP32 мають модулі, сумісні з Wi-Fi/Bluetooth. Голосові асистенти, такі як Amazon Alexa або Google Assistant є зручним способом взаємодії з пристроями. Arduino, ESP32 або Raspberry Pi можуть бути інтегровані з Google Assistant або Alexa SDK для керування пристроями через Wi-Fi. Також можливе управління за допомогою жестів, завдяки сенсорам руху або камерам із обробкою зображень. Наприклад, датчик жестів та кольору APDS-9960 для Arduino.

LED-індикатори та дисплеї використовуються для візуального зворотного зв’язку. Наприклад, світлодіоди можуть показувати стан системи а LCD-екрани – поточні деталізовані дані. Звукові модулі забезпечують зворотний зв’язок у формі звукових сигналів.

Через те, що пристрої обмінюються інформацією безпосередньо з контролерами, це забезпечує автономність від зовнішнього Інтернет з'єднання. Наприклад, мобільний телефон може напряму підключатися до контролера і взаємодіяти з пристроями в системі. Системи можна забезпечити резервним живленням у вигляді акумуляторів або блоків безперебійного живлення. Більшість плат Arduino та ESP32 також можуть працювати від акумуляторів.

Висновки. У ході аналізу були розглянуті можливості швидкого прототипування, що мають велику кількість доступних плат і модулів з підтримкою Wi-Fi, Bluetooth, ІЧ-передавачів, реле, датчиків руху. Були розглянуті можливості зворотнього зв'язку з користувачем, а саме: LED-індикатори, звукові модулі та дисплеї. Таким чином, рішення в рамках IoT дозволяють контролювати і керувати побутовими пристроями віддалено, автоматизувати рутинні процеси, а також оптимізувати енергоспоживання.

Список літератури

1. Perepelitsyn, A. Service for communication of devices with internet access: analysis of technologies and method of creation [Text] / A. Perepelitsyn, O. Vdovichenko, & V. Mikhalevskyi // Radioelectronic and Computer Systems. – 2023. No. 4. Page 197–208. DOI: 10.32620/reks.2023.4.14.

2. Вдовіченко, О. О. Організація взаємодії пристроїв з доступом в інтернет на основі мікроконтролерів із обмеженою кількістю ресурсів [Текст] / О. О. Вдовіченко, А. Є. Перепелицин // Авіаційно-космічна техніка і технологія. 2023. № 6. С. 76–85. DOI: 10.32620/aktt.2023.6.09.

3. The power of IoT home automation | IoT Now News & Reports. *IoT Now News - How to run an IoT enabled business*. URL: https://www.iot-now.com/2024/07/30/145721-the-power-of-iot-home-automation (дата звернення: 24.10.2024).

Відомості про авторів

Самарченко Владислав Сергійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», v.samarchenko@student.csn.khai.edu

Перепелицин Артем Євгенович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.perepelitsyn@csn.khai.edu

Секція 2

ДОСЛІДЖЕННЯ ТА РОЗРОБЛЕННЯ СИСТЕМИ ПЛАНУВАННЯ ТА БРОНЮВАННЯ ВІДПУСТОК НА ОСНОВІ ЗБОРУ ТА АНАЛІЗУ ВЕЛИКИХ ДАНИХ

Сафронова Г. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Желтухін О. В.

Актуальність. В умовах сучасної цифрової ери управління людськими ресурсами стає все більш залежним від технологічних інновацій, що дозволяють ефективніше планувати і координувати робочий процес. Одним з таких інструментів є системи планування та бронювання відпусток, які дозволяють оптимізувати графіки відпусток, зменшити навантаження на HR-відділи і забезпечити зручність для працівників [1]. Використання великих даних дозволяє не тільки автоматизувати процес, але й аналізувати тренди, передбачати потреби в персоналі та виявляти потенційні проблеми в управлінні кадрами [2].

Метою даної роботи є дослідження та розроблення системи планування і бронювання відпусток на основі збору та аналізу великих]даних. Вона дозволить підприємствам більш ефективно управляти робочим часом та ресурсами, мінімізуючи вплив людського фактора і забезпечуючи зручність для всіх користувачів системи.

Основні положення. Для досягнення цієї мети в роботі було використано декілька методів. Збір та обробка даних: використано великі обсяги даних про попередні відпустки, включаючи їх тривалість, частоту, сезонність і інші параметри. Аналіз таких даних дозволяє визначати тренди і оптимізувати процес планування відпусток на майбутнє [3]. Аналіз потреб: за допомогою алгоритмів машинного навчання було розроблено модель для прогнозування кількості відпусток у певні періоди, що дозволяє компанії краще підготуватися до відсутності працівників і уникнути надмірного навантаження на колектив [2]. Інтеграція з існуючими системами: розроблена система інтегрується з HR-системами компаній, дозволяючи автоматично оновлювати графіки роботи, відстежувати доступні дні відпусток та їх залишки [1].

Висновки. Система планування і бронювання відпусток на основі збору та аналізу великих даних є інноваційним рішенням, яке дозволяє значно підвищити ефективність управління персоналом. Завдяки використанню технологій великих даних, підприємства можуть оптимізувати процеси,

мінімізувати втрати через людський фактор та забезпечити комфортні умови для працівників при плануванні відпусток.

Список літератури

1. Коваленко І. О. Автоматизовані системи управління персоналом в умовах цифрової трансформації // Наукові праці Національного університету харчових технологій. 2022. С. 100-110.
2. Brown A., Smith J. Data-Driven HR: How Big Data Can Support HR Analytics // HR Journal. 2021. Page 45-60.
3. Machine Learning for Human Resource Management: A Comprehensive Review of Algorithms and Applications // Journal of Data Science. 2023. Page 15-30.

Відомості про авторів

Сафронова Ганна Василівна, магістрантка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», safronova.hanna.v@gmail.com
Желтухин Олександр Васильович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.zheltukhin@csn.khai.edu

Секція 2

ФУНКЦІОНАЛЬНА БЕЗПЕКА ТА НАДІЙНІСТЬ IOT-СИСТЕМ

Тимченко О. А.
Сумський Державний Університет
Науковий керівник: Колесніков В. А.

Актуальність. Системи Інтернету речей (IoT) швидко інтегруються в критичні сфери, як-от промисловість, медицина, енергетика та інфраструктура «розумного міста». Це викликає необхідність забезпечення їхньої функціональної безпеки та стійкості до збоїв, що можуть призвести до значних ризиків для користувачів та об'єктів інфраструктури. Актуальні дослідження сфокусовані на захисті IoT-пристроїв від фізичних маніпуляцій та збоїв у мережах з обмеженими ресурсами.

Мета роботи. Вивчення методів забезпечення функціональної безпеки IoT-систем для підвищення стійкості до збоїв, надійної роботи в умовах потенційних загроз та захисту від несанкціонованого фізичного доступу.

Основні положення. Забезпечення безперервності роботи IoT-систем. Використання децентралізованих та периферійних обчислень, таких як туманні обчислення, є важливим для стабільної роботи IoT-систем у випадку відсутності зв’язку з основним сервером. Це дозволяє знижувати навантаження на центральні вузли та забезпечує швидку обробку даних без затримок [2]. Стійкість до збоїв і відмов пристроїв. Сучасні методи резервного копіювання і дублювання критичних функцій сприяють відновленню роботи після збоїв. Наприклад, методи самовідновлення з автоматичною переадресацією на резервні вузли підвищують надійність системи в реальному часі [3]. Захист від фізичних маніпуляцій. Дослідження показують ефективність інтеграції легковагих методів шифрування і спеціальних сенсорів для виявлення несанкціонованого доступу до IoT-пристроїв. Такі методи спрямовані на запобігання фізичному втручанню та захист даних навіть в умовах обмежених ресурсів [1]. Адаптація до вимог критичної інфраструктури. Використання сучасних міжнародних стандартів, таких як IEC 62443, та адаптація їх до умов української інфраструктури сприятиме підвищенню рівня безпеки і надійності IoT-систем у промислових мережах [1]. Впровадження міжнародних стандартів, зокрема IEC 62443, дозволяє забезпечити відповідність IoT-систем вимогам безпеки, що є особливо важливим для критичних галузей, таких як енергетика, медицина та промисловість. Адаптація цих стандартів до специфіки української інфраструктури є

важливим кроком для покращення функціональної безпеки і захисту IoT в умовах підвищених ризиків.

Висновки. Функціональна безпека IoT-систем є комплексною задачею, яка потребує інтеграції різноманітних технологічних, архітектурних та організаційних рішень для забезпечення стійкості до збоїв і стабільної роботи навіть у несприятливих умовах. Децентралізація обробки даних за допомогою туманних обчислень знижує навантаження на центральні сервери та підвищує швидкість обробки критично важливої інформації в режимі реального часу. Це значно збільшує стійкість систем до часткових відмов або втрати зв'язку, що особливо важливо для IoT у критичних інфраструктурах. Використання методів резервного копіювання і дублювання забезпечує високий рівень відновлення після збоїв та мінімізує втрати інформації, що дозволяє зберігати стабільність системи під час виникнення несподіваних відмов. Таким чином, функціональна безпека IoT-систем повинна базуватися на багаторівневому підході, який включає використання децентралізованих архітектур, алгоритмів самовідновлення, сенсорів безпеки, відповідних криптографічних протоколів, а також дотримання міжнародних стандартів. Цей комплекс заходів забезпечує стійкість IoT-систем до загроз та підвищує надійність їх роботи, що є надзвичайно важливим для захисту критичної інфраструктури й інших галузей, де стабільність та безперервність роботи мають ключове значення.

Список літератури

1. Васильченко, А. Інформаційна та функціональна безпека IoT-систем в критичній інфраструктурі. Науковий журнал Національного університету зв'язку. 2023. Том 4 № 3. С. 45-53.
2. Соколов В. М., Поліщук О. В. (2022). Периферійні обчислення для підвищення функціональної безпеки IoT в умовах критичної інфраструктури України. Вісник Одеського національного університету 2022. Том 2 № 34. С. 112-119.
3. Сичова І. С., Мазуренко Л. В. Проблеми кібербезпеки в Інтернеті речей та функціональна надійність IoT-систем. Кібербезпека: освіта, наука, техніка. 2022. Том 2 №10. С. 42-47.

Відомості про авторів

Тимченко Олександр Анатолійович, аспірант кафедри комп'ютерних наук, СумДУ, altymchenko@ukr.net
Колесніков Валерій Анатолійович, професор кафедри комп`ютерних наук, СумДУ, д.т.н., v.kolesnikov@cs.sumdu.edu.ua

Section 2

ANALYSIS OF FILE SYSTEMS AND TECHNOLOGICAL SOLUTIONS FOR LOCAL DATA STORAGE

Alona Chepelevych
National Aerospace University «Kharkiv Aviation Institute»
Scientific adviser: Artem Perepelitsyn

Relevance. During the construction of modern systems that use large arrays of data, there is a need to index this data between different drives and servers [1]. The process of transfer itself between them represents the work with small files or the chunks. Using this approach can increase the efficiency of the drive itself and the file system and also simplify the downloading process when working with such a cloud storage system [2].

In order to implement support for local storage with file partitioning into blocks, it is necessary to search for technical solutions that most file systems will support and to consider the target file systems themselves.

The purpose of this study is to analyse file systems and technological solutions for local data storage. To achieve this goal, it is necessary to solve the problem of analysing the most universal of the common file systems, analysing technological solutions for working with a large number of large files and proposing the practical implementation of the research results.

Principal provisions. In order to make access easier and faster, certain blocks can be placed on different physical drives. This can solve the problem of the size of such a file if its size is hundreds of gigabytes. At the same time, checksums of individual chunks within a file make it easier to identify and localise a value mismatch than for the entire file. Also, an individual chunk can be more easily double-checked, read, or written during transmission.

For most practical applications and non-critical areas of application tasks, this form of file storage can significantly reduce the time required to work with files. They can also be placed in most data storage systems as part of archives [1]. Information about the whole file is stored in the form of metadata. This makes the process of working with such files and indexing them discrete and speeds up access to them on storage devices. It also simplifies the task for the drive buffer itself when accessing a part of a file as part of a file system or files as part of archives.

In order to utilise more elements, it is necessary to search for file systems themselves [3].

A preliminary review of file systems shows that the following file systems are prioritised for maximum support by most existing operating systems: exFAT, FAT32 and UDF.

Conclusions. The analysis shows that using separate blocks simplifies the work with large files. The analysis of file systems for removable drives for file storage shows that the following priority set is advisable for maximum support among existing operating systems: exFAT, FAT32 and UDF.

List of references

1. Analysis of Archive Formats applicability for practical use: Comparison of Compression [Text] / A. Perepelitsyn, A. Litvinov, & A. Chepelevych // Proceedings 2024 14th International Conference on Dependable Systems, Services and Technologies, DESSERT 2024, – 2024. – 6 p., accepted.
2. Optimized private cloud storage for heterogeneous files in an university scenario [Text] / B. Prabavathy, P. Ramya, & C. Babu // Proceedings of 2013 IEEE International Conference on Recent Trends in Information Technology ICRTIT 2013, 2013, pp. 323-328, DOI: 10.1109/ICRTIT.2013.6844224.
3. Forensics filesystem with cluster-level identifiers for efficient data recovery [Text] / M. Alhussein, A. Srinivasan, & D. Wijesekera // 2012 International Conference for Internet Technology and Secured Transactions, 2012, pp. 411-415.

Information about the authors

Alona Chepelevych, student at the Computer Systems, Networks and Cybersecurity Department, National Aerospace University «Kharkiv Aviation Institute», a.i.chepelevych@student.csn.khai.edu
Artem Perepelitsyn, Associate professor at the Computer Systems, Networks and Cybersecurity Department, National Aerospace University «Kharkiv Aviation Institute», PhD, a.perepelitsyn@csn.khai.edu

Section 2

CYBERSECURITY OF COMMUNICATION CHANNELS OF UNDERWATER MONITORING DEVICES

Mykyta Shypunov
National Aerospace University «Kharkiv Aviation Institute»
Zemlianko Heorhii

Relevance. Relevance. Underwater monitoring devices are essential in oceanography, marine exploration, environmental monitoring, and defense. However, the communication channels transmitting this data are vulnerable to cyber threats. Underwater environments pose challenges like limited bandwidth, high latency, signal degradation, and energy constraints, hindering traditional cybersecurity methods [1]. Acoustic communication, the primary method for underwater transmission, is prone to interference and signal loss, making it exploitable [2]. Optical and RF systems, while better in bandwidth and latency, are limited by range and security vulnerabilities [2,3]. This underscores the need for tailored cybersecurity solutions for underwater networks.

The purpose of this work is to investigate the cybersecurity risks associated with the communication channels of underwater monitoring devices and propose effective mechanisms to mitigate these risks. The study focuses on evaluating the vulnerabilities of acoustic, optical, and RF communication technologies commonly used in underwater environments and explores hybrid communication systems as potential solutions. The objective is to identify specific attack vectors, including data interception, man-in-the-middle attacks, and signal manipulation, and to propose cybersecurity protocols that can be implemented without overloading the energy and computational capacities of underwater devices.

Principal provisions. Vulnerabilities of Acoustic Communication: Acoustic communication is particularly susceptible to signal interference, attenuation, and eavesdropping. The slow data rates inherent to this technology make the integration of sophisticated encryption protocols challenging, as they can significantly increase the energy consumption of devices [3]. These limitations increase the risk of unauthorized data interception, particularly in noisy or hostile marine environments [4]. Challenges in Optical and RF Communication: Optical systems, while offering high bandwidth, are limited by short ranges and physical signal interception [3]. RF systems, used in surface communication, face absorption issues and intermittent security risks [4]. Hybrid Systems: Combining acoustic, optical, and RF communication offers flexibility, but adds complexity in securing multiple channels [4]. Multi-layer encryption can help but requires further optimization [5]. Device Physical Security: Physical tampering of

underwater devices can lead to data breaches. Tamper-proof hardware and integrity checks are vital [5].

Conclusions. The cybersecurity of communication channels in underwater monitoring devices presents significant challenges due to the limitations imposed by the marine environment, including signal attenuation, noise interference, and energy constraints. Acoustic, optical, and RF communication technologies each have specific vulnerabilities that can be exploited by malicious actors. Hybrid communication systems offer flexibility but introduce additional security complexities. To enhance cybersecurity in underwater networks, it is necessary to develop lightweight encryption protocols, adaptive security frameworks, and tamper-proof hardware designs that balance the need for robust security with the operational constraints of these systems. Future research should focus on testing these solutions in real-world environments to validate their effectiveness.

List of references

1. Abdi A., Zhang E., Rashid R. Multichannel signal transmission and reception using compact multichannel underwater communication devices: a unified theory and experimental results from different underwater media. *The journal of the acoustical society of america*. 2024. Volume 155(3). P. A317. DOI: https://doi.org/10.1121/10.0027648.
2. Sea water channel for underwater communication / T. S. Priya et al. *E3S web of conferences*. 2023. Volume 399. P. 01015. DOI: https://doi.org/10.1051/e3sconf/202339901015.
3. Channel polarization scheme for ocean turbulence channels in underwater visible light communication / X. Li et al. *Journal of marine science and engineering*. 2023. Volume 11(2). Page 341. DOI: https://doi.org/10.3390/jmse11020341.
4. Communication for underwater robots: recent trends / A. Quattrini Li et al. *Current robotics reports*. 2023. DOI: https://doi.org/10.1007/s43154-023-00100-4.
5. Pavlov I. I., Myshkin V. F., Khan V. A. Organization of an underwater wireless communication system. *T-Comm*. 2024. Volume 18(1). Page 4–12. DOI: https://doi.org/10.36724/2072-8735-2024-18-1-4-12.

Information about the authors

Mykyta Shypunov, cybersecurity researcher, kin.shypunov@gmail.com
Heorhii Zemlianko, a Senior Lecture, PhD of cybersecurity from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», g.zemlynko@csn.khai.edu

Секція 2

АНАЛІЗ МОЖЛИВИХ ЗАСОБІВ ІНДИКАЦІЇ В СИСТЕМАХ ПОБУТОВОЇ АВТОМАТИЗАЦІЇ

Якушов Б. С.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник: Перепелицин А. Є.

Актуальність. Моніторинг інформації в реальному часі є одним із важливих елементів сучасних IoT-проєктів [1]. Для безпосередньої настройки можуть використовуватися системи індикації. Такі пристрої IoT потребують найкращих рішень для індикації, які будуть відповідати потребам, включаючи енергоефективність, інформативність та легкість індикації. Аналіз існуючих технологій дозволить обрати можливе рішення для індикації в IoT пристроях.

Метою роботи є дослідження сучасних засобів індикації, які використовуються в пристроях з мікроконтролерами. Для досягнення цієї мети необхідно провести порівняльний аналіз, за такими критеріями як, сумісність і інтеграція, енергоефективність, якість відображення та ціна, а також виконати розробку прототипу проекту для демонстрації роботи обраного варіанту індикації.

Основні положення. Для аналізу існуючих рішень було обрано самі розповсюджені дисплеї для індикації, а саме OLED, LCD та LED [2-3]. Порівняння дисплеїв проведено за такими критеріями як енергоефективність, якість, сумісність та інтеграція, а також ціна.

OLED дисплеї забезпечують чіткість відображення, контрастність, яскравість та насиченість, стабільне зображення під різними кутами, а також визначаються енергоефективністю. Такі модулі сумісні із розповсюдженими мікроконтролерами Arduino та ESP32 із підключеням по I2C і SPI. Для Arduino існують готові бібліотеки. Їх недоліком є ціна, яка значно вища інших варіантів індикації .

LED дисплеї мають доступну ціну, але не надають високу роздільну здатність та кут огляду, а також мають підвищений рівень енергоспоживання, завдяки тому що потребують підсвітку.

LCD коштують дешевше за OLED, а також не потребують багато енергії, проте якість зображення залежіть від конкретної моделі.

Було розроблено та створено прототип на основі Arduino Nano у вигляді невеликої ігрової консолі, яка має чотири кнопки для керування, дисплей та динамік. Підключення OLED дисплею до плати Arduino Nano

проводиться по інтерфейсу I2C. SCL під'єднується до піну A5 та SDA до піну A4. Кнопки та динамік підключаються до пінів D2-6 на платі. Код написаний у середовищі Arduino IDE з бібліотеками для керування OLED дисплеями Adafruit_GFX та Adafruit_SSD1306 з перевіркою роботи та завантаження на плату.

У результаті створено невелику ретро-консоль з відомою грою. Керування здійснюється за допомогою двох кнопок, які відповідають за рух вгору та вниз, також маємо кнопку паузи та оновлення рахунку. Виводиться все на невеликий OLED дисплей з роздільною здатністю 128*64 пікселів.

Висновки. У ході аналізу були розглянуті переваги і недоліки популярних дисплеїв, що допомогло при виборі системи індикації для розробки демонстраційного проекту на базі мікроконтролеру Arduino.

За результатом аналізу, можна сказати, що для розробки проєктів OLED дисплеї будуть самим оптимальним варіантом, завдяки якості зображення та невисоким енергоспоживанням.

Список літератури

1. Вдовіченко, О. О. Організація взаємодії пристроїв з доступом в інтернет на основі мікроконтролерів із обмеженою кількістю ресурсів [Текст] / О. О. Вдовіченко, А. Є. Перепелицин // Авіаційно-космічна техніка і технологія. 2023. № 6. С. 76–85. DOI: 10.32620/aktt.2023.6.09.

2. 6 Best IoT Display Technologies Comparison | Ynvisible. *Ynvisible: Cost-Effective E-paper Display Manufacturer*. URL: https://www.ynvisible.com/news-inspiration/iot-displays?datasheet-popup-close=1 (дата звернення: 11.11.2024).

3. Visualizing IoT: The Future of Device Displays. *IoT For All*. URL: https://www.iotforall.com/visualizing-iot-the-future-of-device-displays (дата звернення: 11.11.2024).

Відомості про авторів

Якушов Борис Сергійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», b.yakushov@student.csn.khai.edu

Перепелицин Артем Євгенович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.perepelitsyn@csn.khai.edu

АЛФАВІТНИЙ ВКАЗІВНИК

АЛФАВІТНИЙ ВКАЗІВНИК

АЛФАВІТНИЙ ВКАЗІВНИК

ЗМІСТ

СТУДЕНТСЬКА КОНФЕРЕНЦІЯ
ІНФОРМАЦІЙНА, ФУНКЦІЙНА і КІБЕРБЕЗПЕКА
СКІФіК

Відповідальний за випуск Г. А. Землянко

Видавець ФОП Бровін О.В.
Свідоцтво про внесення субєкта до Державного реєстру видавців та виготовників видавничої продукції серія ДК 3587 від 23.09.09 р.
Формат 60х84/16. Ум. друк. арк. 10.11. Тир. 100 прим. Зам. 807.

Надруковано з макету замовника ФОП Бровіна І.П.
61022, м. Харків, вул. Трінклера, 2, корп.1, к.19. Т. (066) 822-71-30

СТИЛЬ-ІЗДАТ®
друкарня
www.stil-izdat.com