НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
„ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"
Кафедра комп'ютерних систем, мереж і кібербезпеки

СТУДЕНТСЬКА КОНФЕРЕНЦІЯ ІНФОРМАЦІЙНА, ФУНКЦІЙНА І КІБЕРБЕЗПЕКА

СКІФіК

Матеріали п'ятої
науково-технічної конференції

27-28 листопада 2025 року

ХАРКІВ - 2025

НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. Н. КАРАЗІНА
УКРАЇНСЬКЕ НАУКОВО-ОСВІТНЄ ІТ-ТОВАРИСТВО
ІНСТИТУТ ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
БОЛГАРСЬКОЇ АКАДЕМІЇ НАУК (СОФІЯ, БОЛГАРІЯ)
МІЖНАРОДНИЙ ЦЕНТР З БЕЗПЕКИ ICCSS (ВАРШАВА, ПОЛЬЩА)

СТУДЕНТСЬКА КОНФЕРЕНЦІЯ «ІНФОРМАЦІЙНА, ФУНКЦІЙНА і КІБЕРБЕЗПЕКА»

СКІФіК

Матеріали п'ятої
науково-технічної конференції
27 – 28 листопада 2025 року

Харків 2025

УДК: 004.056 / UDC: 004.056
С 88

У збірнику подано тези доповідей п’ятої науково-технічної студентської конференції «Студентська Конференція Інформаційна, Функційна і Кібербезпека». Розглянуті питання за такими напрямами: інформаційна безпека; функційна безпека; кібербезпека; управління інформаційною безпекою; захист інформації в інформаційно-комунікаційних системах; системи симетричного та асиметричного шифрування; системи захисту інформації для веб та мобільних додатків; безпека хмарних систем; методи атак та захисту за допомогою штучного інтелекту; захист смарт-системи; захист інтернет речей та автономні системи; нормативно-правові аспекти інформаційної та кібербезпеки. Конференція поділена на три секції: інформаційна та кібербезпека; функційна безпека; правове забезпечення кібербезпеки.

This collection presents the abstracts from the fifth student scientific and technical conference, “Student Conference Information, Functional, and Cybersecurity”. The proceedings cover a range of research areas, including: Information Security; Functional Safety; Cybersecurity; Information Security Management; Data Protection in Information and Communication Systems; Symmetric and Asymmetric Encryption Systems; Information Protection Systems for Web and Mobile Applications; Cloud Systems Security; Attack and Defense Methods utilizing Artificial Intelligence; Smart System Protection; Protection of the Internet of Things and Autonomous Systems; Regulatory and Legal Aspects of Information and Cybersecurity. The conference is structured into three dedicated sections: Information and Cybersecurity; Functional Safety; Cybersecurity Law and Regulation.

С 88 Студентська конференція інформаційна, функційна і кібербезпека СКІФіК: матеріали п’ятої науково-технічної конференції 27-28 листопада 2025 року. – Харків: ФОП Бровін О.В., 2025. – 205 с.
ISBN 978-617-8587-21-5

NATIONAL AEROSPACE UNIVERSITY «KHARKIV AVIATION INSTITUTE»
KHARKIV NATIONAL UNIVERSITY NAMED AFTER. V.N. KARAZINA
UKRAINIAN SCIENTIFIC AND EDUCATIONAL IT SOCIETY
INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES OF THE BULGARIAN ACADEMY OF SCIENCES (SOFIA, BULGARIA)
ICCSS INTERNATIONAL SECURITY CENTER (WARSAW, POLAND)

STUDENT CONFERENCE "INFORMATION, FUNCTIONAL AND CYBERSECURITY"

SCIFiC

Proceedings of the Fifth
Scientific and Technical Conference
27–28 November 2025

Kharkiv 2025

ПРОГРАМНИЙ КОМІТЕТ

ЛИТВИНОВ Олексій Миколайович (д.ю.н., професор, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна);
ПЄВНЄВ Володимир Яковлевич (д.т.н., доцент, професор кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна);
ФЕСЕНКО Герман Вікторович (д.т.н., професор, професор кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна);
ТЕЦЬКИЙ Артем Григорович (к.т.н., доцент кафедри комп'ютерних систем, мереж і кібербезпеки Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна);
ГОРБЕНКО Іван Дмитрович (д.т.н., професор, професор кафедри безпеки інформаційних систем і технологій, Харківський національний університет ім. В. Н. Каразіна, Харків, Україна);
ЗАСЛАВСЬКИЙ Володимир Анатолійович (д.т.н., професор, член Правління Українського науково-освітнього ІТ-Товариства, Харків, Україна);
МІНЧЕВ Златогор (доктор філософії, доцент, керівник відділу інформаційних технологій і кібербезпеки Інституту інформаційних і комунікаційних технологій Болгарської академії наук, Софія, Болгарія);
ПАТУРЕЙ Кшиштоф (президент, Міжнародний центр з безпеки ICCSS, Варшава, Польща).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

ХАРЧЕНКО В'ячеслав Сергійович (д.т.н., професор, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна);
ЮДІН Олесь Вікторович (аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна).
ЗЕМЛЯНКО Георгій Андрійович (PhD з кібербезпеки, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна);
СТЯГЛИК Наталя (к.пед.н., доцент, завідувач кафедри інформаційних технологій та математичного моделювання Навчально-наукового інституту «Каразінський банківський інститут»);
ДРАКОН Дар'я Сергіївна (студентка 4 курсу, Харківський національний університет імені В. Н. Каразіна, м. Харків, Україна).
ФЕДОРЕНКО Дар'я Дмитрівна (студентка 3 курсу, кафедра комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», Харків, Україна).

PROGRAM COMMITTEE

LYTVYNOV Oleksiy Mykolayovych (Doctor of Law, Professor, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine);
PEVNEV Volodymyr Yakovlevych (Dr. Sc. (Tech.), Assoc. Prof., Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine);
FESENKO Herman Viktorovych (Dr. Sc. (Tech.), Professor, Department of Computer Systems, Networks and Cyber Security National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine);
TETSKY Artem Hryhorovych (PhD, Associate Professor, Department of Computer Systems, Networks and Cyber Security National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine);
HORBENKO Ivan Dmytrovych (Dr. Sc. (Tech.), professor, professor of the Department of Security of Information Systems and Technologies, Kharkiv National University named after. V. N. Karazina, Kharkiv, Ukraine);
ZASLAVSKY Volodymyr Anatoliyovych (Dr. Sc. (Tech.), professor, member of the Board of the Ukrainian Scientific and Educational IT Society, Kharkiv, Ukraine);
MINCHEV Zlatogor (PhD, Associate Professor, Head of the Information Technology and Cyber Security Department of the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences, Sofia, Bulgaria);
PATUREY Krzysztof (President, International Center for Security ICCSS, Warsaw, Poland).

ORGANIZATIONAL COMMITTEE

KHARCHENKO Viacheslav Serhiiovych (Dr. Sc. (Tech.), Prof., Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine);
YUDIN Oles Viktorovych (PhD student, Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine);
ZEMLIANKO Heorhii Andriiovych (PhD in Cybersecurity, Assoc. Prof., Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine);
STYAGLYK Natalya (candidate of pedagogical sciences, associate professor, head of the department of information technologies and mathematical modeling of the Educational and Scientific Institute «Karazin Banking Institute»);
DRAKON Daria Sergeevna (4th-year student, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine);
FEDORENKO Daria Dmytrivna (Student of group 535-b, Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine).

ПЛАН ПЕРШОГО ДНЯ КОНФЕРЕНЦІЇ

27 листопада 2025 року, Час: 15:00 – 19:00, онлайн	
15:00 – 15:10	Вітальне слово
15:10 – 15:15	Вітальне слово спонсора конференції «Харківський ІТ Кластер»
15:15 – 15:35	Експерт з кібербезпеки та захисту даних, Руанда Jean Pierre Nzabahimana Тема: From KhAI to a Cybersecurity Leader.
15:35 – 15:55	Спеціаліст з кібербезпеки CyberLab / Національний центр ядерних досліджень, Польща Suchorab Jakub Тема: Cybersecurity Research and Operations at CyberLAB
15:55 – 16:00	Перерва
16:00 – 18:45	Секція 1. Інформаційна та кібербезпека https://meet.google.com/xwr-mxbv-dpc
	Секція 2. Функційна безпека https://meet.google.com/afr-deqo-ghv
	Секція 3. Правове забезпечення кібербезпеки https://meet.google.com/zbt-cxit-fuo
18:45 – 19:00	Обговорення результатів роботи секцій

ПЛАН ДРУГОГО ДНЯ КОНФЕРЕНЦІЇ

28 листопада 2025 року, Час: 15:00 – 19:00, онлайн	
15:00 – 15:05	Оголошення Оргкомітету
15:10 – 15:30	Дослідник з Інститут інформаційних і комунікаційних технологій, Болгарська академія наук, Болгарія Yulian Hristov Тема: Machine Learning Analysis Advancing Security Planning
15:30 – 16:50	Аспірант кафедри 503, НАУ «ХАІ», Україна Іван Рябко Тема: Методи і засоби штучного інтелекту для забезпечення кібербезпеки медичних веб-систем
16:50 – 16:55	Перерва
16:55 – 18:30	Секція 1. Інформаційна та кібербезпека https://meet.google.com/xwr-mxbv-dpc
	Секція 2. Функційна безпека https://meet.google.com/afr-deqo-ghv
	Секція 3. Правове забезпечення кібербезпеки https://meet.google.com/zbt-cxit-fuo
18:30 – 18:45	Перерва
18:45 – 19:00	Підсумкове пленарне засідання

PLAN FOR THE FIRST DAY OF THE CONFERENCE

27 November 2025, 3:00 – 7:00 PM (Kyiv time, UTC+2), Online	
03:00 – 03:15 pm	Welcome words
03:10 – 03:15 pm	Welcome words by the sponsor of the conference, “Kharkiv IT Cluster”
03:15 – 03:35 pm	Cybersecurity and Data Privacy Leader, Rwanda Jean Pierre Nzabahimana Topic: From KhAI to a Cybersecurity Leader.
03:35 – 03:55 pm	Cybersecurity Specialist, CyberLab / National Centre For Nuclear Research, Poland Suchorab Jakub Topic: Cybersecurity Research and Operations at CyberLAB
03:55 – 04:00 pm	Coffee-break
04:00 – 06:45 pm	Section 1. Information and cybersecurity https://meet.google.com/xwr-mxbv-dpc
	Section 2. Functional safety https://meet.google.com/afr-deqo-ghv
	Section 3. Cybersecurity law and regulation https://meet.google.com/zbt-cxit-fuo
06:45 – 07:00 pm	Discussion of Section Results

PLAN FOR THE SECOND DAY OF THE CONFERENCE

28 November 2025, 3:00 – 7:00 PM (Kyiv time, UTC+2), Online	
03:00 – 03:05 pm	Announcement by the Organizing Committee
03:10 – 03:30 pm	Speech by researcher from the Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, Bulgaria Yulian Hristov Topic: Machine Learning Analysis Advancing Security Planning
03:30 – 03:50 pm	PhD student from 503 Department, National Aerospace University "Kharkiv Aviation Institute", Ukraine Ivan Ryabko Topic: Methods and tools of Artificial Intelligence for ensuring cybersecurity of medical web systems
03:50 – 03:55 pm	Coffee-break
03:55 – 06:30 pm	Section 1. Information and cybersecurity https://meet.google.com/xwr-mxbv-dpc
	Section 2. Functional safety https://meet.google.com/afr-deqo-ghv
	Section 3. Cybersecurity law and regulation https://meet.google.com/zbt-cxit-fuo
06:30 – 06:45 pm	Coffee-break
06:45 – 07:00 pm	Closing Plenary Session

ПРОГРАМА КОНФЕРЕНЦІЇ

27 – 28 листопада 2025 року, Онлайн формат

Відкриття конференції, привітання учасників організаторами конференції та запрошеними гостями

Пленарні доповіді:

Експерт з кібербезпеки та захисту даних, Руанда; **Jean Pierre Nzabahimana**. Тема: «From KhAI to a Cybersecurity Leader».

Спеціаліст з кібербезпеки CyberLab / Національний центр ядерних досліджень, Польща; **Suchorab Jakub**. Тема: «Cybersecurity Research and Operations at CyberLAB».

Дослідника з Інститут інформаційних і комунікаційних технологій, Болгарська академія наук, Болгарія; **Yulian Hristov**. Тема: «Machine Learning Analysis Advancing Security Planning».

Аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», Україна; **Рябко Іван Богданович**. Тема: «Методи і засоби штучного інтелекту для забезпечення кібербезпеки медичних веб-систем».

CONFERENCE PROGRAM

27 – 28 November 2025, Online Format

Conference Opening, Welcome of Participants by the Organizers and Invited Guests

Plenary Presentations:

Cybersecurity and Data Privacy Leader, Rwanda; **Jean Pierre Nzabahimana**. Topic: "From KhAI to a Cybersecurity Leader".

Cybersecurity Specialist, CyberLab / National Centre For Nuclear Research, Poland; **Suchorab Jakub**. Topic: "Cybersecurity Research and Operations at CyberLAB".

Researcher from the Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, Bulgaria; **Yulian Hristov**. Topic: "Machine Learning Analysis Advancing Security Planning".

PhD student from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Ukraine; **Ivan Ryabko**. Topic: "Methods and tools of Artificial Intelligence for ensuring cybersecurity of medical web systems".

РОБОТА СЕКЦІЙ / WORK OF SECTIONS

Секція 1. Інформаційна та кібербезпека
Посилання: https://meet.google.com/xwr-mxbv-dpc
Модератор: Юдін Олесь Вікторович

Секція 2. Функційна безпека
Посилання: https://meet.google.com/afr-deqo-ghv
Модератор: Землянко Георгій Андрійович

Секція 3. Правове забезпечення кібербезпеки
Посилання: https://meet.google.com/zbt-cxit-fuo
Модератор: Федоренко Дар'я Дмитрівна

Section 1. Information and cybersecurity
Link: https://meet.google.com/xwr-mxbv-dpc
Host: Oles Yudin

Section 2. Functional safety
Link: https://meet.google.com/afr-deqo-ghv
Host: Heorhii Zemlianko

Section 3. Cybersecurity law and regulation
Link: https://meet.google.com/zbt-cxit-fuo
Host: Daria Fedorenko

ТЕЗИ ДОПОВІДЕЙ

Секція 1. Інформаційна та кібербезпека

ABSTRACTS OF REPORTS

Section 1. Information and cybersecurity

Секція 1

КОНФІДЕНЦІЙНІСТЬ ДАНИХ У СИСТЕМАХ ШТУЧНОГО ІНТЕЛЕКТУ: РИЗИКИ ВИТОКУ ТА ПІДХОДИ ДО ЗАХИСТУ

Антонов Є. О.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Стадник А. О.

Актуальність. Штучний інтелект активно впроваджується у фінансову сферу, медицину, логістику, електронну комерцію та державне управління, що робить питання конфіденційності даних особливо важливим. Сучасні моделі ШІ обробляють великі обсяги персональної інформації, яка може бути ненавмисно розкрита через вразливості алгоритмів або цілеспрямовані атаки. Зокрема, критичність проблеми посилюється можливістю проведення специфічних атак інференсу, які дозволяють зловмисникам реконструювати фрагменти навчальних наборів або деанонімізувати суб'єктів даних через аналіз градієнтів та вихідних ймовірностей моделі. Традиційні методи захисту периметра виявляються недостатніми через непрозорість архітектур глибокого навчання та необхідність забезпечення відповідності нормативним вимогам [1]. Саме тому дослідження ризиків у системах ШІ є актуальним завданням.

Мета роботи. Проаналізувати основні ризики витоку даних у системах штучного інтелекту та визначити сучасні підходи до забезпечення конфіденційності.

Основні положення. Системи штучного інтелекту все частіше працюють з конфіденційними даними користувачів - медичними записами, фінансовою інформацією, логістичними профілями тощо. Високий рівень складності моделей створює нові можливості для атак. Одним із найбільш небезпечних типів є model inversion, коли зловмисник може відновити частину початкових даних, використаних у навчанні. Інший поширений ризик – membership inference, який дозволяє визначити, чи входили конкретні дані в навчальний набір моделі [1, 2, 3].

Крім того, небезпеку становлять атаки через API, коли неправильно захищена система дозволяє дізнатися статистичні властивості даних або витягнути фрагменти відповідей, що містять конфіденційну інформацію. Значною проблемою є також ненавмисна «пам’ять» нейронних мереж, яка може призвести до того, що модель випадково відтворює реальні дані користувачів [1, 4, 5].

Серед ефективних підходів до захисту конфіденційності слід відзначити:

– диференційовану приватність, яка контролює рівень витоку інформації у відповідях моделі [1];

– федеративне навчання, що дозволяє тренувати моделі без централізації даних [4];

– захищені обчислення (Secure Multi-Party Computation, Homomorphic Encryption) [5];

– аудит та тестування моделей на витоки перед розгортанням [5].

Ці технології стають критично необхідними у системах, де обробляються персональні дані.

Висновок. Сучасні системи штучного інтелекту створюють значні виклики у сфері захисту конфіденційності. Атаки на моделі, непрозорість алгоритмів та зростання обсягів даних збільшують ризики витоку інформації [3]. Для мінімізації загроз необхідно впроваджувати сучасні технології захисту – диференційовану приватність, федеративне навчання, захищені обчислення – а також регулярно проводити аудит та моніторинг систем [1, 4, 5]. Комплексний підхід дозволяє значно знизити ризики та забезпечити безпечне використання ШІ.

Список літератури

1. Dwork C., Roth A. The Algorithmic Foundations of Differential Privacy. Нью-Йорк : Now Publishers, 2014

2. Carlini N., Zhang C., Zhang J. та ін. The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks. In: Proceedings of the 28th USENIX Security Symposium, Santa Clara, CA, 2019. P. 263-280

3. European Union Agency for Cybersecurity (ENISA). Artificial Intelligence Threat Landscape. Heraklion : ENISA, 2023. 56 p

4. Google Research. Federated Learning: Collaborative Machine Learning without Centralized Training Data. Mountain View : Google LLC, 2020. 24 p

5. OpenAI Security Practices. OpenAI. URL – https://openai.com/security (дата звернення: 14.11.2025)

Відомості про автора

Антонов Єгор Олексійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.antonov@student.csn.khai.edu

Стадник Анастасія Олександрівна, старший викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.stadnyk@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТЕХНОЛОГІЇ WEBAR

Андрійчук М. С.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Куланов В. О.

Актуальність. В час технологічного прогресу, незважаючи на розвиток методів захисту, зловмисники навчилися адаптуватися та створювати нові загрози для різного роду IT-сегментів, представників компаній, звичайних користувачів мережі Інтернет або провайдерів послуг. Згідно звіту компанії Gartner, близько 188 мільярдів доларів було інвестовано у розвиток інформаційної безпеки [1]. Розвиток безпеки повинен враховувати такі аспекти, як конфіденційність користувачів і сервісів, а також доступність, що дасть змогу ширшому колу людей забезпечити власний захист, водночас мінімізуючи ризики виникнення вразливостей, які можуть бути використані зловмисниками. Одним із сервісів послуг, що також може бути вразливим до зовнішніх атак – є технологія WebAR. Окрім збору звичних даних, наприклад електронної пошти, такі сайти використовують камеру смартфона для реалізації доповненої реальності, що, у разі витоку даних, може наражати користувача на ризик розкриття конфіденційної інформації – зокрема локації, зображення обличчя чи інших особистих відомостей. Згідно з дослідженням, попри значний прогрес у цій сфері, залишаються невирішеними питання, пов'язані із безпекою даних та доцільністю їх використання для подальшого розвитку інфраструктури. Іншими словами, під сумнівом перебувають якість і продуктивність галузі, які можуть суперечити вимогам безпеки потенційних користувачів [2, 3].

Метою даного дослідження є аналіз методів забезпечення безпеки в сфері WebAR технологій.

Враховуючи особливості роботи цієї сфери, яка включає обробку та інтеграцію реального світу через камери смартфонів, необхідно знайти метод за яким пріоритетною є можливість забезпечити користувачу більший рівень конфіденційності, але також забезпечити системі той самий обсяг матеріалу для навчання. Таким чином ціллю є дослідження ефективних механізмів та принципів безпеки, які не погіршують загальний досвід та зручність користування технологією WebAR.

Основні положення. Однією з потреб сучасних інформаційних технологій є збір даних. Аналіз вподобань для розповсюдження реклами,

фідбек для збору реакцій, огляд поведінки і так далі. Повертаючись до потреб WebAR у використанні реального світу, ми можемо спробувати реалізувати декілька моментів для находження балансу між зручністю для користувача, а також безпекою.

Одним з варіантів є можливість розробки архітектуру серверної обробки з шифруванням, коли після надання дозволу користувачем, дані з камери будуть надсилатися на сервер з додатковим шифруванням Encryption-at-rest, після чого відбувається обробка доповненої реальності та результат повертається до користувача).

Інший варіант – локальна обробка, що включає в себе анонімізацію. Деякі з технологій доповненої реальності активно використовують маркери – скриті для зору людини знаки на обраних об'єктах, які при використанні додатку доповненої реальності реалізують прив'язаний контент. Отже, цю можливість можна використати для анонімізації – наприклад, реалізувати функцію видалення обличчя на зображеннях, водночас зберігаючи розпізнавання контурів приміщення (стіни, підлога тощо).

Висновки. Було проведено дослідження розвитку безпеки у сфері WebAR – сфері, яка активно розвивається і яка активно взаємодіє з ризиками конфіденціальної інформації. Але потрібно також враховувати, що навіть у випадку успіху розвитку безпеки, також через деякий час обов'язково виникне розвиток і у ризиках якими будуть користуватися зловмисники, тому ця тема завжди буде актуальна, так як ніколи не стоїть на місці.

Список літератури

1. Bennouk, K.; Ait Aali, N.; El Bouzekri El Idrissi, Y.; Sebai, B.; Faroukhi, A.Z.; Mahouachi, D. A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies. J. Cybersecur. Priv. 2024, 4, 853-908. DOI: https://doi.org/10.3390/jcp4040040

2. El-Hajj, M. Cybersecurity and Privacy Challenges in Extended Reality: Threats, Solutions, and Risk Mitigation Strategies. Virtual Worlds 2025, 4, 1. DOI: https://doi.org/10.3390/virtualworlds4010001

3. Qureshi, I.; Habeeb, M.A.; Shadab, S.G.M.; Mohammad, B.; Irfan, M.; Shavalliuddin, S.M.; Gupta, M. Examining Techniques to Enhance the Security and Privacy of IoT Devices and Networks against Cyber Threats. Eng. Proc. 2024, 62, 23. DOI: https://doi.org/10.3390/engproc2024062023

Відомості про авторів

Андрійчук Максим Сергійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.andriichuk@student.csn.khai.edu

Куланов Віталій Олександрович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», v.kulanov@csn.khai.edu

Секція 1

АНАЛІЗ ПОТОКОВОГО ШИФРУ GRAIN-128A ЯК ОБЧИСЛЮВАЛЬНОГО ЕКСТРАКТОРА ВИПАДКОВОСТІ ДЛЯ QRNG

Анохін Д. А.
Харківський національний університет ім. В. Н. Каразіна, м. Харків, Україна
Науковий керівник: Нарєжній О. П.

Актуальність. Істинно випадкові генератори чисел (TRNG), зокрема квантові (QRNG), є основою сучасної криптографії. Проте, сирі дані, отримані з фізичних джерел, неминуче містять статистичні дефекти (зміщення, автокореляції) через вплив класичного шуму та недосконаліть апаратури [1]. Використання таких "слабких" джерел напряму є неприпустимим, що вимагає обов'язкового етапу постобробки — екстракції випадковості. Традиційні екстрактори на базі хеш-функцій (SHA-3) або блокових шифрів (AES) є ефективними, але обчислювально "важкими" для пристроїв з обмеженими ресурсами (IoT). Потокові шифри, як-от Grain-128a, відомі своєю високою продуктивністю та низькими вимогами до ресурсів, що робить їх дослідження в якості альтернативних екстракторів актуальною задачею кібербезпеки.

Метою даної роботи є теоретичне обґрунтування доцільності використання потокового шифру Grain-128a як обчислювального кондиціонера (екстрактора) для постобробки сирих даних, отриманих з QRNG.

Основні положення. Існують дві основні парадигми постобробки: теоретико-інформаційна (на базі LHL) та обчислювальна (на базі криптографічних припущень). У даній роботі Grain-128a розглядається саме як обчислювальний кондиціонер, що відповідає стандартизованій моделі NIST SP 800-90 (Джерело ентропії + DRBG) [2].

Пропонується архітектура, де 224 послідовних біти сирих даних QRNG (з їхніми дефектами) завантажуються безпосередньо у входи шифру: 128 біт як «Ключ» (Key) та 96 біт як «Вектор ініціалізації» (IV) [3]. У цьому контексті вся 224-бітна послідовність розглядається як єдиний «ентропійний вхід» (seed) для засівання генератора. Теоретичне обґрунтування безпеки такого підходу базується на аналізі 256-тактової фази «прогріву» (warm-up) шифру [3]. Під час цієї фази вихідний потік не генерується; натомість вихід нелінійної функції h(x) подається назад на входи обох регістрів (LFSR та NFSR). Цей механізм зворотного зв'язку

перетворює шифр на замкнену нелінійну динамічну систему, яка 256 разів ітеративно «перемішує» початковий стан.

Ефективність цього перемішування ґрунтується на тому, що архітектура Grain-128a була цілеспрямовано посилена (зокрема, через модифікацію фази ініціалізації та асиметричне заповнення) для протидії диференційним та кубічним атакам, які виявилися успішними проти її попередника, Grain-128 [4].

Висновки. Фаза ініціалізації Grain-128a діє як потужна обчислювальна функція кондиціонування. Її доведена стійкість до складних диференційних та алгебраїчних атак (які зламали її попередника) дає обґрунтовану впевненість, що вона здатна знищити простіші стохастичні залежності, такі як зміщення та кореляції, у сирих даних QRNG. Таким чином, Grain-128a є теоретично обґрунтованим, надійним та ресурсоефективним кандидатом для використання в якості екстрактора випадковості в сучасних системах кібербезпеки.

Список літератури

1. M. Wahl, M. Stoll, and J. S. R. Vazquez. Characterization of a Quantum Random Number Generator Based on Homodyne Detection. Applied Sciences. 2021. 11(16), 7413. URL – https://www.mdpi.com/2076-3417/11/16/7413 (дата звернення: 12.11.2025)

2. National Institute of Standards and Technology. SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation. NIST Computer Security Resource Center. 2018. URL – https://csrc.nist.gov/pubs/sp/800/90/b/final (дата звернення: 12.11.2025)

3. Ågren M., Hell M., Johansson T., Meier W. Grain-128a: A new version of Grain-128 with optional authentication. ECRYPT Stream Cipher Workshop (SKEW 2011), Lund, Sweden. 2011. URL – https://lucris.lub.lu.se/ws/portalfiles/portal/6156802/1981684.pdf (дата звернення: 12.11.2025)

4. H. Zhang, X. Wang. Cryptanalysis of Stream Cipher Grain Family. International Conference on Information Science and Technology. 2011. URL – https://eprint.iacr.org/2009/109 (дата звернення: 12.11.2025)

Відомості про авторів

Анохін Даніїл Андрійович, магістрант кафедри кібербезпеки інформаційних систем, мереж і технологій, ХНУ ім. В. Н. Каразіна, anokhin2020kb12@student.karazin.ua

Нарєжній Олексій Павлович, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій, ХНУ ім. В. Н. Каразіна, к.т.н., o.nariezhnii@karazin.ua

Секція 1

PYTHON ПРОТИ ІНШИХ МОВ У КІБЕРБЕЗПЕЦІ

Артьомов А. І.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Хмарук М. І.

Актуальність. У сучасному цифровому середовищі кіберзагрози стають дедалі складнішими, що вимагає від фахівців з кібербезпеки швидких, ефективних та адаптивних інструментів для виявлення та нейтралізації атак. Python зарекомендував себе як потужний інструмент завдяки своїй простоті, багатій екосистемі бібліотек та широкому застосуванню в автоматизації процесів безпеки, аналізі вразливостей та розробці інструментів для тестування на проникнення.

Метою роботи є дослідження Python у кібербезпеці та його порівняння з іншими мовами для ефективного захисту й автоматизації.

Основні положення. Порівняльний аналіз Python з іншими мовами програмування, такими як C++, Java, Go, Rust дозволяє оцінити його переваги та обмеження в контексті кібербезпеки. Наприклад, Python часто обирають для розробки інструментів автоматизації та скриптів завдяки його простоті та потужним бібліотекам, таким як Scapy та Requests [1]. Однак важливо враховувати й потенційні ризики, пов'язані з використанням Python у кібербезпеці. Наприклад, у 2025 році дослідники виявили багатоступеневу атаку на Python Package Index (PyPI), де зловмисники використовували шкідливі пакети для збору даних розробників [2].

Python є одним із найпопулярніших інструментів у сфері кібербезпеки завдяки простоті освоєння, широкому набору бібліотек та можливості швидкої розробки скриптів для аналізу, тестування й автоматизації. Основні напрямки застосування Python у кібербезпеці включають тестування на проникнення, аналіз шкідливого програмного забезпечення, цифрову криміналістику, захист вебдодатків, автоматизацію процесів безпеки та моніторинг, криптографію та шифрування, а також використання методів штучного інтелекту для виявлення та протидії кібератакам. При порівнянні Python з іншими мовами програмування, такими як C/C++, Java, Go, Rust та Bash, виявляються його специфічні переваги та обмеження у контексті кібербезпеки. Результати аналізу представлені у наступному вигляді. Python широко використовується для

створення скриптів і засобів автоматизації SOC/SIEM, однак має обмеження – низьку швидкодію, велику кількість залежностей та непридатність для роботи в реальному часі. C та C++ забезпечують високу продуктивність, системний контроль і прямий доступ до пам'яті, що робить їх придатними для низькорівневого програмування у сфері безпеки. Водночас ці мови вимагають високої кваліфікації розробника та схильні до помилок управління пам'яттю. Go (Golang) поєднує швидкість виконання, ефективну роботу з паралельними процесами та мінімальну кількість залежностей, однак має відносно невеликий набір бібліотек для кібербезпеки. Rust вирізняється високою швидкодією та безпечною роботою з пам'яттю, що мінімізує ризики вразливостей, пов'язаних із її неправильним використанням. Основним недоліком є складність опанування мови. Bash залишаються ключовими інструментами для автоматизації завдань на рівні операційної системи, проте їхні можливості обмежені при виконанні складних аналітичних обчислень. Java забезпечує високу безпечність завдяки власній віртуальній машині та розвинутим мережевим бібліотекам, однак характеризується повільним запуском програм і громіздкою структурою коду.

Висновки. Python залишається провідним інструментом у кібербезпеці завдяки простоті освоєння, широкому набору бібліотек та швидкій розробці скриптів для аналізу, тестування та автоматизації. Майбутні дослідження мають зосередитися на підвищенні безпеки екосистеми Python, інтеграції з новітніми технологіями та оцінці його ефективності у порівнянні з іншими мовами в умовах сучасних кіберзагроз.

Список літератури

1. 10 Best Programming Languages for Cybersecurity. Legit Security. URL – https://www.legitsecurity.com/aspm-knowledge-base/best-programming-language-for-cyber-security (дата звернення: 05.05.2025)
2. Jordyn Alger. New Research: Multi-Stage Malware Attack on Python Package Index Discovered. Security Magazine. URL – https://www.securitymagazine.com/articles/101700-new-research-multi-stage-malware-attack-on-python-package-index-discovered (дата звернення: 18.06.2025)

Відомості про авторів

Артьомов Артемій Ігорович, студент кафедри інженерії програмного забезпечення, НАУ «ХАІ», a.i.artomov@student.khai.edu
Хмарук Микола Іванович, асистент кафедри інформаційних технологій проєктування, НАУ «ХАІ», m.khmaruk@khai.edu

Секція 1

ДОСЛІДЖЕННЯ МЕТОДІВ ПОШУКУ ВРАЗЛИВОСТЕЙ ЗАСОБАМИ РОЗВІДКИ НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ

Вірський Я. М.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Тецький А. Г.

Актуальність. З розвитком кіберзагроз, кількість атак на інформаційні системи зросла на 84% у 2025 році, де ransomware становить 35% усіх інцидентів [1]. Це призвело до стрімкого зростання використання розвідки на основі відкритих джерел (OSINT) для проактивного виявлення вразливостей. OSINT дозволяє збирати публічно доступну інформацію з інтернету, соціальних мереж та баз даних для ідентифікації потенційних ризиків без прямого доступу до цільової системи [2]. Серед інструментів OSINT, такі як Shodan та Maltego, займають провідні позиції, охоплюючи до 40% ринку кіберрозвідки станом на 2025 рік [3]. Однак, зростання обсягів відкритих даних привернуло увагу зловмисників, які використовують OSINT для рекогносцировки. Згідно зі звітом SentinelOne, 60% нових вразливостей виявляються через OSINT-сканування, але лише 45% організацій впроваджують такі інструменти для захисту [4]. Статистичні дані збираються за допомогою OSINT-платформ, які не тільки сканують відкриті джерела на предмет вразливостей, а й формують аналітику для прогнозування загроз.

Метою даної роботи є дослідження методів пошуку вразливостей за допомогою засобів розвідки на основі відкритих джерел. У дослідженні акцентується увага на систематизації технік пасивного моніторингу цифрового сліду для ідентифікації поверхні атаки без прямої взаємодії з цільовою інфраструктурою. Зокрема, аналізуються алгоритми автоматизованої агрегації метаданих із публічних репозиторіїв, баз даних Whois та спеціалізованих пошукових систем.

Аналізуючи ринок кібербезпеки, дослідники компанії CrowdStrike виявили нові тенденції в OSINT-атаках, де зловмисники використовують інструменти на кшталт Recon-ng для виявлення незахищених API та конфігурацій. Такі методи дозволяють швидко ідентифікувати вразливості в хмарних сервісах та IoT-пристроях. Способом поширення загроз є публічно доступні бази даних, такі як Shodan, де зловмисники шукають незахищені порти [5].

Основні положення. Для своєчасного виявлення вразливостей використовуються два типи OSINT-методів: пасивні (збір даних без взаємодії) та активні (сканування з мінімальним впливом). Серед пасивних інструментів ефективним є Shodan, який сканує інтернет на наявність відкритих портів та вразливих пристроїв по базі CVE. При аналізі, інструмент перевіряє конфігурації серверів, незахищені сервіси та метадані. База CVE є однією з найбільших баз вразливостей у кіберпросторі. У роботі розглянуто переваги та недоліки OSINT-інструментів, таких як Maltego для візуалізації зв'язків та Recon-ng для автоматизованої рекогносцировки.

Висновки. Розвідка на основі відкритих джерел (OSINT) є невід'ємною частиною сучасних технологій кібербезпеки та має багатогранні інструменти для пошуку вразливостей. Однак, більшість інструментів не інтегровані за замовчуванням у корпоративні системи. Більшість фахівців не орієнтовані на повне використання OSINT через брак знань. Зменшити ризик кібератак можна за допомогою OSINT-сканерів, однак даний метод є лише емпіричним інструментом і не гарантує повну безпечність.

Список літератури

1. Key Cyber Security Statistics for 2025. SentinelOne. URL – https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics (дата звернення: 12.11.2025)
2. What is OSINT Open Source Intelligence? CrowdStrike. URL – https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/open-source-intelligence-osint (дата звернення: 12.11.2025)
3. Top 15 OSINT Tools For Cybersecurity In 2026. Cyble. URL – https://cyble.com/knowledge-hub/top-15-osint-tools-for-powerful-intelligence-gathering (дата звернення: 12.11.2025)
4. 192 Cybersecurity Statistics for 2025. Indusface Blog. URL – https://www.indusface.com/blog/key-cybersecurity-statistics (дата звернення: 12.11.2025)
5. Top 9 OSINT Tools. Wiz. URL – https://www.wiz.io/academy/osint-tools (дата звернення: 12.11.2025)

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 ЩОДО ЗАХИСТУ БАЗ ДАНИХ ВЕБ-СЕРВІСІВ

Власова Злата Олексіївна
Харківського національного університету внутрішніх справ, м. Харків, Україна
Науковий керівник: Землянко Г.А.

Актуальність. Веб-сервіси (Web-Services) і API є основою сучасної цифрової інфраструктури, забезпечуючи взаємодію між додатками і доступ до даних. Центральним компонентом цих послуг є бази даних (BD), які агрегують і зберігають важливу інформацію, включаючи персональні дані користувачів, фінансові операції та комерційну таємницю. Згідно з статистикою, бази даних стають основною мішенню для кібератак, а витоки даних призводять до величезних репутаційних і фінансових втрат, що підкреслює неадекватність традиційних систем захисту периметра [1].

Метою даної роботи є аналіз актуальних векторів атак на бази даних, що використовуються веб-сервісами, та систематизація сучасних методів захисту.

Найбільш критичною та поширеною загрозою залишається «Ін’єкція» (Injection), яка незмінно займає лідируючі позиції в рейтингу OWASP Top 10 (A03:2021) [2]. Ця категорія включає як класичні SQL-ін’єкції, так і NoSQL-ін’єкції, спрямовані на нечутливі сховища (наприклад, MongoDB, Redis), які часто використовуються в архітектурі сучасних веб-сервісів. Крім того, «Неправильна конфігурація безпеки» (A05:2021) представляє високий ризик, наприклад, використання паролів за замовчуванням, відсутність шифрування або відкриття портів SUBD для загального доступу.

Основні положення. Для протидії атакам типу «Ін’єкція» застосовується багаторівневий підхід, що починається на рівні застосунку. Він включає сувору валідацію та санітарну обробку вхідних даних, а також повну відмову від динамічної конкатенації SQL. Ключовим є використання параметризованих запитів (prepared statements) та ORM-фреймворків, які абстрагують доступ до БД та автоматично екранують спецсимволи [3].

Другий рівень захисту будується на стороні СУБД. Тут обов'язково застосовується принцип найменших привілеїв (PoLP), що жорстко обмежує права доступу облікового запису веб-сервісу. Додатково, для захисту самих даних, застосовується шифрування «даних у спокої» (data-at-rest) за

допомогою механізмів TDE та «даних у дорозі» (data-in-transit) з використанням актуальних версій TLS [4].

Третій, проактивний рівень захисту, включає моніторинг і аудит. Використання брандмауерів веб-додатків (WAF) дозволяє фільтрувати шкідливий трафік, включаючи спроби ін'єкції, ще до того, як він досягне веб-сервісу. Системи класу Database Activity Monitoring (DAM) забезпечують безперервний моніторинг запитів баз даних у реальному часі шляхом виявлення аномальної активності (наприклад, нетипових запитів від законного облікового запису або перевизначень) і автоматичного їх блокування відповідно до концепції Zero Trust [1, 4].

Висновки. Захист бази даних веб-сервісів вимагає комплексного багаторівневого підходу, що охоплює код програми, конфігурацію сервера БД і моніторинг мережевої активності. Недостатня увага до будь-якого з цих рівнів створює критичні вразливості. Однією з неочевидних загроз є небезпечна обробка винятків (винятків) у коді веб-сервісу, що може розкрити структуру бази даних або версії програмного забезпечення зловмиснику. У тезах розглянуто основні вектори атак та запропоновано класифікацію захисних заходів, яка формує основу для побудови безвідмовної та захищеної архітектури веб-сервісу.

Список літератури

1. A comprehensive survey of cybersecurity threats, attacks, and effective countermeasures in industrial internet of things / A. M. Alnajim et al. *Technologies*. 2023. Vol. 11, no. 6. P. 161. DOI: https://doi.org/10.3390/technologies11060161

2. A03 injection – OWASP top 10:2021. *OWASP Foundation*. URL – https://owasp.org/Top10/A03_2021-Injection (дата звернення: 23.10.2025)

3. Ron A., Shulman-Peleg A., Puzanov A. Analysis and mitigation of nosql injections. *IEEE security & privacy*. 2016. Vol. 14, no. 2. P. 30–39. DOI: https://doi.org/10.1109/msp.2016.36

4. Ensuring the data integrity in infocommunication systems / V. Pevnev et al. *International journal of computing*. 2022. P. 228–233. DOI: https://doi.org/10.47839/ijc.21.2.2591

Відомості про авторів

Власова Злата Олексіївна, магістрант кафедри кібербезпеки та DATA-технологій ННІ № 5, Харківського національного університету внутрішніх справ (ХНУВС)

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

Секція 1

ЗАСТОСУВАННЯ КРИПТОГРАФІЧНОЇ ГЕШ-ФУНКЦІЇ SHA-3 ЯК ЕКСТРАКТОРА ВИПАДКОВОСТІ ДЛЯ QRNG

Волотковський Д. С.
Харківський національний університет ім. В. Н. Каразіна, м. Харків, Україна
Науковий керівник: Нарєжній О. П.

Актуальність. Квантові генератори випадкових чисел (КГВЧ, QRNG) є основою сучасної криптографії, оскільки використовують фундаментальну квантову невизначеність для генерації істинно випадкових послідовностей. Проте, «сирі» (raw) дані, отримані безпосередньо з КГВЧ, неминуче містять статистичні дефекти через вплив класичного шуму, теплові флуктуації детекторів та недосконаліть вимірювальної апаратури. До них належать зміщення (bias) у розподілі ймовірностей бітів та, що більш небезпечно, часові автокореляції – прихована статистична залежність між послідовними значеннями вибірки. Наявність цих дефектів критично знижує реальну непередбачуваність (мін-ентропію) вихідного потоку, створюючи вектори атак для прогнозування ключів шифрування. Це робить обов'язковою імплементацію процедур постобробки – алгоритмічної екстракції випадковості (randomness extraction) на базі універсальних хеш-функцій або екстракторів Тепліца, що дозволяє нівелювати вплив апаратних артефактів та гарантувати криптографічну стійкість генеруємої послідовності відповідно до стандартів NIST SP 800-90B [1].

Метою даної роботи є теоретичне обґрунтування доцільності використання криптографічної геш-функції SHA-3 як обчислювального екстрактора для постобробки «сирих» статистично дефектних даних, отриманих з КГВЧ.

Основні положення. Аналіз простих статистичних екстракторів, що не враховують автокореляції, продемонстрував їхню категоричну непридатність для постобробки квантових даних. Їхня теорія працює лише за критичного припущення, що вхідні біти є незалежними та однаково розподіленими (IID) [2]. «Сирі» дані КГВЧ, що містять автокореляції, прямо порушують це припущення, тому метод не усуває залежності [2]. SHA-3, на відміну від SHA-2 (з конструкцією Меркла-Дамгарда), використовує інноваційну губкову конструкцію (sponge construction). Її внутрішня функція Keccak-f забезпечує потужний лавинний ефект

(avalanche effect), а нелінійний крок χ (Chi) визначений як $a' = a \oplus ((\neg b) \wedge c)$, гарантовано руйнує кореляції. SHA-3 є детерміністичним екстрактором (не вимагає «зерна»), що вирішує «проблему курки та яйця» та надає XOF (SHAKE) для виходу довільної довжини [2,3]. Зокрема, застосування функцій SHAKE128/256 дозволяє гнучко адаптувати пропускну здатність (throughput) постобробки до швидкості фізичного джерела, виконуючи функцію конденсора ентропії. Це забезпечує ефективне згладжування (smoothing) вхідного розподілу з низькою мін-ентропією та стійкість до атак на розрізнення (distinguishing attacks).

Висновки. «Сирі» дані КГВЧ є статистично дефектними через наявність автокореляцій. Прості методи (напр., Фон Неймана) недієві, оскільки базуються на хибному для КГВЧ припущенні IID. Криптографічна геш-функція SHA-3 є прагматичним та надійним інженерним рішенням. Її губкова конструкція та нелінійні властивості гарантовано руйнують складні статистичні залежності, перетворюючи дефектний потік на криптографічно стійку випадковість, що успішно проходить верифікацію за стандартами NIST SP 800-22 та Dieharder..

Список літератури

1. Ma, X., et al. (2013). Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. Physical Review A, 87(6). URL: https://arxiv.org/pdf/1207.1473 (дата звернення: 11.11.2025)

2. Vadhan, S. P. (2012). Pseudorandomness: Randomness Extractors. Foundations and Trends® in Theoretical Computer Science, 7(1–3). URL: https://people.seas.harvard.edu/~salil/pseudorandomness/extractors.pdf (дата звернення: 11.11.2025)

3. Dworkin, M. (2015). SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions (NIST FIPS 202). URL: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.202.pdf (дата звернення: 11.11.2025)

Відомості про авторів

Волотковський Дмитро Сергійович, магістрант кафедри кібербезпеки інформаційних систем, мереж і технологій, ХНУ ім. В. Н. Каразіна, volotkovskyi2020kb12@student.karazin.ua

Нарєжній Олексій Павлович, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій, ХНУ ім. В. Н. Каразіна, к.т.н., o.nariezhnii@karazin.ua

Секція 1

ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ ІГРОВОЇ ПЛАТФОРМИ STEAM

Ганзера М. О.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Бабешко Є. В.

Актуальність. У сучасному цифровому середовищі ігрові платформи стали привабливою мішенню для кіберзлочинців. Найбільшою платформою на даний момент є Steam - сервіс цифрової дистрибуції ігор для ПК [1], який щодня обробляє мільйони транзакцій і зберігає величезні обсяги даних користувачів, включаючи платіжну інформацію, цифрові активи та ідентифікаційні дані. Зростання частоти фішингу, крадіжок облікових записів та атак шкідливого програмного забезпечення [2] підкреслює нагальну потребу в надійних механізмах кібербезпеки. Тому вивчення технологій безпеки Steam є надзвичайно важливим для розуміння того, як великі споживчі платформи захищаються кіберзагроз, що постійно розвиваються. Забезпечення цілісності екосистеми вимагає впровадження адаптивних алгоритмів виявлення аномалій та криптографічного захисту каналів передачі даних в умовах високонавантаженої розподіленої архітектури.

Метою роботи є аналіз технологій та протоколів кібербезпеки, що використовуються платформою Steam для забезпечення захисту даних користувачів, запобігання несанкціонованому доступу та підтримання цілісності платформи. Аналіз дозволить отримати практичні висновки, які можна застосувати до інших великомасштабних цифрових платформ, що сприятиме поліпшенню стратегій управління безпекою та зменшенню ризиків у галузі ігор та цифрових послуг.

Основні положення. Steam використовує систему двофакторної аутентифікації (2FA) під назвою Steam Guard [3], яка пов'язує обліковий запис користувача з його підтвердженою електронною адресою або мобільним пристроєм. Система використовує одноразові паролі на основі часу (TOTP) для запобігання несанкціонованим входам. Протоколи шифрування TLS (Transport Layer Security) для всіх комунікацій між клієнтами та серверами, забезпечує шифрування передачі даних та захист від атак типу «людина посередині». Також відстежується активність входу та позначаються незвичайні сеанси. Таким чином, вхід з нового пристрою викликає перевірку електронною поштою або мобільним телефоном, що

зменшує ризик перехоплення сеансу. Steam інтегрує систему управління цифровими правами (DRM) [4] для запобігання піратству та несанкціонованому поширенню контенту. А Steamworks API керує безпечною взаємодією між іграми та платформою. Платформа активно використовує автоматизовані системи аналізу поведінки та виявлення аномалій для виявлення підозрілої активності облікового запису. Служба підтримки Steam використовує багаторівневу перевірку для відновлення ідентичності, а утримання торгів та функції безпеки ринку спільноти мінімізують шахрайські торги та спроби фішингу в цифровій економіці.

Висновки. Підсумовуючи, можна сказати, що модель кібербезпеки Steam поєднує багаторівневий захист, адаптивну реакцію та відкриту комунікацію. Також, прозора співпраця Valve з спільнотою з питань безпеки та швидке вирішення інцидентів значно зміцнюють її репутацію та стійкість. Постійно вдосконалюючи системи шифрування, аутентифікації та виявлення шахрайства, Steam демонструє, як проактивна, прозора стратегія кібербезпеки може стати не тільки захисним інструментом, але й конкурентною перевагою. Такий підхід підкреслює важливий принцип галузі: максимальна відкритість у вирішенні питань безпеки сприяє зміцненню довіри користувачів та корпоративної репутації ефективніше, ніж мовчазне виправлення помилок.

Список літератури

1. Top 5 Gaming Platforms Of 2025. *TechDogs.* URL – https://www.techdogs.com/td-articles/product-mine/top-gaming-platform (дата звернення: 21.10.2025)
2. The Latest 2025 Phishing Statistics (updated October 2025). *AAG*. URL – https://aag-it.com/the-latest-phishing-statistics (дата звернення: 22.10.2025)
3. What Is Steam Guard? The Comprehensive. CS2.ad. URL – https://blog.cs2.ad/what-is-steam-guard (дата звернення: 22.10.2025)
4. What Is Digital Rights Management (DRM)? FORTINET. URL – https://www.fortinet.com/resources/cyberglossary/digital-rights-management-drm (дата звернення: 23.10.2025)

Відомості про авторів

Ганзера Марина Олексіївна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.o.ganzera@student.csn.khai.edu
Бабешко Євген Васильович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., e.babeshko@csn.khai.edu

Секція 1

АНАЛІЗ ВИТОКІВ ДАНИХ СПРИЧИНЕНИХ ШТУЧНИМ ІНТЕЛЕКТОМ

Гарт Д. О.
Харківський національний університет внутрішніх справ, м. Харків, Україна
Науковий керівник: Цуранов М. В.

Актуальність. Штучний інтелект (ШІ) все більше проникає в різні сфери життя від побуту до освіти. У повсякденному використанні ШІ вже працює в пошукових системах, де аналізує запити та надає відповіді, так і у текстових редакторах, які доповнюють речення, узагальнюють тексти та генерують чернетки. Основою ШІ є моделі, тобто алгоритми, які навчаються на великих обсягах даних, щоб виконувати завдання, які потребують людського мислення. Розвиток таких моделей бере початок у 1950-х роках. Зідно з базою даних Epoch AI [1], у цей період було створено близько 10 експериментальних моделей, зокрема Theseus та ADALINE. У наступні десятиліття з'явилися складніші архітектури, серед яких Cognitron, LSTM, які поступово вдосконалювали можливості машинного навчання. Наприклад, у 1980–1990-х роках було розроблено близько 30 моделей, а у 2000–2010-х існувало вже понад 70 моделей. Починаючи з 2010 року, розпочалася ера машинного навчання, під час якої було створено сотні потужних моделей – GANs, GPT-3, GPT-4, Gato тощо. Цей період характеризується стрімким зростанням кількості та складності моделей, було створено більше ніж 1000 систем, це суттєво вплинуло на використання штучного інтелекту. Станом на 2025 рік, база Epoch AI містить понад 3100 моделей ШІ, з чіткою динамікою зростання: від експериментальних систем у 1950-х роках до сотень нових моделей щороку після 2017 [1]. З того часу люди почали використовувати ШІ скрізь, в тому числі для обробки конфіденційних даних.

Метою даної роботи є провести аналіз витоку даних які були спричинені використанням систем штучного інтелекту.

Основні положення. Існує багато випадків коли співробітники компаній надавали ШІ доступ до корпоративних даних, так зокрема, у січні 2023 року Amazon виявила, що відповіді ChatGPT майже дослівно відтворювали внутрішні документи компанії включно з кодом і звітами. Після того, як співробітники ввели цю інформацію в модель для допомоги в роботі [2]. У відповідь Amazon негайно видала офіційне попередження всім працівникам про заборону вводити будь-яку конфіденційну

інформацію в ChatGPT, посилила моніторинг використання зовнішніх ШІ-інструментів і нагадала про ризики витоку через можливе використання даних для тренування моделі [2]. У квітні 2023 року працівники компанії Samsung Electronics ненавмисно ввели в ChatGPT чутливу інформацію, включно з вихідним кодом програмного забезпечення та внутрішніми нотатками, що призвело до витоку даних [3]. Інцидент стався через використання ШІ для оптимізації робочих процесів. В результаті компанія Samsung запровадила політику, що забороняє використання зовнішніх генеративних ШІ на робочих пристроях та підсилила заходи безпеки, включаючи внутрішні роз'яснення щодо ризиків таких технологій. Цей випадок підкреслив вразливість компаній до витоків даних через некероване використання ШІ та необхідність чітких корпоративних політик безпеки [3].

Висновки. Через витоки даних компанії зазнали значних репутаційних та економічних збитків. Штучний інтелект, використовуючи інтелектуальну власність приватних компаній для навчання, може ненавмисно передавати її іншим користувачам. Це створює ризики неконтрольованого поширення конфіденційної інформації. Для запобігання витоку конфіденційних даних перш за все необхідно постійно навчати співробітників, розробляти політики безпеки, які будуть регламентувати правила використання ШІ, а також впроваджувати технічні засоби захисту, що унеможливлюють витоки даних через ШІ-системи.

Список літератури

1. Дані про моделі штучного інтелекту. Epoch. URL: https://epoch.ai/data/ai-models (дата звернення: 05.10.2025)

2. Amazon попереджає співробітників про обережність із ChatGPT. Gizmodo. URL: https://gizmodo.com/amazon-chatgpt-ai-software-job-coding-1850034383 (дата звернення: 07.10.2025)

3. Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak. Bloomberg. URL – https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak (дата звернення: 10.10.2025)

Відомості про авторів

Гарт Дарина Олегівна, студентка кафедри кібербезпеки та DATA-технологій, ННІ № 5 Харківського національного університету внутрішніх справ, darina.hart10@gmail.com

Цуранов Михайло Віталійович, ст. викладач кафедри кібербезпеки та DATA-технологій ННІ № 5 Харківського національного університету внутрішніх справ, ukrear2006@gmail.com

Секція 1

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ У ВЕБДОДАТКАХ

Гродецький О. С.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Фесенко Г. В.

Актуальність. Вебдодатки є основою цифрової інфраструктури – від корпоративних систем до банківських сервісів, але з розвитком веб-технологій зростає й кількість кібератак, коли зловмисники експлуатують SQL-ін'єкції, міжсайтовий скриптинг (Cross Site Scripting, XSS), міжсайтова підробка запиту (Cross Site Request Forgery, CSRF) та інші вразливості коду, знаходячи логічні помилки у коді [1]. Проблема в тому, що класичні методи — сигнатурний аналіз і статичне сканування – не встигають за новими загрозами, адже розпізнають лише відомі атаки, але безсилі перед комбінованими чи новими експлойтами. Саме тому все більше уваги приділяється штучному інтелекту (ШІ), який здатний навчатися на реальних прикладах атак і виявляти аномалії в поведінці як користувачів, так і самого вебдодатка, що робить його незамінним інструментом для сучасної кібербезпеки.

Мета. Дослідити та розробити практичні методи застосування машинного навчання для автоматичного виявлення вразливостей у вебдодатках на всіх етапах їх життєвого циклу – від стадії розроблення та тестування до реальної експлуатації в продакшн-середовищі.

Основні положення. Машинне навчання дає можливість аналізувати вебзапити, логи подій і навіть структуру HTML/JS-коду, виявляючи в них ознаки потенційної небезпеки, використовуючи при цьому перевірені алгоритми – метод випадкового лісу (Random Forest), метод опорних векторів (Support Vector Machine, SVM), а також глибокі нейронні мережі (Deep Neural Network, DNN), які вміють знаходити закономірності в поведінці користувачів і систем [2]. Особливо цікавим є динамічний аналіз HTTP-трафіку, де ШІ виявляє аномальні патерни – наприклад, серії однакових POST-запитів чи підозрілі символи у рядках, а автоенкодери й рекурентні мережі допомагають знаходити нові типи атак без наявних сигнатур [3]. Важливим технічним аспектом реалізації є попередня обробка даних, що включає токенізацію та векторизацію пейлоадів за допомогою методів NLP (Word2Vec, BERT) для перетворення неструктурованих даних

у векторний простір ознак. У дослідженні запропонована концепція інтеграції ШІ-модуля безпосередньо в CI/CD-конвеєр, що дає змогу автоматично перевіряти кожен новий коміт вебдодатка, виявляти вразливості на ранніх етапах і постійно покращувати модель на основі отриманих результатів та зворотного зв'язку від системи [4].

Висновки. Застосування ШІ у кіберзахисті вебдодатків підвищує точність виявлення вразливостей і швидкість реакції на загрози, адже поєднання традиційних сканерів із моделями машинного навчання створює адаптивну систему, що самонавчається та оцінює ризики за контекстом. Подальші дослідження передбачають застосування навчання з підкріпленням (Reinforcement Learning, RL) для автоматизованого прийняття рішень щодо блокування підозрілих запитів безпосередньо в режимі реального часу, що сприятиме формуванню повністю автономної системи захисту вебдодатків.

Список літератури

1. OWASP Foundation. OWASP Top Ten Web Application Security Risks. 2017. URL – https://owasp.org/www-project-top-ten (дата звернення: 03.11.2025)
2. Kaur R., Gabrijelčić D., Klobučar T. Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. Information Fusion, 2023. DOI: https://doi.org/10.1016/j.inffus.2023.101804 (дата звернення: 03.11.2025)
3. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, 2010. DOI: https://doi.org/10.1109/SP.2010.25 (дата звернення: 05.11.2025)
4. NIST. Managing Cybersecurity and Privacy Risks in the Age of Artificial Intelligence. National Institute of Standards and Technology, 2024. URL: https://www.nist.gov/blogs/cybersecurity-insights (дата звернення: 06.11.2025)

Відомості про авторів

Гродецький Олексій Сергійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.s.hrodetskyi@student.csn.khai.edu
Фесенко Герман Вікторович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., h.fesenko@csn.khai.edu

Section 1

SECURE USER AUTHENTICATION IN MODERN

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

Relevance. In the contemporary digital landscape, the issue of secure user authentication remains one of the most pressing concerns. Even today, the most common password worldwide is “123456”, and a considerable proportion of users continue to rely on passwords shorter than twelve characters or composed solely of digits. Equally widespread is the practice of reusing the same password across multiple services, which significantly weakens the overall security posture. Such behaviour leaves modern applications increasingly vulnerable to attacks, phishing attempts, and unauthorised access. For these reasons, the question of ensuring secure authentication stands among the most important challenges.

Objective. The aim of this study is to examine the fundamental principles and contemporary approaches to secure user authentication. Particular attention is given to the methods adopted by leading companies and developers, as well as to the solutions designed to reduce the likelihood of unauthorised access and mitigate the risks associated with the human factor.

Key Points. Secure authentication is grounded in a defence-in-depth model, as a single password can no longer be considered an adequate barrier. While passwords remain the fundamental means of verifying identity, their protective value depends entirely on the user’s ability to create a unique and sufficiently complex combination. Even long passwords become ineffective when reused across multiple platforms or stored insecurely. To mitigate such behavioural vulnerabilities, password managers are increasingly employed, ensuring both the generation of strong credentials and their encrypted storage [1].

A strong password, however, forms only the first step in a resilient authentication system. Two-factor authentication adds an independent layer of verification and significantly increases resistance to unauthorised access [3]. Hardware security keys and applications generating time-based one-time codes are currently viewed as the most dependable methods, whereas SMS-based solutions are considered comparatively weak. Alongside this, modern systems are moving toward passwordless authentication, including WebAuthn and biometric validation, which reduce reliance on traditional character-based credentials and diminish susceptibility to phishing attacks.

Equally important is the protection of authentication data on the server side and the defence against automated threats. Contemporary systems employ robust hashing algorithms such as bcrypt, scrypt, and Argon2, combined with salt values, which prevents the recovery of original passwords even in the event of a data breach. Rate-limiting mechanisms, behavioural analysis, CAPTCHA verification and bot-detection systems further strengthen resilience by identifying suspicious activity during its earliest stages [2]. Furthermore, the evolution of authentication paradigms is increasingly shifting towards Zero Trust architectures and Continuous Authentication models. These approaches utilize machine learning algorithms to analyze telemetry data and user behavioral biometrics in real-time, ensuring that identity verification is not a one-time event but a continuous process that dynamically assesses trust levels throughout the entire session.

Conclusion. Taken together, secure authentication is a layered process whose effectiveness relies on the combined use of modern cryptographic methods, multi-factor verification and reliable server-side data protection. In a digital environment where automated attacks continue to grow in sophistication, measures such as strong hashing algorithms, hardware-based keys and passwordless WebAuthn technologies significantly enhance resilience against unauthorised access. Yet the human element remains critical: no technical solution can be fully effective without responsible user behaviour.

List of references

1. NIST Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management. – National Institute of Standards and Technology, 2023. URL: https://pages.nist.gov/800-63-3/sp800-63b.html (date of access: 13.11.2025)
2. Authentication Cheat Sheet. OWASP Foundation. URL – https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html (date of access: 14.11.2025)
3. WebAuthn & FIDO2 Technical Overview. FIDO Alliance. URL – https://fidoalliance.org/specifications (date of access: 15.11.2025)

Information about the authors

Daria Drakon, student of ERI “Karazin Banking Institute”, Cybersecurity in Finance, daria.drakon@student.karazin.ua
Natalya Stiahlyk, Head of the Department of Information Technology and Mathematical Modeling, Karazin Banking Institute, V.N. Karazin Kharkiv National University, Ph.D., natalia.stiahlyk@karazin.ua

Секція 1

ІНФОРМАЦІЙНА БЕЗПЕКА СИСТЕМ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

Дудка Б. А.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Стадник А.О

Актуальність. Технології доповненої реальності (AR) активно впроваджуються у різні сфери діяльності, зокрема освіту, маркетинг, медицину та обслуговування [1]. Водночас їх використання супроводжується зростанням ризиків, пов'язаних із обробкою персональних даних користувачів, передачею мультимедійного контенту та можливістю втручання у роботу програмного забезпечення. Тому питання інформаційної безпеки у системах доповненої реальності набувають особливої актуальності.

Мета. Забезпечення конфіденційності, цілісності та доступності даних у AR-додатках шляхом виявлення потенційних загроз і розроблення рекомендацій для безпечної взаємодії користувачів із цифровим контентом.

Основні положення. Системи доповненої реальності базуються на інтеграції цифрового контенту у фізичне середовище через обробку відеопотоку з камер пристроїв, аналіз просторових координат, позиційних маркерів і сенсорних даних [3,4]. Для забезпечення роботи AR-додатків часто використовуються хмарні сервіси, що дозволяють зберігати та обробляти 3D-моделі, текстури, аудіо- й відеофайли, а також дані користувачів [5].

Основні загрози інформаційній безпеці включають несанкціонований доступ до відеопотоку, підміну або спотворення контенту, компрометацію облікових даних, а також уразливості у бібліотеках AR SDK (зокрема ARCore, ARKit, Vuforia) та механізмах обробки просторових метаданих [2,3]. Витік таких даних може розкрити інформацію про місцезнаходження користувача, його біометричні параметри або поведінкові шаблони. Для запобігання маніпуляціям сенсорними даними (Sensor Spoofing), що загрожують травмуванням через спотворення реальності, необхідно впровадити перехресну верифікацію датчиків (Sensor Fusion) та використовувати довірені середовища виконання (TEE) для ізоляції критичних процесів рендерингу.

Для підвищення рівня захищеності пропонується реалізація багаторівневої автентифікації, застосування сучасних методів шифрування каналів зв'язку (TLS 1.3 або DTLS 1.2), контроль цілісності переданих даних, періодичне оновлення бібліотек і компонентів SDK, а також обмеження доступу до камер, мікрофонів і сенсорів згідно принципу найменших привілеїв. Важливо, щоб розробники AR-додатків упроваджували політику безпеки даних ще на етапі проєктування («Security by Design») та дотримувалися вимог GDPR і ISO/IEC 27001 під час обробки персональної інформації.

Висновки. Проведений аналіз показав, що впровадження технологій доповненої реальності потребує комплексного підходу до забезпечення інформаційної безпеки, який охоплює як технічні, так і організаційні аспекти. Використання сучасних криптографічних протоколів, надійних методів автентифікації, а також системного контролю доступу до апаратних і програмних ресурсів дозволяє суттєво зменшити ризики кібератак[5], запобігти витоку конфіденційних даних та забезпечити довіру користувачів до мобільних AR-додатків.

Список літератури

1. Azuma R. A Survey of Augmented Reality. *Presence: Teleoperators and Virtual Environments*, 1997. DOI: https://doi.org/10.1162/pres.1997.6.4.355
2. Muhammad Z., Anwar Z., Javed A. R., Saleem B., Abbas S., Gadekallu T. R. Smartphone Security and Privacy: A Survey on APTs, Sensor-Based Attacks, Side-Channel Attacks, Google Play Attacks, and Defenses. *Technologies*, 2023, 11(3): 76. DOI: https://doi.org/10.3390/technologies11030076
3. Vuforia Developer Library. Vuforia. URL – https://developer.vuforia.com (дата звертання: 28.10.2025)
4. Unity AR Foundation Documentation. Unity Technologies. URL – https://docs.unity3d.com/Packages/com.unity.xr.arfoundation (дата звертання: 28.10.2025)
5. Kharchenko V. Functional Safety and Cybersecurity in Intelligent Systems. Springer, 2021. DOI: https://doi.org/10.1007/978-3-030-77411-0

Відомості про авторів

Дудка Богдан Андрійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», b.dudka@csn.khai.edu
Стадник Анастасія Олександрівна, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.stadnyk@csn.khai.edu

Секція 1

АНАЛІЗ ЗАГРОЗ БЕЗПЕЦІ В ІНТЕРНЕТІ РЕЧЕЙ (IoT) ТА МЕТОДІВ ЇХ УСУНЕННЯ

Єрофєєв М. Д.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Пєвнєв В. Я.

Актуальність. У сучасному цифровому середовищі Інтернет речей (IoT) стрімко інтегрується в повсякденне життя, охоплюючи як побутові пристрої (розумні годинники, системи «розумного дому»), так і промислові рішення (сенсори, системи моніторингу та управління). За прогнозами Statista, до 2030 року кількість IoT-пристроїв перевищить 25 мільярдів [1]. Масове підключення створює нові можливості для бізнесу та суспільства, проте одночасно загострює проблему кібербезпеки. Уразливості IoT здатні призвести до витоку конфіденційних даних, порушення цілісності даних і роботи критичної інфраструктури та масштабних DDoS-атак [2,3].

Метою роботи є визначення ключових загроз безпеці IoT та аналіз сучасних методів їх усунення для забезпечення стабільної та безпечної роботи таких систем.

Основні положення. Основною частиною доповіді є аналіз загроз середовищем, які можуть призвести як до незначних збоїв у IoT, так і до фатальних наслідків.

Серед головних загроз безпеці IoT можна виокремити:

– проблеми автентифікації та відсутність багаторівневого контролю доступу;
– низький рівень шифрування каналів передачі даних;
– відсутність централізованих оновлень та перевірки прошивок;
– високий ризик перетворення пристроїв на частину ботнетів [2].

Під час доповіді для підвищення рівня захисту IoT пропонується застосовувати такі рішення:

– використання захищених протоколів (TLS, DTLS) для передачі даних;
– впровадження багатофакторної автентифікації та управління ключами;
– автоматизовані механізми оновлення програмного забезпечення з перевіркою цілісності;

– сегментація мережі та моніторинг аномальної активності [4,5].

Окрему увагу приділено імплементації легковагових криптографічних алгоритмів для ресурсномістких сенсорів, що не підтримують стандартні методи шифрування, а також розгортанню IDS/IPS систем безпосередньо на граничних шлюзах (Edge Gateway), що дозволяє нівелювати атаки на периферії мережі без навантаження на центральні сервери.

Важливим напрямком також є підвищення обізнаності користувачів і виробників щодо необхідності безпечної конфігурації пристроїв, регулярного оновлення прошивок та дотримання принципів кібергігієни, таких як оновлення паролів, використання брандмауерів, обмежений доступ, резервне копіювання та збереження даних у хмарах.

Висновки. Результати проведеного аналізу дозволяють сформувати рекомендації для створення безпечних IoT-систем, що сприятиме захисту користувачів, збереженню довіри до цифрових технологій у побутовій та промисловій сферах, а також зниженню ризику масштабних кібератак

Список літератури

1. Statista. Internet of Things (IoT) connected devices installed base worldwide from 2019 to 2030. Statista. URL – https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide (дата звернення: 05.10.2025)

2. Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead // Computer Networks. – 2015. – № 76. – P. 146–164

3. Пєвнєв В. Я. Моделі загроз і забезпеченння цілісності інформаціїї // Системи та технології – 2018. – №2 (56/1) –. С. 79- 94. DOI: https://doi.org/ 10.32836/2521-6643-2018.2-56.6

4. Roman R., Zhou J., Lopez J. On the features and challenges of security and privacy in distributed internet of things // Computer Networks. – 2013. – № 57. – P. 2266–2279

5. Conti M., Dehghantanha A., Franke K., Watson S. Internet of Things security and forensics: Challenges and opportunities // Future Generation Computer Systems. – 2018. – № 78. – P. 544–546

Відомості про автора

Єрофєєв Максим Дмитрович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.d.yerofieiev@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

ВЕБСЕРВІС ДЛЯ ОЦІНКИ СКЛАДНОСТІ ТА ГЕНЕРАЦІЇ ПАРОЛІВ

Загнібеда А.О.
Харківський національний економічний університет імені Семена Кузнеця, м. Харків, Україна
Науковий керівник: Міхєєв І.А.

Актуальність. У сучасному світі розвиток хакерських технологій, зокрема атаки грубої сили та аналіз витоків даних, значно підвищує ризик несанкціонованого доступу до облікових записів користувачів. Згідно зі звітом Digital Defense Report [1] Україна у 2021 році посіла друге місце у рейтингу країн, що найчастіше зазнавали хакерських атак. Вже у 2024 році було зафіксовано зростання кількості кібератак на 69,8% порівняно з 2023 роком [2-3]. Близько 60% атак спрямовані безпосередньо на паролі: фішинг, атаки методом підбору (brute force) та повторне використання паролів. Використання слабкого пароля підвищує ймовірність витоку даних до 80%. Аналіз існуючих сервісів оцінки (2ip.io, Password Monster, UIC, Security.org) та генерації (Хостинг Україна, 2ip.ua, LastPass, Password Generator Plus 3.0) виявив певні недоліки – відсутність можливості створювати кілька паролів одночасно чи функції приховування/відкриття символів. Це свідчить про доцільність комбінування таких інструментів, адже використання лише одного сервісу не забезпечує повної надійності [4].

Метою даної роботи є розробка багатофункціонального вебсервісу, що надає кількісну й якісну оцінку складності паролів та створює стійкі до зламу паролі, а також включає реалізацію у вигляді Web-API.

Область застосування інструменту є широкою для:

– кінцевих користувачів – підвищення кібергігієни та усвідомленості щодо надійності паролів;

– розробників програмного забезпечення – інтеграція перевірки та генерації у форми реєстрації/зміни паролів через Web-API;

– для фахівців з інформаційної безпеки – застосування у системах управління ідентифікацією (IAM) та моніторингу безпеки.

Основні положення. Користувач взаємодіє з вебсервісом через вебзастосунок і API. У вебзастосунку можна оцінити пароль або згенерувати новий, результати відображаються в HTML. Через API запити обробляються у форматі JSON. В основі вебсервісу покладено технології Python і Flask та реалізовано два алгоритми:

1. Оцінка складності паролів – розрахунок ентропії на основі теорії ймовірності, визначення рівня надійності, перевірка на скомпрометовані паролі, а також оцінка часу зламу.

2. Генерація паролів – створення криптостійких паролів із заданими параметрами: довжина, набори символів, виключення схожих або повторюваних символів.

Ключовим результатом є реалізація Web-API, що забезпечує інтеграцію з іншими системами безпеки. Методи /api/check_password та /api/generate_password дозволяють автоматизувати перевірку і генерацію у зовнішніх застосунках, системах IAM та моніторингу.

Висновки. Робота показала, що розроблений вебсервіс виступає універсальним інструментом, що поєднує оцінку складності та генерацію паролів у вигляді сайту та Web-API. Це підвищує рівень обізнаності користувачів у сфері кібербезпеки та надає гнучкі можливості для автоматизації захисту облікових записів.

Список літератури

1. Microsoft Digital Defense Report. Microsoft. URL – https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/FY21-Microsoft-Digital-Defense-Report.pdf (дата звернення: 01.11.2025)

2. В Україні за рік кількість кібератак зросла на 70%: найпоширеніші типи інцидентів і головні цілі хакерів. Forbes Ukraine. URL: https://forbes.ua/news/v-ukraini-za-rik-kilkist-kiberatak-zrosla-na-70-nayposhirenishi-tipi-intsidentiv-i-golovni-tsili-khakeriv-08012025-26137 (дата звернення: 03.11.2025)

3. Password statistics and trends. JumpCloud blog. URL: https://jumpcloud.com/blog/password-statistics-trends (дата звернення: 05.11.2025)

4. Загнібеда А.О. Безкоштовні сервіси для оцінки складності та генерації паролів. Тези, с. 40. URL: https://repository.hneu.edu.ua/bitstream/123456789/35624/3/foss-2025-theses.pdf (дата звернення: 05.11.2025)

Відомості про авторів

Загнібеда Анастасія Олександрівна, магістрантка кафедри кібербезпеки та інформаційних технологій, ХНЕУ ім. Семена Кузнеця, anastasiia.zagnibeda@gmail.com

Міхєєв Іван Андрійович, доцент кафедри кібербезпеки та інформаційних технологій, ХНЕУ ім. Семена Кузнеця, к.т.н., i.a.mikheev@gmail.com

Секція 1

МЕТОДИ ЗБОРУ ТА АГРЕГАЦІЇ ІНФОРМАЦІЇ ПРО КІБЕРЗАГРОЗИ З ВІДКРИТИХ ДЖЕРЕЛ

Заячковська І. С.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Узун Д. Д.

Актуальність. У сучасному цифровому світі кількість кібератак зростає експоненційно [1]. За даними аналітичних компаній, щороку фіксується мільйони нових кіберінцидентів, що загрожують як корпоративному сектору, так і критичній інфраструктурі держав [2]. Для ефективного протидії кіберзагрозам необхідно своєчасно виявляти та аналізувати інформацію про нові вразливості, методи атак та індикатори компрометації. Відкриті джерела інформації (OSINT – Open Source Intelligence) стали важливим інструментом для збору даних про кіберзагрози, оскільки значна частина інформації про інциденти, вразливості та тактики зловмисників публікується у відкритому доступі [3]. Однак, розпорошеність даних по різних джерелах та відсутність систематизованого підходу до їх збору ускладнює процес аналізу та прийняття рішень у сфері кібербезпеки.

Метою даної роботи є дослідження методів збору та агрегації інформації про кіберзагрози з відкритих джерел для підвищення ефективності систем кібербезпеки, а також розробка єдиної платформи для аналізу отриманих даних з метою оперативного виявлення нових загроз.
Відкриті джерела інформації про кіберзагрози включають: бази даних вразливостей (CVE, NVD), спеціалізовані платформи обміну інформацією про загрози (threat intelligence feeds), соціальні мережі, форуми хакерів, технічні блоги, репозиторії з аналізом шкідливого програмного забезпечення, та звіти про інциденти від компаній з кібербезпеки. Аналіз цих джерел дозволяє виявляти нові загрози на ранніх етапах та формувати проактивні стратегії захисту [4].

Основні положення. У роботі розглянуто основні категорії відкритих джерел інформації про кіберзагрози та методи їх моніторингу. Досліджено автоматизовані інструменти для збору даних, такі як веб-скрапінг, API-інтеграції з платформами threat intelligence, RSS-агрегатори безпекових новин. Проаналізовано формати обміну даними про кіберзагрози (STIX, TAXII, OpenIOC), які дозволяють стандартизувати процес агрегації

інформації. Розглянуто підходи до фільтрації та верифікації даних для зменшення кількості хибних спрацювань. Особлива увага приділена методам корреляції інформації з різних джерел для виявлення зв'язків між окремими індикаторами компрометації та формування цілісної картини кіберзагроз. Досліджено можливості використання машинного навчання для автоматичної класифікації та пріоритезації зібраних даних.

Висновки. Систематичний збір та агрегація інформації про кіберзагрози з відкритих джерел є критично важливим компонентом сучасних систем кібербезпеки. Використання OSINT-методів дозволяє організаціям отримувати актуальну інформацію про нові загрози з мінімальними фінансовими витратами. Однак, ефективність такого підходу залежить від правильного вибору джерел інформації, автоматизації процесів збору та обробки даних, а також наявності кваліфікованих фахівців, здатних аналізувати отримані дані. Інтеграція систем агрегації OSINT-даних з існуючими засобами захисту дозволяє значно підвищити рівень кібербезпеки та скоротити час реагування на інциденти.

Список літератури

1. CERT-UA минулого року опрацювала 4315 кіберінцидентів. Державна Служба Спеціального Зв'язку та Захисту Інформації. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (дата звернення: 03.11.2025)
2. Microsoft Digital Defense Report 2025. Microsoft. URL – https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025?msockid=3043950b234760192cb984bd274766c4 (дата звернення: 03.11.2025)
3. Ландє Д. В. OSINT у кібербезпеці: навч. пос. – Київ: ТОВ «Інжиніринг», 2024. – 522 с.
4. What Are Open Source Threat Intelligence Feeds? Threat Media. URL – https://threat.media/definition/what-are-open-source-threat-intelligence-feeds (дата звернення: 04.11.2025)

Відомості про авторів

Заячковська Ірина Сергіївна, магістрантка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.zaiachkovska@student.csn.khai.edu
Узун Дмитро Дмитрович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., d.uzun@csn.khai.edu

Section 1

METHODS OF DETECTING AND PREVENTING PERSONAL DATA LEAKAGE

Oleh Zuban
National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine
Language adviser: Olha Kudlai

Relevance. In the modern digital environment, the volume of personal data processing increases daily, which raises the risks of data leakage. Information leakage can lead to financial losses, violations of confidentiality, and legal liability [1]. Threats arise not only due to technical vulnerabilities of systems but also because of the human factor and social engineering [2]. These circumstances necessitate the implementation of effective methods for detecting and preventing data leakage.

Purpose. The purpose of the study is to identify modern methods for detecting personal data leakage and to develop a comprehensive approach to its prevention, taking into account both technical and organizational aspects of security.

Main points. Various technical tools are used to detect personal data leaks. These include network traffic monitoring systems that allow real-time tracking of suspicious or abnormal data flows, as well as access log analysis, which records attempts of unauthorized access or unusual user activity. In addition, intrusion detection systems (IDS), which automatically signal potential threats, and data loss prevention systems (DLP), which restrict the transmission or copying of confidential information, are widely used [3]. To enhance detection accuracy, it is rational to integrate User and Entity Behavior Analytics (UEBA) based on machine learning algorithms. By establishing baseline behavioral models, these systems identify anomalous deviations indicative of insider threats or zero-day attacks that static signature-based methods fail to recognize. Additionally, implementing content fingerprinting within DLP solutions ensures precise identification of sensitive data across structured and unstructured formats. Furthermore, to minimize the reaction time to incidents, it is advisable to implement Security Orchestration, Automation, and Response (SOAR) systems. These platforms allow for the automatic isolation of compromised nodes and the blocking of suspicious sessions based on data received from SIEM, thereby implementing the concept of adaptive security architecture.

Data leakage prevention is ensured through a number of organizational and technical measures. Among them are data encryption, which makes information

inaccessible to third parties even in the case of unauthorized access, multi-level authentication that strengthens user access control, and network segmentation, which limits potential leakage pathways. An essential component is regular staff training and raising awareness of risks and protection methods [3].

The synthesis of technical solutions with legal regulation, in particular compliance with the Law of Ukraine "On Personal Data Protection" [1], forms a comprehensive information security system that includes technological, organizational, and regulatory aspects [4].

Conclusions. The analysis of methods for detecting and preventing personal data leakage shows that effective protection is possible only through a comprehensive approach. The combination of technical measures, such as network traffic monitoring and IDS/DLP systems, with organizational mechanisms of access control and staff training significantly reduces the risk of unauthorized access, while integrated solutions incorporating machine learning algorithms enhance system resilience and ensure reliable data protection.

References

1. Law of Ukraine «On Personal Data Protection» dated 01.06.2010 No. 2297-VI. URL – https://zakon.rada.gov.ua/laws/show/2297-17 (date of access 27.10.2025)

2. S. Syarova, S. Toleva - Stoimenova, A. Kirkov, S. Petkov, and K. Traykov, «Data leakage prevention and detection in digital configurations: a survey», ETR, vol. 2, pp. 253–258, Jun. 2024, DOI: 10.17770/etr2024vol2.8045

3. Herrera Montano, I., García Aranda, J.J., Ramos Diaz, J. et al. Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat. Cluster Comput 25, 4289–4302 (2022). DOI: 10.1007/s10586-022-03668-2

4. A Literature Survey on Data Leak Detection and Prevention Methods, ResearchGate, 2023. URL – https://www.researchgate.net/publication/396512210_A_Literature_Survey_on_Data_Leak_Detection_And_Prevention_Methods (date of access 27.10.2025)

Author information

Oleh Zuban', student from the Department of Aircraft Production Technologies, National Aerospace University «Kharkiv Aviation Institute», o.k.zuban@student.khai.edu

Olha Kudlai, assistant from the Department of Foreign Languages, National Aerospace University «Kharkiv Aviation Institute», o.kudlai@khai.edu

Секція 1

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У ВЕБДОДАТКУ ДЛЯ АВТОМАТИЗАЦІЇ СКЛАДСЬКИХ ПРОЦЕСІВ ІЗ ВИКОРИСТАННЯМ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ДАНИХ

Іванов А.Г.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Стадник А.О.

Актуальність. У сучасних умовах цифровізації бізнес-процесів питання захисту інформації стає одним із ключових для будь-якого вебдодатку, особливо якщо він використовується у сфері складської логістики. Дані про запаси, переміщення товарів, замовлення чи роботу персоналу є критично важливими, і їхня компрометація може призвести до фінансових збитків, зупинки операцій або втрати конкурентних переваг підприємства. Більшість готових програмних рішень на ринку або мають високий поріг входу, або потребують складної та дорогої кастомізації, до того ж рівень їхнього захисту не завжди відповідає потребам конкретного бізнесу [1]. Саме тому питання створення вебдодатку з вбудованими сучасними механізмами безпеки набуває особливої актуальності. Крім того, підприємства дедалі частіше стикаються з кіберзагрозами, спрямованими на викрадення, зміну або блокування доступу до даних. В умовах зростання кількості атак на вебсервіси важливо не лише автоматизувати складські процеси, але й гарантувати надійність і безпечність довірених системі даних. Розробка власного рішення дозволяє інтегрувати засоби безпеки без необхідності значних фінансових вкладень, зберігаючи при цьому гнучкість і можливість подальшого розвитку системи.

Мета. Створення вебдодатку для автоматизації процесів управління складом, у якому з самого початку інтегровані сучасні механізми кіберзахисту.

Основні положення. Вебдодатки працюють за принципом взаємодії клієнтської та серверної частин, де браузер користувача надсилає запити до сервера, а той повертає відповідь у вигляді даних. У межах складського обліку це дає можливість у режимі реального часу переглядати статус замовлень, перевіряти розташування товару, переглядати історію руху та працювати зі складськими операціями незалежно від місця перебування користувача.

Разом із тим вебдодатки є потенційно вразливими до низки кіберзагроз, які можуть порушити їхню роботу або призвести до викрадення конфіденційних даних. Серед поширених атак виділяються ін'єкції в базу даних, спроби несанкціонованого доступу до облікових записів, перехоплення токенів авторизації, міжсайтові скриптові атаки, маніпуляції з даними або втручання у взаємодію між клієнтом і сервером [2].

У проєкті передбачається комплексний захист, що охоплює всі ключові аспекти роботи вебдодатку. Для аутентифікації буде використано механізм JSON Web Token, який забезпечує безпечну передачу інформації про сеанс користувача та запобігає його підміні. Паролі будуть зберігатися у зашифрованому вигляді з використанням алгоритму bcrypt, що гарантує їх стійкість до злому. Валідація всіх даних, отриманих від користувача, включатиме регулярні вирази, перевірку типів і обмеження довжини, що дозволить мінімізувати ризики ін'єкцій та XSS-атак. Додатково буде реалізовано розмежування прав доступу, журналювання дій персоналу та контроль коректності взаємодії з базою даних – усе це забезпечить високий рівень захисту інформації та стабільність роботи системи.

Висновки. Розробка вебдодатку для автоматизації складських процесів потребує особливої уваги до питань кібербезпеки, оскільки система працює з критично важливими даними підприємства. Використання сучасних механізмів захисту, таких як хешування паролів алгоритмом bcrypt, аутентифікація за допомогою JSON Web Token, ретельна валідація введених даних і контроль прав доступу, забезпечує стійкість системи до основних загроз, що притаманні вебсередовищу. Отже, інтеграція комплексних заходів безпеки є необхідною умовою створення надійного, ефективного та сучасного інструменту для управління складською логістикою.

Список літератури

1. WMS, The good, bad and the ugly. Reddit. URL – https://www.reddit.com/r/Warehousing/comments/1f7tp17/wms_the_good_bad_and_the_ugly (дата звертання: 06.11.2025)
2. OWASP Top 10 Web Application Security Risks. OWASP Foundation. URL – https://owasp.org/Top10 (дата звертання: 06.11.2025)

Відомості про авторів

Іванов Андрій Геннадійович, магістрант кафедри комп'ютерних систем і мереж, НАУ «ХАІ», a.g.ivanov@student.csn.khai.edu
Стадник Анастасія Олександрівна, доцент кафедри комп'ютерних систем і мереж, НАУ «ХАІ», к.т.н., a.stadnyk@csn.khai.edu

Секція 1

АНАЛІЗ ТЕНДЕНЦІЙ КІБЕРЗАГРОЗ НА ОСНОВІ OWASP TOP 10:2025 RC

Іовенко І. Є.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Узун Д. Д.

Актуальність. У сучасному цифровому світі веб-додатки стали основою бізнес-процесів більшості організацій, обробляючи критично важливі дані та забезпечуючи взаємодію з мільйонами користувачів по всьому світу. Випуск OWASP Top 10:2025 у листопаді 2025 року знаменує восьму ітерацію цього важливого документа і демонструє суттєві зміни у ландшафті загроз порівняно з версією 2021 року [1]. Аналіз цих змін є критично важливим для розробників, архітекторів безпеки та організацій, які прагнуть захистити свої цифрові активи. Особливої актуальності набувають нові категорії загроз, такі як «Software Supply Chain Failures» та «Mishandling of Exceptional Conditions», що відображають сучасні виклики, пов'язані зі складністю екосистем розробки програмного забезпечення та зростанням кількості атак на ланцюги постачання. Згідно з дослідженням, атаки на ланцюги постачання програмного забезпечення стали одним з найскладніших викликів сучасної кібербезпеки, оскільки вони використовують довіру між компонентами системи [2]. Розуміння цих змін дозволяє організаціям адаптувати свої стратегії безпеки та процеси розробки для ефективного протистояння новим загрозам.

Метою роботи є комплексний порівняльний аналіз змін між OWASP Top 10:2021 та OWASP Top 10:2025, виявлення ключових тенденцій у еволюції загроз веб-безпеки.

Основні положення. OWASP Top 10:2025 демонструє еволюцію від симптоматичного підходу до фокусування на першопричинах проблем безпеки. Кількість аналізованих CWE (Common Weakness Enumeration) зросла з приблизно 400 у 2021 році до 589 у 2025 році, що забезпечує більш комплексне охоплення потенційних вразливостей. Згідно з дослідженням ланцюгів постачання, сучасні системи вимагають захисту не лише окремих компонентів, але й усього ланцюга взаємодій між ними [3].

Із ключових методологічних змін можна відмітити збільшення масштабу аналізу на основі використання даних 2,8 мільйонів додатків. Додана інтеграція даних CVSS v2, v3 та v4 для оцінки експлуатованості та

впливу. При цьому збережено гібридного підходу, де є 8 категорій основних даних та 2 категорії з опитування спільноти.

A01: Broken Access Control залишається на першій позиції в обох версіях, A07: Authentication Failures зберігає 7-му позицію. A02: Security Misconfiguration піднялася з 5 на 2, A04: Cryptographic Failures опустилася з 2 на 4, A05: Injection впала з 3 на 5 місце. В 2025 році з'явилися нові категорії: A03: Software Supply Chain Failures – розширення категорії «Vulnerable and Outdated Components» (A06:2021), що охоплює всю екосистему залежностей, системи збірки та інфраструктуру розповсюдження; A10: Mishandling of Exceptional Conditions – повністю нова категорія, що включає 24 CWE, фокусується на неправильній обробці помилок, логічних помилках та інших сценаріях, пов'язаних з аномальними умовами. A08: Software or Data Integrity Failures – розширена версія «Insecure Deserialization», тепер фокусується на довірі та цілісності на нижчому рівні, ніж Software Supply Chain Failures. A09: Logging & Alerting Failures – оновлена назва (раніше Security Logging and Monitoring Failures) для підкреслення важливості оповіщень, а не тільки логування.

Висновки. Еволюція OWASP Top 10 від версії 2021 до 2025 року демонструє фундаментальні зміни у підходах до безпеки веб-додатків. Основний тренд – перехід від реактивного виявлення вразливостей до проактивного забезпечення безпеки на всіх етапах життєвого циклу розробки програмного забезпечення. Організації, які врахують ці зміни у своїх практиках розробки та безпеки, матимуть значно кращі позиції для захисту від сучасних кіберзагроз.

Список літератури

1. Introducing the OWASP Top 10:2025. OWASP Foundation. URL – https://owasp.org/Top10 (дата звернення: 10.11.2024)
2. Wang Z. Construction of Software Supply Chain Threat Portrait Based on Chain Perspective / Z. Wang, Y. Zhang, C. Li // Mathematics. – 2023. – Vol. 11, No. 23. – Art. 4856. DOI: 10.3390/math11234856
3. Cybersecurity in Supply Chain Systems: The Farm-to-Fork Use Case / H. C. Leligou, A. Lakka, P. A. Karkazis [et al.] // Electronics. – 2024. – Vol. 13, No. 1. – Art. 215. DOI: 10.3390/electronics13010215.

Відомості про авторів

Іовенко Іван Євгенович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.y.iovenko@student.khai.edu
Узун Дмитро Дмитрович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., d.uzun@csn.khai.edu

Секція 1

АНАЛІЗ ЕФЕКТИВНОСТІ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ВІД ФІШИНГОВИХ АТАК

Каджаров А.А.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Пєвнєв В.Я

Актуальність. Фішинг є одним із найпоширеніших кіберзагроз у світі, що активно розвивається завдяки використанню методів соціальної інженерії. Під фішингом розуміють кібератаку, в якій зловмисники, використовуючи фальшиві повідомлення або видаючи себе за інших, намагаються отримати доступ до конфіденційної інформаціїЗгідно зі звітом Anti-Phishing Working Group, лише у 2024 році зафіксовано понад 4,7 мільйона фішингових інцидентів [1]. Зловмисники дедалі частіше застосовують персоналізовані повідомлення, підроблені сайти та фейкові сервіси, що суттєво ускладнює процес виявлення атак. Це створює порушення конфіденційності та цілісності інформації, великі фінансові та репутаційні ризики як для організацій, так і для окремих користувачів [2].

Мета роботи є дослідження сучасних методів протидії фішинговим атакам, оцінка їхньої ефективності та можливостей застосування у реальних умовах.

Основні положення. У доповіді розглядаються основні методи, за допомогою яких проводяться фішингові атаки. Найбільш поширені методи – це помилкова довіра, маніпулювання емоціями, потреба дії та підступне спілкування.

Найпоширеніші типи фішингових атак це фішинг в електронних листах, смішинг (фишинг в SMS) і вішинг (фішинг за допомогою телефона).

Серед ключових підходів до протидії фішинговим атакам розглядаються:

– антифішингові фільтри поштових сервісів і браузерів (Google Safe Browsing, Microsoft Defender SmartScreen);

– багатофакторна автентифікація як бар’єр для зловмисників;

– алгоритми машинного навчання, що здійснюють класифікацію електронних листів та вебсторінок. Окремий акцент зроблено на аналізі архітектури гібридних систем виявлення, що поєднують сигнатурний пошук із поведінковою аналітикою на базі глибокого навчання (Deep Learning) та обробки природної мови (NLP). Це дозволяє ідентифікувати

складні атаки нульового дня (zero-day) та BEC-атаки (Business Email Compromise), які не містять шкідливого коду, а базуються виключно на лінгвістичних маніпуляціях;

– освітні програми з кібергігієни, спрямовані на підвищення обізнаності користувачів [2,3].

Для перевірки ефективності застосовуються:

– аналіз статистичних даних про фішингові інциденти;

– тестування існуючих систем захисту на реальних наборах даних;

– адаптація інтелектуальних алгоритмів машинного навчання під сучасні сценарії атак [4,5].

Висновки. Дослідження показує, що лише комплексне застосування технічних рішень (фільтрація, автентифікація, ML-моделі) у поєднанні з освітніми заходами для користувачів забезпечує стійкість до сучасних фішингових атак. Результати сприятимуть вдосконаленню методів захисту, мінімізації фінансових збитків та формуванню більш захищених цифрових екосистем.

Список літератури

1. Phishing Activity Trends Report 2024. Anti-Phishing Working Group. URL – https://apwg.org/trendsreports (дата звернення: 02.10.2025)

2. Пєвнєв В. Я. Моделі загроз і забезпеченння цілісності інформаціїї // Системи та технології – 2018. – №2 (56/1) –. С. 79- 94. DOI: https://doi.org/10.32836/2521-6643-2018.2-56.6

3. Khonji M., Iraqi Y., Jones S. A survey on phishing detection techniques // IEEE Communications Surveys & Tutorials. – 2013. – Vol. 15(4). – P. 2091–2121. DOI: https://doi.org/10.1109/SURV.2013.032213.00009

4. Abdelhamid N., Ayesh A., Thabtah F. Phishing detection based associative classification data mining // Expert Systems with Applications. – 2014. – Vol. 41(13). – P. 5948–5959. DOI: https://doi.org/10.1016/j.eswa.2014.03.019

5. Basit, A., Zafar, M., Liu, X. et al. A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommun Syst 76, P. 139–154 (2021). DOI: https://doi.org/10.1007/s11235-020-00733-2

Відомості про автора

Каджаров Анар Аріфович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.a.kadzharov@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

ВИКОРИСТАННЯ OSINT ТА ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

Карапетян А. С.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Узун Д. Д.

Актуальність. Сучасний розвиток цифрових технологій призводить до значного зростання кіберзагроз, що вимагає удосконалення методів їх виявлення та протидії. Одним із перспективних напрямів є поєднання Open-Source Intelligence (OSINT) – методів збору й аналізу інформації з відкритих джерел – з технологіями розпізнавання облич (Face Recognition) [1]. Ця інтеграція дозволяє не лише ідентифікувати суб'єктів за доступними цифровими слідами, але й покращує швидкість і точність аналітичних процесів. Водночас застосування біометричних технологій у межах OSINT ставить ряд етичних, правових та технічних викликів, що пов'язані з захистом персональних даних, ризиками несанкціонованого доступу та можливими зловживаннями.

Метою роботи є комплексний аналіз можливостей впровадження технологій розпізнавання облич у процеси OSINT для підвищення ефективності виявлення кіберзагроз, а також оцінка потенційних ризиків, пов'язаних із застосуванням біометричних даних у цифровій розвідці та кіберзахисті.

Основні положення. OSINT базується на зборі інформації з відкритих джерел: соцмереж, публічних баз, фото та відеоматеріалів. Технології розпізнавання облич (Face Recognition) розширюють можливості ідентифікації навіть за неповними чи низькоякісними зображеннями. Алгоритми OpenFace, FaceNet, Dlib мають високу точність і здатні обробляти великі обсяги даних, що робить їх корисними у кіберрозслідуваннях [2]. Технічна реалізація таких систем передбачає використання згорткових нейронних мереж (CNN) для екстракції унікальних векторних ознак (embeddings) та їх подальшої кластеризації. Це дозволяє виконувати автоматизовану перехресну кореляцію візуальних образів із текстовими масивами даних OSINT, будуючи деталізовані графи зв'язків між суб'єктами загроз та зменшуючи ймовірність помилок атрибуції інцидентів. Ці технології допомагають виявляти учасників фішингових атак, шахрайств, поширення шкідливого ПЗ та інших

кіберзлочинів [3]. Водночас використання біометрії викликає проблеми з приватністю – можливі деанонімізація, цифрове переслідування та зловживання. Для мінімізації ризиків необхідно дотримуватись норм GDPR і впроваджувати надійні механізми захисту біометричних даних [4]. Таким чином, інтеграція Face Recognition в OSINT вимагає технічного, правового та етичного контролю для безпечного й відповідального застосування [5].

Висновки. Поєднання OSINT і розпізнавання облич підвищує ефективність виявлення кіберзагроз, збільшуючи точність і швидкість ідентифікації. Водночас необхідно враховувати ризики для приватності та безпеки, впроваджуючи технічні, правові й організаційні заходи. Подальші дослідження мають зосередитись на стандартизації обробки біометричних даних і підвищенні кваліфікації кібербезпекових фахівців.

Список літератури

1. OpenFace: Open Source Face Recognition Project. Github. URL – https://cmusatyalab.github.io/openface (дата звернення: 14.11.2025)
2. Schroff F., Kalenichenko D., Philbin J. FaceNet: A Unified Embedding for Face Recognition. Google Research. URL: https://arxiv.org/abs/1503.03832 (дата звернення: 14.11.2025)
3. GDPR – General Data Protection Regulation. GDPR. URL – https://gdpr-info.eu (дата звернення: 14.11.2025)
4. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks – Denise Almeida, Konstantin Shmarko, Elizabeth Lomas. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC8320316/ (дата звернення: 14.11.2025)
5. Almeida D, Shmarko K, Lomas E. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI Ethics. 2022;2(3):377-387. DOI: 10.1007/s43681-021-00077-w

Відомості про авторів

Карапетян Арман Суренович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.s.karapetian@student.csn.khai.edu
Узун Дмитро Дмитрович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., d.uzun@csn.khai.edu

Section 1

RESEARCH ON METHODS FOR ANALYZING SMART CONTRACT VULNERABILITIES

Ruslan Karpenko
Dniprovsky State Technical University, Kamianske, Ukraine
Scientific adviser: Kateryna Yalova

Relevance. A smart contract is a piece of computer code deployed on a blockchain network that automatically controls, executes, and enforces the terms of an agreement between parties [1]. Smart contracts operate according to an «if-then» logic, ensuring that contractual actions are performed only when predefined conditions are met, without the need to trust a centralized intermediary. The rapid expansion of Web3 technologies has generated a strong demand for secure, scalable, and efficient contracts, making smart contract security one of the critical challenges in the Web3 ecosystem.

The purpose of the study is the development of a software toolkit and the experimental detection of vulnerabilities in smart contracts written in Solidity, combining static analysis, dynamic testing, and a hybrid approach utilizing machine learning methods. Within the scope of the research, it is planned to:

– implement a Python-based software toolkit for the automatic loading, analysis, and generation of security reports for smart contracts;

– employ and compare the effectiveness of static analysis tools, dynamic testing frameworks, and machine learning models trained on publicly available datasets;

– evaluate the accuracy, rate of false positives, and practical utility of these methods for identifying common vulnerabilities.

Principal provisions. Smart contracts can be exposed to a range of critical vulnerabilities, which may lead to financial losses, functionality disruption, or unauthorized access [1]. Smart contract vulnerabilities can be categorized by attack type and technical error as follows:

– interaction and transaction sequencing vulnerabilities, arising from the dynamic interplay between contracts and the order of transaction execution, including reentrancy, unchecked external calls, phishing, and short address attacks;

– data handling and arithmetic vulnerabilities, resulting from errors in the internal logic of numeric operations and interactions with external data, such as integer overflow/underflow, timestamp dependency, randomness vulnerability, and uninitialized storage pointers;

– business logic and authorization vulnerabilities, associated with incorrect implementation of contract logic or access control mechanisms, including access control issues, logic flaws, and misuse of self-destruct functionality;

– blockchain environment interaction vulnerabilities, related to protocol or network-level weaknesses, including denial of service, gas limit/out-of-gas issues, front-running, and replay attacks.

There are several primary approaches and methods for the software-based analysis of smart contract vulnerabilities, which are conventionally categorized as static, dynamic, and hybrid models [2]. Static analysis involves examining the source code or bytecode without executing the contract. Its main advantage lies in the ability to apply it rapidly prior to deployment; however, it may produce false positives. Dynamic analysis comprises methods that assess the behavior of smart contracts during execution in a controlled testing environment, enabling the detection of errors and vulnerabilities that manifest only at runtime. Implementing dynamic analysis requires substantial time and computational resources to perform a large number of tests. The hybrid approach combines machine learning with static or dynamic analysis, leveraging both methods' strengths, but requires large datasets for training and testing.

Conclusions. The development of a software toolkit for assessing smart contract vulnerabilities, which integrates static analysis, dynamic testing, and hybrid machine learning models, will provide broader coverage of potential vulnerabilities and enable more effective detection of both technical and logical flaws in contracts, even before their deployment on the blockchain, where they become immutable.

List of references

1. Luliano G., Nucci D. Smart contact vulnerabilities, tools, and benchmarks: an updated systematic literature review. URL – https://arxiv.org/abs/2412.01719 (access date: 10.11.2025)

2. Liao X. Smart contact vulnerability detection based on dynamic and static combination: Proceedings of the International Conference on Digital Economy, Blockchain and Artificial Intelligence, 23–25 august 2024, Guangzhou, China, 2024. – PP. 412–416

Information about the authors

Ruslan Karpenko, a master`s student from the Department of Systems Software, Dniprovsky State Technical University, ru_karpenko@gmail.com

Kateryna Yalova, Head of the Department of the Systems Software, Dniprovsky State Technical University, Candidate of Technical Sciences, associate professor, yalovakateryna@gmail.com

Секція 1

ЦІЛІСНІСТЬ ДАНИХ СУПУТНИКОВОГО МОНІТОРИНГУ ЯК ФУНДАМЕНТ ОЦІНКИ ЗАСМІЧЕННЯ ПЛАСТИКОМ У СИСТЕМІ АЕРОКОСМІЧНОГО МОНІТОРИНГУ ОКЕАНІВ

Кифорук Ю. М.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Андрєєв С. М

Актуальність. Забруднення океанів пластиковими відходами досягло рівня глобальної екологічної кризи, що потребує постійного й високоточного моніторингу. Основним інструментом для цього стали аерокосмічні системи спостереження, зокрема супутники Sentinel-1/2/3, які дозволяють оцінювати площі забруднення, формувати спектральні карти накопичення пластикових відходів та аналізувати їх динаміку [1]. Однак ефективність таких систем безпосередньо залежить від цілісності даних дистанційного зондування.

Мета. Метою дослідження є аналіз впливу порушення цілісності супутникових даних на достовірність оцінки пластикового забруднення океанів, визначення основних кібернетичних загроз для аерокосмічних екологічних систем та розроблення заходів для підвищення надійності моніторингу у рамках екосистеми Copernicus.

Основні положення. Система аерокосмічного моніторингу забруднення океанів включає космічний сегмент (Sentinel-1 – SAR, Sentinel-2 – MSI, Sentinel-3 – IR), наземні центри приймання та обробки, аналітичні кластери машинного навчання та картографічні геопортали. Будь-яке порушення цілісності на одному з рівнів веде до помилкового формування карт забруднення та хибних оцінок площ пластикових акваторій. Загрози цілісності супутникових даних. До основних загроз належать MITM-атаки на канали передачі, підміна спектральних каналів, втручання у SAR-дані через радіочастотне придушення, порушення алгоритмів атмосферної корекції, компрометація моделей ML-класифікації та викривлення геоприв'язки. Такі втручання можуть зменшити виявлені площі скопичення пластику у 2–5 разів або створити хибні артефакти забруднення. Вплив порушення цілісності на екологічну аналітику [2,3]. Спотворення первинних даних призводить до: невірного визначення меж пластикових плям;плутання пластику з водоростями, піною або дрейфуючим органічним матеріалом; некоректних розрахунків індексів Floating Debris Index та інших спектральних показників; хибних прогнозів дрейфу пластикових масивів; викривлення оцінок робочої ефективності

систем очищення океану. Для захисту супутникових даних застосовуються криптографічне хешування (SHA-256/512), цифрові підписи, блокчейн-фіксація історії обробки знімків, багатосенсорна валідація, аудит та контроль ML-моделей, а також перевірка атмосферних і геометричних корекцій [4]. Геопортали, що використовуються для відображення пластикових забруднень, повинні перевіряти цифрові підписи та контрольні суми даних при імпорті картографічних шарів [5]. Це дозволяє уникнути підміни KMZ/KML-файлів та забезпечує достовірність інформації, доступної для науковців та управлінських структур.

Висновки. Цілісність даних супутникового моніторингу є критично важливою для точного визначення масштабу та характеру пластикового забруднення океанів. Порушення цілісності призводить до суттєвих помилок у картографічних моделях, неправдивих наукових висновків та неефективного планування міжнародних екологічних програм. Комплексне застосування криптографічних, кіберзахисних та аналітичних методів є необхідною умовою стабільної та надійної роботи аерокосмічної екологічної інфраструктури.

Список літератури

1. ESA Sentinel Technical Guides. Copernicus. URL – https://sentinels.copernicus.eu (дата звернення: 15.11.2025)
2. Kaandorp M. L. A. Global mass of buoyant marine plastics Nature eoscience, 2023.
3. Eriksen M. et al. A growing plastic smog. PLOS One, 2023.
4. Pevnev, V., Frolov, A., Tsuranov, M., Zemlianko, H. (2022). Ensuring the Data Integrity in Infocommunication Systems. International Journal of Computing, 21(2), P. 228-233. DOI: https://doi.org/10.47839/ijc.21.2.2591
5. Кифорук Ю.М. Створення аерокосмічного моніторингу забруднення океанів та морів виходами пластика // Дніпровська орбіта – 2025: матеріали XX наукових читань (22-24 жовтня 2025 р.) / Нац. центр аерокосмічної освіти молоді ім. О.М. Макарова, ДП “Конструкторське бюро “Південне” ім. М.К. Янгеля” Нац. музей космонавтики ім. С.П. Корольова, Дніпровський нац. ун-т ім. О. Гончара.– Дніпро, 2025.– С. 213-214.

Відомості про авторів

Кифорук Юрій Миколайович, студент кафедри геоінформаційних технологій та космічного моніторингу Землі, НАУ «ХАІ», y.m.kyforuk@student.khai.edu

Андрєєв Сергій Михайлович, доцент кафедри геоінформаційних технологій та космічного моніторингу Землі, НАУ «ХАІ», к.т.н., s.andreev@khai.edu

Section 1

APPLICATION OF MACHINE LEARNING TECHNOLOGIES FOR PREDICTIVE CYBER PROTECTION IN SMART HOME SYSTEMS

Danylo Kirichenko
University of Duisburg-Essen, Duisburg, Germany
Scientific adviser: Heorhii Zemlianko

Relevance. The proliferation of intelligent housing systems and integrated Internet of Things (IoT) devices has significantly expanded the domestic digital landscape. However, this increased connectivity introduces a complex and often vulnerable attack surface [1]. Smart home subsystems-controlling critical functions like access, climate, and surveillance – are frequently targeted by cyberattacks. Traditional security measures are often insufficient for the heterogeneous and resource-constrained nature of IoT devices, a challenge systematically reviewed in recent studies [2]. This highlights the urgent need for a shift from reactive to proactive, predictive defense mechanisms. Machine learning (ML) presents a robust approach for analyzing complex network traffic and device behavior to identify and preempt threats [3].

The purpose of this work is to analyze the methods of applying machine learning for the predictive identification and prevention of cyberattacks on smart home subsystems.

Principal provisions. The research begins with a systematic analysis of existing threats for IoT subsystems in smart homes [1, 2]. Subsequently, the work provides a comparative analysis of machine learning algorithms suitable for anomaly detection. This includes: Neural Networks (NN) (for modeling complex, non-linear patterns), Decision Trees (DT) (for generating interpretable rules), and Support Vector Machines (SVM) (for high-accuracy classification). A review of current literature shows these algorithms are foundational to modern IoT intrusion detection systems [2, 4]. Consideration is being given to hybrid and collective approaches to enhance the resistance of anomaly detectors to noise and drift propagation. Emphasis on the preliminary processing of telemetry data: normalization, selection of time intervals, choice of statistical and frequency functions, evaluation of trade-offs between accuracy, response time and memory/energy consumption. Based on this analysis, the work is dedicated to building a conceptual model for an intelligent predictive cyber defense system. This system is designed to predict potential cyberattacks by analyzing network traffic and device behavior patterns. The concept explores both supervised (trained on labeled attack datasets) and unsupervised (detecting novel deviations

from established normal behavior) learning methods. Finally, the paper discusses the practical challenges and strategies for the integration of this model into existing smart home architectures, focusing on lightweight and robust frameworks [3]. Proposed multi-level architecture «collection - forecast - response», to recognize known attacks and identify new anomalies. Mechanisms of adaptive training and calibration in drift and seasonal changes, taking into account confidentiality and data integrity.

Conclusions. The study concludes that machine learning technologies provide a powerful and necessary framework for advancing smart home cybersecurity from a reactive to a predictive posture. The proposed conceptual model, which leverages behavioral analysis, demonstrates a viable path for foreseeing and mitigating potential cyberattacks. The paper concludes by offering specific recommendations for further improvement and integration. These recommendations focus on model optimization for resource-constrained IoT devices and pathways for continuous model adaptation to counter the evolving threat landscape.

List of references

1. Kirichenko D. Cybersecurity of smart homes. Abstracts of reports from the "Student Conference on Information, Functional, and Cyber Security": IV Scientific and Practical Conference "Student Conference on Information, Functional, and Cyber Security of SCIFiC," Kharkiv, Nov. 29–Oct. 30, 2024. Kharkiv, 2024. P. 48. DOI: https://doi.org/10.13140/RG.2.2.14272.75521

2. Yogendra Kumar, Vijay Kumar, "A Systematic Review on Intrusion Detection System in Wireless Networks: Variants, Attacks, and Applications", *ACM Computing Surveys*, vol. 133, p. 395–452, Dec. 2023. DOI: https://doi.org/10.1007/s11277-023-10773-x

3. M. Bagaa, T. Taleb, J. B. Bernabe and A. Skarmeta, "A Machine Learning Security Framework for Iot Systems", in *IEEE Access*, vol. 8, pp. 114066-114077, 2020, DOI: 10.1109/ACCESS.2020.2996214

4. M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security", in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646-1685, thirdquarter 2020, DOI: 10.1109/COMST.2020.2988293

Information about the authors

Danylo Kirichenko, a master`s student from the Department of General Computer Science, danylo.kirichenko@stud.uni-due.de

Heorhii Zemlianko, associate professor from the Department of Computer Systems, Networks and Cybersecurity, NAU «KhAI», PhD in Cybersecurity, g.zemlynko@csn.khai.edu

Секція 1

КІБЕРЗАГРОЗИ ФІЗИЧНИМ СЕНСОРАМ ТА ЇХ ЗОВНІШНІМ ІНТЕРФЕЙСАМ

Коваленко Г. О.
Дніпровський фаховий коледж радіоелектроніки, м. Дніпро, Україна
Науковий керівник: Кифорук Ю. М.

Актуальність. Кіберфізичні системи (КФС), що містять розгалужені сенсорні мережі, є ключовими елементами у транспортних, аерокосмічних, енергетичних, медичних та промислових комплексах. Сенсори забезпечують перетворення фізичних величин у цифрові дані, однак їх безпосередній контакт із навколишнім середовищем створює значні ризики кібервтручання. Уразливості виникають через можливість впливу на фізичні параметри, підміну сигналів, створення штучних перешкод, порушення калібрування та атаки на інтерфейси I²C, SPI, CAN, UART, Ethernet [1]. З огляду на критичну роль сенсорних даних у прийнятті рішень КФС, компрометація цих компонентів створює потенційну небезпеку аварій, збоїв керування та порушення цілісності інфраструктури.

Мета. Метою роботи є визначення основних кіберзагроз фізичним сенсорам, аналіз методів їх реалізації та дослідження підходів до захисту, що охоплюють механізми забезпечення цілісності сенсорних даних [2].

Основні положення. Кіберзагроза сенсору – це навмисний або ненавмисний вплив на фізичні чи інформаційні канали, який призводить до некоректного сприйняття даних у КФС. У доповіді розглянуто сенсорні атаки фальшивими сигналами, атаки на цифрові інтерфейси (I²C, SPI, CAN, UART), компрометація калібрування та енергетичні атаки (Power Fault Injection) [1,3].

У доповіді надані приклади таких атак як акустичні атаки на MEMS-гіроскопи, атаки на датчики тиску й температури у SCADA-системах, електромагнітні атаки на GPS-модулі: дозволяють непомітно змінювати координати без фізичного втручання, дезорієнтуючи транспортні й навігаційні системи [3].

Методи захисту. Захист сенсорних систем включає поєднання фізичних, апаратних та програмних підходів: екранування та фільтрація сигналів для усунення паразитних впливів; криптографічний захист інтерфейсів та протоколів обміну; використання апаратних маркерів автентичності (PUF) для ідентифікації сенсорів; інкапсуляція сенсорів у захисні модулі; сенсорна надмірність, що забезпечує перехресну перевірку даних між

кількома незалежними каналами; алгоритми виявлення аномалій, засновані на статистичних моделях, прогнозуванні поведінки сенсора, машинному навчанні та крос-перевірці потоків даних. Захист аналого-цифрового тракту потребує: протидії атакам насичення через архітектуру Zero Trust на Edge-вузлах із застосуванням апаратних коренів довіри для автентифікації сенсорів, що виключає атаки через ланцюги постачання та підміну пристроїв. Сучасні КФС дедалі частіше застосовують інтелектуальні сенсорні вузли з механізмами оцінки довіри до даних (trust flag), що підвищує їхню стійкість до складних комбінованих атак [1,4].

Висновки. Фізична або інформаційна компрометація сенсорів є однією з найнебезпечніших загроз для кіберфізичних систем, оскільки викривлення первинних даних порушує їх коректне функціонування на всіх рівнях. Ефективний захист потребує комплексного підходу, який включає фізичну безпеку, криптографічні методи, перевірку автентичності, контроль цілісності даних, використання інтелектуальних алгоритмів виявлення аномалій та регулярну самодіагностику. Подальші дослідження мають бути спрямовані на створення адаптивних систем моніторингу стану сенсорних мереж із застосуванням методів штучного інтелекту.*ƒ*

Список літератури

1. Zhao L., et al. Sensor Attack Taxonomy and Defense Mechanisms in Cyber–Physical Systems. IEEE Internet of Things Journal, 2023
2. Petit J., Shladover S.E. Potential Cyberattacks on Automated Vehicles. IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 2, 2015
3. Checkoway S., et al. Comprehensive Experimental Analyses of Automotive Attack Surfaces. USENIX Security Symposium, 2011
4. Кифорук Ю.М Створення аерокосмічного моніторингу забруднення океанів та морів виходами пластика // Дніпровська орбіта – 2025: матеріали XX наукових читань (22-24 жовтня 2025 р.) / Нац. центр аерокосмічної освіти молоді ім. О.М. Макарова, ДП “Конструкторське бюро “Південне” ім. М.К. Янгеля” Нац. музей космонавтики ім. С.П. Корольова, Дніпровський нац. ун-т ім. О. Гончара.– Дніпро, 2025.– С. 213-214

Відомості про авторів

Коваленко Георгій Олександрович, учень-член гуртка “МЕХАТРОНІКА_ДФКР” Дніпровського фахового коледжу радіоелектроніки, georg.arduino.g@gmail.com
Кифорук Юрій Миколайович, керівник гуртка «МЕХАТРОНІКА_ДФКР», Дніпровського фахового коледжу радіоелектроніки, kiforuk.yury@gmail.com

Section 1

GITLESS OPS AS A METHOD FOR INFRASTRUCTURE DEPLOYMENT

Bohdan Kosarevskyi
National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine
Scientific advisor: Artem Tetskyi

Relevance. The contemporary landscape of cloud-native infrastructure is marked by growing complexity, stricter regulation and the rapid expansion of distributed edge environments. Traditional provisioning methods increasingly struggle to ensure consistency, auditability and security at scale. Git Operations (GitOps) emerged to address these challenges by enforcing a declarative, version-controlled single source of truth [1]. However, its dependence on Git repositories creates limitations in large-scale, multi-zone or highly regulated deployments. GitLess Ops has therefore been proposed as a variant in which Open Container Initiative (OCI) compliant artifact registries replace Git as the authoritative source of truth. This model is especially relevant for hybrid infrastructures, edge/cloud orchestration and autonomous deployment frameworks where latency, heterogeneity and supply-chain security are critical.

Purpose. The primary purpose of this study is to articulate the conceptual and operational foundations of GitLess Ops, contextualise its role within modern infrastructure deployment workflows, and propose its adoption as a method for enabling secure, scalable, declarative infrastructure at the edge and in cloud environments. Specifically, it seeks to clarify the motivation for replacing Git with OCI-artifact registries as the core single source of truth, enumerate the key provisions of the GitLess Ops model and draw conclusions regarding its implications for academic research and operational deployment practices.

Main provisions. First, GitLess Ops retains the four central design tenets of GitOps - declarative configuration, version-controlled state, automated pull-based reconciliation, and continuous drift correction - but relocates the authoritative source from Git repositories to OCI-compliant artifact registries [2]. Second, it emphasises artifact-centric delivery, where manifests, container images, SBOMs, signatures and other deployment artefacts are pushed to OCI registries, enabling provenance tracking, vulnerability scanning, and regional replication directly from the registry. Third, GitLess Ops alleviates operational constraints associated with Git-server access, especially in edge or air-gapped scenarios, by permitting infrastructure nodes to reconcile from locally replicated OCI artifacts rather than relying on live Git communications. Fourth, this

approach enhances supply-chain security: signed OCI artifacts and registry-level cryptographic controls replace Git commit history as the principal audit trail. Fifth, from a methodological perspective, GitLess Ops is particularly suited to research and deployment of hybrid MEC–Cloud infrastructures, where the decoupling of configuration dissemination from a central Git host allows nodes to operate with greater autonomy, lower latency and higher resilience. This architecture employs SHA256-referenced configurations to enable immutable infrastructure, ensuring deterministic deployments and eliminating the consistency issues of distributed Git repositories.

Conclusions. In sum, GitLess Ops represents a substantive evolution of the GitOps paradigm by relocating the authoritative infrastructure artefact store from Git to OCI registries, improving scalability, security and operational efficiency. For academic research, it enables new directions in declarative infrastructure at scale, edge–cloud orchestration and autonomous deployment [3]. Operationally, it offers clear benefits in distributed and regulated environments through manifest replication, cryptographic provenance and Git-less reconciliation. At the same time, it raises questions about pipeline design, artifact consistency across registries, and the measurement of latency or drift in closed-loop reconciliation. Overall, GitLess Ops should be viewed as a timely and methodologically grounded deployment model for hybrid, high-velocity systems, meriting further empirical validation.

List of references

1. An Introduction to GitOps. RedHat. URL – https://www.redhat.com/en/blog/an-introduction-to-gitops (date of access: 26.10.2025)
2. FluxCD Core Concepts. Fluxcd. URL – https://fluxcd.io/flux/concepts (date of access: 26.10.2025)
3. Performance Evaluation of Intent-Based Networking Scenarios: A GitOps and Nephio Approach. URL – https://arxiv.org/abs/2509.13901 (date of access: 26.10.2025).

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

Section 1

THREAT MODEL AND ATTACK SURFACE: GITOPS VS GITLESS OPS

Bohdan Kosarevskyi
National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine
Scientific advisor: Artem Tetskyi

Relevance. Escalating supply-chain attacks and rapidly distributed deployments enlarge the operational attack surface. National Institute of Standards and Technology (NIST) urges integrating Software Supply Chain (SSC) security directly into Continuous Integration (CI) or Continuous Delivery pipelines "to protect the integrity" of build-deploy stages [1]. The Cloud Native Computing Foundation (CNCF) Security Whitepaper underscores the rising impact of supply-chain compromises and recommends end-to-end verifiable practices [2]. European Union Agency's for Cybersecurity (ENISA) latest Threat Landscape highlights persistent intrusion activity "with ransomware at its core" [3]. In this context, GitLess Ops - a registry-centric variant of GitOps - is considered as a model in which trust and exposure shift from Git servers to Open Container Initiative (OCI) artifact registries.

Purpose. The objective is to formalize a comparative threat model for GitOps (Git as source of truth) versus GitLess Ops (OCI registry as source of truth), quantify attack surface across key data flows (Development→CI, CI→Source of Truth (SoT), SoT→Controller, ImagePull), and derive security design guidelines grounded in established supply-chain frameworks (e.g., SLSA). Supply-chain Levels for Software Artifacts (SLSA) provides a cross-industry specification intended to "prevent tampering, improve integrity" through provenance levels.

Main provisions. The threat model incorporates protected assets (manifests, images, attestations, controller credentials) and adversarial capabilities (man-in-the-middle attacks, token theft, registry/repository modification, dependency poisoning). NIST highlights Software Bill of Materials (SBOM) and attestation as foundational elements of SSC assurance. In GitOps, typical risks include commit-history tampering, pull-request bypass, token leakage, and Git server outages.

In a GitLess Ops model, transferring the source of truth to an OCI registry reduces reliance on Git availability and branch protection, while simultaneously introducing registry-specific risks such as mutable tags, signature stripping, and robot-account compromise. CNCF guidance stresses storing and verifying SBOMs and attestations directly within OCI-compliant artifact repositories.

The attack surface is represented through a flow-exposure function $E(f) = \sum w_v(1 - m_v)$ and overall $AS = \sum a_f E(f)$, where m_v reflects control effectiveness (e.g., signed commits vs. signature-verified OCI provenance), w_v - severity weight of a vulnerability, a_f - exposure weight of a data flow. GitLess Ops reduces attack vectors through VCS-production decoupling and cryptographically verified OCI artifacts.

Conclusions. The comparison indicates a reallocation of risk rather than its elimination: GitLess Ops mitigates Git-centric vectors (history rewrite, Git service compromise) while increasing the importance of image immutability, signature enforcement and narrowly scoped registry credentials. NIST and CNCF guidance consistently emphasize attestation-driven verification and policy-as-code controls, which align with registry-centric reconciliation. As a result, GitLess Ops can be regarded as a security-oriented alternative when combined with SLSA-style provenance and OCI-native verification, particularly in distributed environments where reducing blast radius and ensuring artifact integrity are critical.

List of references

1. Strategies for the Integration of Software Supply Chain Security in DevSecOps CI/CD Pipelines. NIST. URL – https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-204D.pdf (date of access: 26.10.2025)
2. Software supply chain best practices V2. CNCF. URL – https://tag-security.cncf.io/community/working-groups/supply-chain-security/supply-chain-security-paper-v2/Software_Supply_Chain_Practices_whitepaper_v2.pdf (date of access: 26.10.2025)
3. ENISA THREAT LANDSCAPE 2025. Enisa. URL – https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025_0.pdf (date of access: 26.10.2025)

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

Секція 1

ЗАСОБИ БЕЗПЕЧНОГО АДМІНІСТРУВАННЯ ВЕБ-САЙТІВ

Краснов В. О.
Харківський національний університет внутрішніх справ, м. Харків, Україна
Науковий керівник: Цуранов М. В.

Актуальність Сучасні веб-сайти є складними системами, навіть веб-додатками, у роботі яких приймають участь компоненти які працюють за технологією клієнт-сервер. На серверах працюють наступні підсистеми: бази даних, файлові сховища, сервіси обробки інформації, адміністрування компонентів. Разом із тим зростає кількість загроз, що безпосередньо впливають на безпеку кожного з компонентів веб-сайтів.

Мета. Метою роботи є дослідження основних проблем безпеки при адмініструванні веб-сайтів.

Основні положення Функціонування веб-сайту, як правило, відбувається цілодобово, тому існують деякі вимоги надійності до серверу та сервісів. Налагодження роботи всіх цих елементів потребує кваліфікованого адміністрування. Для виконання своєї роботи, адміністратор має отримати особливі привілеї в системі, які мають були доступні лише йому. Адміністратор може використовувати стандартні паролі, чи занадто прості, що може давати змогу зловмиснику виконати атаку на підсистему адміністрування[1]. При віддаленому адмініструванні особливо важливо розуміти як передається інформація, якщо вона відсилається в нешифрованому вигляді, то отримати пароль адміністратора становиться дуже легко. Це дозволяє зловмисникам у разі зламу здійснювати зміни у конфігураціях, редагувати або видаляти інформацію на сервері, елементи веб-додатку становляться уразливими. Адміністрування може відбуватися через веб-протоколи, що означає пересилання інформації. Якщо інформація пересилається через HTTP без SSL або при помилках у SSL-сертифікаті (само підписаний) існує ризик перехоплення запитів та зловмисник може переглядати або змінювати інформацію, що передається у відкритому вигляді [2]. Якщо SSL-сертифікат недійсний або його параметри налаштовані з помилками, система адміністрування, попереджає адміністратора про небезпечне з'єднання. Веб-сайт який приймає інформацію на вхід та обробляє її, може страждати від SQL-ін'єкцій та XSS-атак [3], коли вразливі поля введення дозволяють вставити неправомірний SQL чи JavaScript-код. Саме тому потрібен моніторинг для всіх можливих ситуацій із введення інформації, в

поля вводу даних, записування її в журнал, аби точно знати як веде себе система [4]. Якщо ж присутнє передавання конфіденційних даних через відкриті або неправильно налаштовані канали зв'язку, атаки типу MiTM [5] дозволяють зловмиснику змінювати передані пакети, що призводить до псування або підміни інформації.

Висновки. Проблеми які можуть створюватись при роботі веб-сайту, можливі при ситуаціях, коли важливу інформацію, про наявні шляхи доступу до інформації, яку не мають знати звичайні користувачі, було розкрито чи дані користувача з привілеями були скомпрометовані. Пересилання інформації між адміністратором та об'єктом адміністрування має бути захищеним від читання, зміни чи руйнації. Таким чином для захисту слід використовувати шифрування через протокол HTTPS. Використання шифрованого середовища захищає інформацію всіх в системі надсилання до веб-сайту, особливо адміністратора, інформація про якого може містити дані автентифікації.

Список літератури

1. Top 200 Most Common Passwords. Nordpass. URL – https://nordpass.com/most-common-passwords-list (дата звернення: 23.10.2025).

2. Різниця між HTTP та HTTPs. Hostiq. URL: https://hostiq.ua/wiki/ukr/http-https (дата звернення: 23.10.2025)

3. Васильченко Д. І., Лавровський І. М. Огляд типових уразливостей Web-сайтів організацій у 2019-2020 році. СУЧАСНИЙ ЗАХИСТ ІНФОРМАЦІЇ. 2021. С. 41–43. ISSN 2409-7292. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2503/2404 (дата звернення: 23.10.2025)

4. ІНФОРМАЦІЙНА БЕЗПЕКА В КОМП'ЮТЕРНИХ МЕРЕЖАХ / Смірнов О.А. та ін. Кропивницький, 2020. 225–226 с.

5. Enkli Ylli, Dr. Julian Fejzaj. Man in the Middle: Attack and Protection. Recent Trends and Applications in Computer Science and Information Technology, University of Tirana, Albania, 21–22 трав. 2021. 2021. С. 198–204.

Відомості про авторів

Краснов Владислав Олександрович, магістрант кафедри кібербезпеки та DATA-технологій ННІ № 5 Харківського національного університету внутрішніх справ, womisvlad@gmail.com

Цуранов Михайло Віталійович, ст. викладач кафедри кібербезпеки та DATA-технологій ННІ № 5 Харківського національного університету внутрішніх справ, ukrear2006@gmail.com

Секція 1

ДОСЛІДЖЕННЯ МЕХАНІЗМІВ ЗАХИСТУ ВЕБ-СЕРВЕРІВ

Ланько Д.О.
Харківський Національний Університет Внутрішніх Справ, м. Харків, Україна
Науковий керівник: Цуранов М. В.

Актуальність. В нинішній час розвитку інформаційних технологій веб-сервери є одними з головних елементів інфраструктури мережі Інтернет. Вони забезпечують доступ до веб-ресурсів, веб-сайтів, баз даних та хмарних ресурсів.

Сьогодні веб-сайти використовуються практично всіма типами організацій від державних установ і навчальних закладів до великих комерційних компаній. Для багатьох бізнесів веб-сайт є основою їхньої діяльності, оскільки через нього здійснюється продаж товарів, надання послуг, клієнтська підтримка та взаємодія з користувачами. Отже, стабільність та безпека веб-сервера безпосередньо впливають на безперебійну роботу підприємства, його репутацію та фінансові показники. Водночас вони можуть стати головною ціллю для кіберзлочинців. Прикладом може стати витік персональних даних через вразливість веб-додатку Equifax у 2017 році [1]. У липні хакери скористувалися невиправленою вразливістю Apache Struts, що призвело до викрадення даних близько 143 млн користувачів – пін-коди, дати народження, адреси та інше. Цей випадок привів до суттєвої зниження репутації та фінансових трат компанії.

Метою даної роботи є комплексний аналіз сучасних механізмів захисту веб-серверів з подальшим обґрунтуванням ефективності їх застосування для протидії кіберзагрозам.

Основні положення. Для своєчасного запобігання кібератакам доцільно застосовувати автомазивоних механізмів котрі налаштують захист веб-серверу та підвищують рівень безпеки та знижують можливість людського фактору.

Важливою частиною системи безпеки є використання вбудованих модулів захисту веб-серверів, які забезпечують багаторівневу оборону. Зокрема: ModSecurity – модуль веб-аплікаційного брандмауера (WAF) для Apache, Nginx та IIS, котрий дає можливість фільтрувати HTTP-запити, виявляти шкідливу активність (SQL-ін’єкції, XSS, brute force) та блокувати атаки ще до їх виконання. Залишається актуальним і підтримуваним у 2025

році, регулярно оновлюється відповідно до стандартів OWASP Core Rule Set [2].

Ще один модуль безпеки веб-серверів- mod_evasive — засіб котрий виявляє та завчасно блокує підозрілі активності, зокрема DDoS-атак. Він автоматично блокує IP-адреси які генерують велику кількість запитів[3]. У сучасних умовах цей модуль залишається потрібним і ефективним для початкового рівня захисту, хоча потребує поєднання з мережевими засобами (CDN, Cloudflare тощо. Зважаючи на це, одним із головних напрямів розвитку є розробка концепту модуля котрий буде збирати інформацію з бази даних, аналізуватиме ризики та проведення оновлень системи захисту та цілодобовий моніторинг стану веб-серверу.

Висновки Аналіз існуючих механізмів захисту показав, що найбільш ефективними є модулі веб-аплікаційного брандмауера (ModSecurity), засоби блокування підозрілої активності (mod_evasive) та модулі шифрування трафіку (mod_ssl / ngx_http_ssl_module). Вони забезпечують багаторівневий захист і залишаються актуальними у 2025 році, хоча потребують правильного налаштування та періодичного оновлення.

Основні елементи системи захисту веб-серверів це брандмауери веб-додатків та аналітичні модулі, ці інструменти потребують ручного налаштування, що може призвести до значної кількості хибних спрацювань і змусить адміністраторів вимкнути вказані інструменти.

Список літератури

1. Витік даних Equifax у 2017 році. Stellar Cyber. URL: https://stellarcyber.ai/uk/mauris-interdum-tempor-tortor/ (дата звернення: 03.11.2025)
2. ModSecurity – веб-аплікаційний брандмауер. OWASP DevGuide. URL: https://devguide.owasp.org/en/09-operations/03-modsecurity/ (дата звернення: 03.11.2025)
3. Apache mod_evasive – модуль захисту від DDoS. PhoenixNAP. URL: https://phoenixnap.com/kb/apache-mod-evasive (дата звернення: 03.11.2025)

Відомості про авторів

Ланько Денис Олександрович, магістрант кафедри кібербезпеки та DATA-технологій ННІ № 5 Харківського національного університету внутрішніх справ, fantom1604@ukr.net

Цуранов Михайло Віталійович, ст. викладач кафедри кібербезпеки та DATA-технологій ННІ № 5 Харківського національного університету внутрішніх справ, ukrear2006@gmail.com

Секція 1

АНАЛІЗ СИСТЕМ АДАПТИВНОЇ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ У CRM-ПЛАТФОРМАХ

Лейковський О. Д.
Державний університет «Київський авіаційний інститут», м. Київ, Україна
Науковий керівник: Висоцька О. О.

Актуальність. Сучасні CRM-платформи (Salesforce, Microsoft Dynamics 365, HubSpot, Zoho, Oracle CX) обробляють великі обсяги конфіденційних клієнтських і корпоративних даних. Збільшення кількості кібератак, фішингових кампаній та викрадення облікових даних зумовлює необхідність застосування гнучких систем автентифікації. Традиційні моделі MFA часто не враховують контекст ризику, тоді як адаптивна багатофакторна автентифікація (Adaptive MFA) автоматично змінює рівень перевірки залежно від поведінкових і середовищних ознак користувача, що значно підвищує безпеку доступу до хмарних сервісів. Окрім зростання кількості атак, варто враховувати і підвищення складності самих загроз. Сучасні методи компрометації включають соціальну інженерію, крадіжку сеансових токенів, підміну пристроїв та автоматизовані атаки на механізми одноразових паролів. У таких умовах статичні підходи до перевірки автентичності користувача стають неефективними. Адаптивна багатофакторна автентифікація дозволяє враховувати контекст доступу, рівень ризику та попередню історію поведінки користувача, що забезпечує більш динамічний і точковий захист від вторгнень. Крім того, поява віддаленого формату роботи та активне використання CRM-сервісів у хмарному середовищі суттєво розширює поверхню потенційних атак. Компанії змушені впроваджувати механізми, які одночасно зберігають зручність для користувачів і підтримують високий рівень безпеки. Використання адаптивної автентифікації сприяє побудові балансованої системи доступу, де перевірка ризику відбувається автоматично, без надмірного навантаження на кінцевого користувача.

Метою роботи є аналіз підходів до впровадження адаптивної багатофакторної автентифікації у провідних CRM-платформах, визначення їхніх переваг та недоліків, а також формування рекомендацій щодо підвищення ефективності механізмів захисту користувацьких сесій.

Основні положення. У роботі досліджено системи адаптивної автентифікації п’яти CRM-платформ. Встановлено, що Salesforce та Microsoft Dynamics 365 реалізують контекстно-залежні політики, які враховують IP-адресу, геолокацію, пристрій та ризикові ознаки поведінки

користувача. HubSpot і Zoho застосовують базові механізми MFA без розвинених моделей ризику, а Oracle CX орієнтована на корпоративний рівень безпеки з підтримкою RBAC/ABAC та апаратних ключів FIDO2. Серед основних проблем – відсутність уніфікованих політик MFA, надмірні дозволи службових акаунтів, використання вразливих методів (SMS), а також недостатня інтеграція з аналітичними системами ризику. Запропоновано рекомендації щодо централізації політик доступу, автоматизації аудиту прав, впровадження поведінкових сигналів і безпарольних методів автентифікації відповідно до стандарту NIST SP 800-63B.

Висновки. Аналіз показав, що адаптивна багатофакторна автентифікація є ключовим елементом побудови безпечних CRM-систем. Найбільш ефективні рішення реалізовані у Salesforce та Microsoft Dynamics 365, однак навіть у них існують ризики, пов'язані з людським фактором і складністю конфігурацій. Упровадження автоматизованого управління доступами, безпарольних технологій та централізованого Risk Engine дозволить суттєво підвищити стійкість CRM-платформ до компрометації облікових записів.

Список літератури

1. Identity and Access Management. *Salesforce Documentation*. URL – https://help.salesforce.com/s/articleView.html (дата звернення 10.09.2025)
2. Conditional Access and Identity Protection. *Microsoft Learn*. URL – https://learn.microsoft.com/en-us/entra/identity/conditional-access (дата звернення 21.09.2025)
3. Authentication and Account Protection. *HubSpot Security Overview*. URL – https://fs.hubspotusercontent00.net/hubfs/742851 (дата звернення 22.09.2025)
4. Security Whitepaper. *Zoho Corporation*. URL – https://www.zoho.com/security.html (дата звернення 01.10.2025)
5. David Temoshok. Digital Identity Guidelines: Authentication and Lifecycle Management: NIST Special Publication 800-63B. Gaithersburg, MD : National Institute of Standards and Technology, 2017. DOI: https://doi.org/10.6028/NIST.SP.800-63B-4

Відомості про авторів

Лейковський Олег Дмитрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, Державний університет «Київський авіаційний інститут», 6867497@stud.kai.edu.ua

Висоцька Олена Олександрівна, викладач кафедри Кібербезпеки, Державний університет «Київський авіаційний інститут», к.т.н., доцент, olena.vysotska@npp.kai.edu.ua

Секція 1

АНАЛІЗ ІСНУЮЧИХ ПРОБЛЕМ ПОЯСНЕННОГО ШІ В КІБЕРБЗПЕЦІ

Лісних О. І.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Морозова О. І.

Актуальність. Широке застосування штучного інтелекту (ШІ) у сфері кібербезпеки робить його критично важливими для розроблення сучасних захисних рішень [1]. Однак, складність розуміння процесу прийняття рішення та вихідні дані моделі, є досить критичним для забезпечення безпеки [2]. Ця «чорна скринька» (black-box) природа ШІ моделей є серйозним недоліком, який знижує довіру користувачів та фахівців з безпеки до систем, особливо в умовах зростаючої складності кібератак [3]. Пояснювальний штучний інтелект (ХАІ) виник як ключова парадигма для вирішення цієї проблеми, дозволяючи операторам краще розуміти модель та мати більшу довіру до вихідних даних. Проте, застосування ХАІ у кібербезпеці має свої недоліки, оскільки воно не лише покращує захисні практики, але й потенційно відкриває систему для нових ворожих атак, оскільки пояснення можуть бути використані зловмисниками. Таким чином, дослідження та усунення проблем, властивих ХАІ в контексті кібербезпеки, є надзвичайно актуальним [1].

Метою роботи є проведення аналізу стану досліджень на перетині ХАІ та кібербезпеки, а також визначення та систематизація існуючих проблем, викликів та нерозв'язаних питань щодо застосування ХАІ моделей для захисних механізмів. Це включає аналіз вразливостей самих ХАІ моделей, проблем з даними та методологічних прогалин, що перешкоджають побудові прозорих і ефективних систем кібербезпеки.

Основні положення. В рамках роботи виділено та проаналізовано такі ключові проблеми ХАІ в кібербезпеці:

– вразливість до ворожих атак, що можуть скомпрометувати або маніпулювати генерованими поясненнями [1-3];

– наявні набори даних часто є застарілими, неактуальними незбалансованими, надлишковими, недостатньо великими, що негативно впливає на продуктивність та зрозумілість моделей [1];

– відсутність загальноприйнятої системи чи уніфікованого набору стандартних метрик для оцінки ефективності та якості пояснень, що ускладнює оцінювання методів XAI у кібербезпеці [4];

– проблема конфіденційності та етики, зокрема дискримінації, упередженості та недобросовісності у прийнятті рішень [5];

– компроміс між високою точністю, та потребою у прозорості та розуміння моделі [1].

Висновки. Пояснювальна модель ШІ може дуже сильно допомогти експертам, операторам та іншим зрозуміти модель та мати чітке уявлення про дії які призвели до такого результату. Однак існуючі рішення мають свої недоліки та переваги. Вирішення недоліків цього підходу є ключовим завданням на сьогоднішній день. Зокрема, подальшого наукового опрацювання вимагають методи верифікації робастності алгоритмів XAI проти атак отруєння та розробка адаптивних механізмів диференційованої прозорості, щоб приховувати критичні параметри моделі.

Список літератури

1. Explainable artificial intelligence for cybersecurity: a literature survey / F. Charmet et al. *Annals of telecommunications*. 2022. DOI: https://doi.org/10.1007/s12243-022-00926-7

2. Explainable artificial intelligence applications in cyber security: state-of-the-art in research / Z. Zhang et al. *IEEE access*. 2022. P. 1. DOI: https://doi.org/10.1109/access.2022.3204051

3. Explainable artificial intelligence in cybersecurity: a survey / N. Capuano et al. *IEEE access*. 2022. P. 1. DOI: https://doi.org/10.1109/access.2022.3204171

4. Kharchenko V., Fesenko H., Illiashenko O. Quality models for artificial intelligence systems: characteristic-based approach, development and application. *Sensors*. 2022. Vol. 22, no. 13. P. 4865. DOI: https://doi.org/10.3390/s22134865

5. Mohamed N. Current trends in AI and ML for cybersecurity: a state-of-the-art survey. *Cogent engineering*. 2023. Vol. 10, no. 2. DOI: https://doi.org/10.1080/23311916.2023.2272358 (date of access: 12.11.2025)

Відомості про авторів

Лісних Олександр Ігорович, аспірант 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

ТЕХНОЛОГІЇ ПРОТИДІЇ ПІРАТСТВУ В СИСТЕМІ ЦИФРОВОЇ ДИСТРИБУЦІЇ ВІДЕОІГОР STEAM

Літвінов А. А.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Бабешко Є. В.

Актуальність. Несанкціоноване використання та розповсюдження цифрового контенту є великою проблемою для всіх індустрій, яка суттєво впливає на прибутковість та подальший розвиток. Відеоігри з самого початку свого існування були жертвами піратства, але раніше це було у вигляді несанкціонованого копіювання фізичних носіїв: картриджів, дискет, дисків тощо. На даний момент більшість ігор поширюється онлайн, і найбільший дистриб'ютор відео ігор на персональних комп'ютерах - Steam [1], кожен день зустрічається зі спробами незаконного копіювання контенту зі своєї платформи. Саме тому вивчення його технологій протидії піратству є актуальним напрямом дослідження в сфері кібербезпеки.

Метою роботи є визначити та проаналізувати основні технології, які використовує платформа Steam для протидії піратству відеоігор, а також оцінити їх ефективність та обмеження.

Основні положення. У Steam використовується комплексний підхід до захисту відеоігор від піратства. Основним інструментом є DRM-оболонка Steam (Steam DRM wrapper), яка перевіряє наявність ліцензії та забезпечує запуск гри лише через офіційний клієнт Steam [2,3]. Вона не є абсолютним засобом протидії піратству, але ефективно запобігає простому копіюванню файлів гри на інші пристрої. Для додаткового контролю платформа надає Steamworks API [4], що дозволяє розробникам інтегрувати перевірку ліцензії безпосередньо у виконуваний код гри, а також використовує технологію CEG (Custom Executable Generation) – створення унікальних виконуваних файлів для кожного користувача, що ускладнює масове поширення зламаних копій. Крім технічних рішень, Steam рекомендує підвищувати цінність легальних копій за допомогою функцій Steamworks – досягнень, хмарних збережень, таблиць лідерів і майстерень, які недоступні на піратських версіях. Розробники можуть за бажанням комбінувати ці засоби зі сторонніми системами DRM, такими як Denuvo або StarForce. Попри те, що жоден із методів не гарантує повного захисту від злому, комплекс технологій Steam суттєво знижує привабливість

піратства, роблячи офіційну версію більш зручною та функціональною для користувача. Одним з головних прикладів обходу систем захисту Steam є використання внутрішнього додатку Spacewar, це спеціальний додаток для тестування функцій Steamworks API з AppID (480), який є відкритим в системі, це дозволяє запускати будь яку гру з цим ідентифікатором, імітуючи її легальний запуск [5]. Цим часто користуються піратські копії ігор, які завдяки цьому мають можливість використовувати функціонал Steamworks.

Висновки. Отже, технології протидії піратству, які застосовує Steam, демонструють ефективний баланс між захистом прав розробників і зручністю користувачів. Завдяки поєднанню власної DRM-системи, перевірки ліцензій через Steamworks API, індивідуальних виконуваних файлів CEG та інтеграції з онлайн-сервісами платформа створює середовище, у якому легальне використання стає вигідним і комфортнішим за піратство. Водночас, Steam не лише перешкоджає незаконному копіюванню, а й стимулює розвиток легального ринку відеоігор, підтримуючи розробників через широкий набір інструментів і можливостей. Таким чином, система захисту контенту Steam є зразком сучасного підходу до кібербезпеки в індустрії цифрової дистрибуції.

Список літератури

1. Steam is the ultimate destination for playing, discussing, and creating games. Steam. URL – https://store.steampowered.com (дата звернення 27.10.2025)
2. What is DRM (Digital Rights Management)? Why Should Businesses Implement DRM? OTTclouds. URL – https://www.ottclouds.com/what-is-drm-digital-right-management (дата звернення: 26.10.2025)
3. Steam DRM. SteamGames. URL – https://partner.steamgames.com/doc/features/drm (дата звернення: 26.10.2025)
4. Steamworks API Overview. Steam. URL – https://partner.steamgames.com/doc/sdk/api (дата звернення 26.10.2025)
5. Steamworks API Example Application (SpaceWar). Steam. URL – https://partner.steamgames.com/doc/sdk/api/example (дата звернення 07.11.2025)

Відомості про авторів

Літвінов Андрій Андрійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.a.litvinov@student.csn.khai.edu
Бабешко Євген Васильович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., e.babeshko@csn.khai.edu

Секція 1

АНАЛІЗ ЛАНДШАФТУ ЗАГРОЗ ІНТЕРНЕТУ РЕЧЕЙ: ВЕКТОРИ АТАК ТА СТРАТЕГІЇ ПРОТИДІЇ

Луговцов Д. В.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Тецький А. Г.

Актуальність. З поступовим зростанням кількості пристроїв Інтернету речей (IoT), які, за прогнозами Transforma Insights, перевищать 31 мільярд уже до 2030 [1], це в свою чергу суттєво розширює поверхню атаки для зловмисників. Виробники IoT-пристроїв часто надають пріоритет швидкості виходу на ринок та низькій вартості, нехтуючи базовими принципами кібербезпеки. Це призводить до того, що мільйони вразливих пристроїв, від домашніх камер до панелей керування промисловими підприємствами, стають легкою ціллю. Як наслідок, скомпрометовані IoT-пристрої використовуються для формування потужних ботнетів (наприклад, класичний Mirai [2] та його сучасні еволюції, як-от Aisuru [3], що працюють за моделлю "DDoS-як-послуга"), шпигунства та як точка входу для атак на корпоративні та домашні мережі.

Метою є дослідження та систематизація основних загроз безпеці екосистем Інтернету речей, аналіз ключових векторів атак та обґрунтування комплексної стратегії протидії на архітектурному та мережевому рівнях.

Основні положення. Для аналізу загроз доцільно розглядати трирівневу архітектуру IoT: рівень пристроїв, рівень мережі та рівень застосунків. Вразливості існують на кожному з цих рівнів. Найбільш критичними є слабкі, вгадувані або жорстко закодовані паролі, що є головною проблемою згідно з індустріальним стандартом OWASP IoT Top 10 [4]. Іншими поширеними проблемами є відсутність механізму безпечного оновлення прошивки, що робить пристрої вразливими назавжди, та використання незахищених мережевих протоколів для передачі даних. Критично важливим є впровадження криптографічних механізмів захисту, зокрема протоколу DTLS для безпеки транспортного рівня в ресурсоємних середовищах, а також використання асиметричного шифрування (ECC) для аутентифікації вузлів та захисту цілісності керуючого трафіку від атак типу MITM. Додатково, перспективним вектором захисту є впровадження архітектури нульової довіри (Zero Trust)

та інтеграція легковисних алгоритмів машинного навчання на рівні граничних обчислень (Edge Computing). Для своєчасного виявлення та запобігання несанкціонованому доступу (НСД) ключовим методом протидії є мережева сегментація – ізоляція всіх IoT-пристроїв в окрему віртуальну локальну мережу (VLAN) або гостьову Wi-Fi мережу. Цей підхід обмежує потенційну шкоду від скомпрометованого пристрою, не дозволяючи йому отримати доступ до критичних ресурсів основної мережі.

Висновки. Безпека IoT-пристроїв є комплексною проблемою, що вимагає уваги як з боку виробників, так і кінцевих користувачів. Більшість вразливостей виникає через нехтування базовими принципами безпеки на етапі проектування та конфігурації пристроїв. Хоча існують інструменти для сканування вразливостей, вони є лише реактивним заходом. Ефективний захист вимагає багаторівневого підходу, де центральну роль відіграє превентивна мережева ізоляція (сегментація) пристроїв та впровадження принципів "Security by Design" виробниками. Зменшити ризик НСД до чутливих об'єктів можливо лише за умови поєднання технічних засобів контролю та підвищення обізнаності користувачів щодо існуючих загроз.

Список літератури

1. IoT Forecast Highlights. Transforma Insights. URL – https://transformainsights.com/research/forecast/highlights (дата звернення: 11.09.2025)
2. Alsaidi, M. (2024). Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. MDPI Sensors. URL: https://www.mdpi.com/1424-8220/24/11/3571 (дата звернення: September 11.09.2025)
3. ASERT Threat Summary: Aisuru and Related TurboMirai Botnet DDoS Attack Mitigation and Suppression. Netscout – URL: https://www.netscout.com/blog/asert/asert-threat-summary-aisuru-and-related-turbomirai-botnet-ddos (дата звернення 09.10.2025)
4. OWASP Internet of Things Project. OWASP. URL – https://owasp.org/www-project-internet-of-things (дата звернення: 11.09.2025)

Відомості про авторів

Луговцов Денис Васильович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.v.luhovtsov@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

ШІ-КЕРОВАНЕ ПЕНТЕСТУВАННЯ: АНАЛІЗ СУЧАСНИХ РІШЕНЬ

Мєдвєдєв Б. Р.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Тецький А. Г.

Актуальність. Сучасна цифрова інфраструктура широко застосовує штучний інтелект, великі дані та автономні системи для автоматизації керування й обробки інформації. Водночас ці технології створюють новий спектр кіберзагроз: вони можуть бути об'єктами атак або джерелами вразливостей. Традиційні методи пентестування залишаються критичними, але інколи не відповідають темпам і складності нових загроз. Використання AI-технологій у пентестуванні відкриває перспективи автоматизації, підвищення точності й глибини аналізу, що посилює кібербезпеку організацій [1].

Мета. Метою дослідження є здійснення системного огляду існуючих рішень у сфері AI-керованого пентестування, аналіз їх сильних і слабких сторін, а також формулювання конкретних пропозицій щодо покращення таких систем із точки зору продуктивності, адаптивності та прозорості.

Основні положення. Проведено огляд ключових AI-пентестинг рішень:

1. PentestGPT – інструмент, що використовує великі мовні моделі (LLM) для автоматизації етапів пентестування: сканування, інтерпретація результатів, генерація команд [1].
2. QualySec – сервіс, що спеціалізується на AI/ML-пентестуванні, враховує специфіку AI-систем, наприклад, атаки на дані, моделі, прийняття рішень [2].
3. Огляд інструментів, наведений на ресурсі Passcurity, включає аналіз рішень Pentera, Darktrace Cyber AI Analyst, Qualys VMDR [3].

Виявлено такі слабкі місця: обмежена база знань і навчальних даних для AI-моделей; недостатня адаптивність до нових типів атак; низька прозорість рішень (відсутність explainable AI) [4]. Для подолання цих обмежень пропонується впровадити архітектуру RAG для динамічного оновлення даних з баз CVE та використати навчання з підкріпленням для оптимізації графів атак, що зменшить кількість помилок генерації та підвищить автономність системи.

Попередні результати порівняння показують, що використання AI-платформи PentestGPT дозволяє скоротити час аналізу сканування приблизно на 70-90 % у порівнянні з ручними підходами [1-5]. При цьому роль людини-експерта залишається ключовою у верифікації результатів [2].

Висновки. AI-кероване пентестування має значний потенціал для підвищення ефективності процесів оцінки кібербезпеки. Огляд існуючих рішень показав, що хоча інструменти активно розвиваються, існують суттєві обмеження, які можуть бути удосконалені. Подальші дослідження мають бути спрямовані на практичну реалізацію цих покращень і масштабування систем у реальних кіберекосистемах.

Список літератури

1. Deng G., Liu Y., Mayoral-Vilches V., Li Y., Xu Y., Zhang T. PentestGPT: Evaluating and Harnessing Large Language Models for Penetration Testing [Електронний ресурс] // USENIX Security ’24 Conference Proceedings. — 2024. URL: https://pentestgpt.ai (дата звернення: 10.11.2025)
2. AI-Based Application Penetration Testing and Its Importance. Qualysec Blog. URL – https://qualysec.com/ai-penetration-testing (дата звернення: 10.11.2025)
3. Exploring the Best AI-Based Penetration Testing Tools. Passcurity. URL – https://passcurity.com/exploring-the-best-ai-based-penetration-testing-tools/ (дата звернення: 10.11.2025)
4. Pratama D., Singh R., Mendez S. CIPHER: Cybersecurity Intelligent Penetration-Testing Helper for Ethical Researchers // Sensors. – 2024. – Vol. 24, No. 21. – 6878. DOI: 10.3390/s24216878
5. White M., Black E., Robinson K. Revolutionizing Penetration Testing: AI-Powered Automation for Enterprise Security [Електронний ресурс] // ResearchGate. – 2024. – URL: https://www.researchgate.net/publication/387043979_Revolutionizing_Penetration_Testing_AI-Powered_Automation_for_Enterprise_Security (дата звернення: 10.11.2025)

Відомості про авторів

Мєдвєдєв Богдан Русланович, аспірант кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», b.r.miedviediev@khai.edu
Тецький Артем Григорович, доцент кафедра комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.tetskiy@csn.khai.edu

Секція 1

НЕСАНКЦІОНОВАНЕ ОТРИМАННЯ ТА ЗАПОБІГАННЯ ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ НА КІНЦЕВІЙ ТОЧЦІ ТА В МУЛЬТИМЕДІЙНОМУ КОНТЕНТІ

Дейнеко Я. О.
Міцик І. В.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Тецький А. Г.

Актуальність. Загроза витоку даних багатовекторна: від кейлогерів до публікацій у мультимедіа [1,3,5]. Наявні DLP-системи обмежено обробляють компрометований ввід та медіафайли [2-4]. Актуальним є створення інтегрованих модулів для нейтралізації цих каналів та аналіз вразливостей сучасних засобів.

Метою є зменшення ризиків витоку/пошук конфіденційних даних шляхом розроблення та інтеграції двох спеціалізованих модулів: перший модуль реалізує алгоритм ідентифікації парольних(корисних) послідовностей у тексті, зібраному локальним кейлогером, на основі кількості інформації; другий – представляє засоби пошуку й маскування конфіденційної текстової інформації у відеофайлах, використання системи для зчитування паролів та текстового матеріалу.

Основні положення. Дослідження базується на узгодженій роботі двох інтегрованих модулів. Перший модуль виявляє потенційні парольні послідовності. Для цього формується статистика трисимвольних комбінацій на основі текстів і даних кейлогерів, що дозволяє оцінювати ймовірності символів у природній мові. Потім для 10-символьних сегментів тексту обчислюється кількість інформації: сегменти з показником нижче середнього вважаються нетиповими, а отже потенційно парольними. Це дає змогу автоматично виділяти лише важливі ділянки введеного тексту.

Другий модуль призначений для виявлення та маскування конфіденційних даних у відео з використанням OCR. Відео аналізується з кроком 2.5 секунди за допомогою багатопотокового EasyOCR. Розпізнаний текст фільтрується за ключовими словами («пароль», «ключ»), після чого евристика близькості визначає сусідні текстові блоки, що містять критичні значення. Виявлений текст автоматично замасковується в кадрі. Застосування ентропійного аналізу дозволяє динамічно адаптувати

порогові значення для ідентифікації аномалій, мінімізуючи помилки першого роду. Оптимізація OCR-алгоритмів забезпечує обробку відеоконтенту з прийнятною обчислювальною складністю.

Висновки. Результатом досліджень є обґрунтування та розробка програмних засобів захисту від витоку інформації. Перший модуль підвищує ефективність аналізу локально скомпрометованих даних, другий – проактивно захищає від витоків через мультимедіа. Їхня інтеграція формує надійніший контур DLP та базу знань про шляхи витоку. Подальші дослідження спрямовані на використання AI та LLM для зменшення ризиків, враховуючи AI-powered атаки.

Список літератури

1. Rajpoot V. S., Singh A. P. Biometric Authentication Techniques: A Study on Keystroke Dynamics. International Journal of Scientific Engineering and Applied Science (IJSEAS). 2016. Vol. 2, Issue 1. P. 215–218. URL: https://ijseas.com/volume2/v2i1/ijseas20160125.pdf (дата звернення: 10.11.2025)
2. Gartner, Inc. Market Guide for Data Loss Prevention. 2025. URL: https://www.paloaltonetworks.com/resources/research/gartner-2025-market-guide-data-loss-prevention (дата звернення: 10.11.2025)
3. Domnik, J., & Holland, A. (2024). On Data Leakage Prevention Maturity: Adapting the C2M2 Framework. Journal of Cybersecurity and Privacy, 4(2), 167-195. DOI: https://doi.org/10.3390/jcp4020009
4. Chang, R.-I., Yang, C., & Hsu, T.-W. (2025). An Automatic Sensitive Image Search System with Generative Artificial Intelligence to Identify Data Leaks on Internet. Electronics, 14(11), P. 2254. DOI: https://doi.org/10.3390/electronics14112254
5. Olena Veprytska, Vyacheslav Kharchenko, and Oleg Illiashenko. 2025. Cybersecurity and Artificial Intelligence: Triad-Based Analysis and Attacks Review. Cybern. Inf. Technol. Vol 25, 3. September 2025. P. 156–185. DOI: https://doi.org/10.2478/cait-2025-0028

Відомості про автора

Дейнеко Ян Олександрович студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.o.deineko@student.csn.khai.edu
Міцик Ілля Володимирович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.v.mitsyk@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

Section 1

ADVERSARIAL APPROACHES TO BOT EVASION AND DETECTION COUNTERMEASURES

Vladyslav Miachkov
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
Scientific adviser: Anatolii Pashko

Relevance. With the growing sophistication of automated bots in modern web environments, traditional detection systems face significant challenges in distinguishing malicious automated activity from legitimate user interactions. Recent advances in anti-detect technologies and adversarial machine learning (AML) enable «intelligent» bots to imitate human behavior, manipulate browser fingerprints, and evade advanced anti-bot mechanisms [1]. These evasive bots pose a serious threat to the cybersecurity of online platforms, financial systems, and e-commerce infrastructures, often being used for data scraping, fraudulent transactions, or large-scale misinformation campaigns [2]. The increasing adaptability of adversarially trained bots highlights the urgent need for resilient detection models capable of identifying and countering such attacks even under conditions of deliberate evasion.

The purpose of this work is to develop and analyze adversarial models of evasive bots and propose robust detection methods based on multi-modal analysis and machine learning techniques.

Principal provisions. The study explores the integration of several complementary directions aimed at strengthening the robustness of modern bot detection systems. It focuses on adversarial modeling of evasive bots [3], where simulated bot agents are trained using adversarial machine learning to replicate realistic evasion tactics observed in the wild. This allows the creation of controlled test environments for analyzing the vulnerabilities of existing detection mechanisms.

A multi-modal detection approach is then applied by combining diverse data sources – browser characteristics, network traces, and behavioral interaction patterns – using supervised and contrastive learning methods. Such integration improves generalization and allows the system to recognize subtle inconsistencies that may indicate automation.

Additionally, an evaluation framework is developed using Selenium-based environments and anti-detect browsers to systematically test the robustness of detection models under adversarial conditions. This framework enables

reproducible experiments on the effectiveness of various defense strategies against adaptive bot behaviors.

The proposed methodology employs Python (TensorFlow, PyTorch) for machine learning model development and C++/Rust for implementing high-performance simulation modules. Evaluation relies on both classical performance metrics (precision, recall, F1-score) and specialized robustness indicators such as evasion success rate, providing a comprehensive view of model reliability and resistance to adversarial manipulation

Conclusions. Adversarial simulation of bot behavior provides a powerful tool for assessing and improving the security of detection systems under realistic and evolving attack scenarios. The expected outcome of this research is a unified experimental framework for generating, testing, and mitigating adversarial bot activity. By combining adversarial modeling with multi-modal detection strategies, the proposed approach aims to enhance the resilience of machine learning–based systems used in web security, anti-fraud mechanisms, and cybersecurity monitoring infrastructures. In the long term, these findings may contribute to the development of more transparent, adaptive, and trustworthy AI-driven defenses against automated malicious agents in digital ecosystems.

List of references

1. S. Pelekis, T. Koutroubas, A. Blika, A. Berdelis, E. Karakolis, C. Ntanos, E . Spiliotis, and D. Askounis, "Adversarial machine learning: a review of methods, tools, and critical industry sectors," *Artificial Intelligence Review*, vol. 58, no. 8, p. 226, 2025. DOI: https://doi.org/10.1007/s10462-025-11147-4

2. H. Venugopalan, S. Munir, S. Ahmed, T. Wang, S. T. King, and Z. Shafiq, "FP-Inconsistent: Detecting Evasive Bots using Browser Fingerprint Inconsistencies," *arXiv preprint arXiv:2406.07647*, Jun. 2024. DOI: 10.48550/arXiv.2406.07647

3. S. Cresci and A. Petrocchi, "Better safe than sorry: An adversarial approach to improve social bot detection," in *Proceedings of the 11th ACM Conference on Web Science (WebSci'19)*, Boston, MA, US, June 30–July 3, 2019. DOI: 10.1145/3292522.3326030

Information about the authors

Vladyslav Miachkov, PhD student on Faculty of Computer Science and Cybernetics, Taras Shevchenko National University of Kyiv, fameowner99@gmail.com

Anatolii Pashko, professor on Faculty of Computer Science and Cybernetics, Taras Shevchenko National University of Kyiv, D. Sc., professor, aap2011@ukr.net

Секція 1

ДОСЛІДЖЕННЯ ТА РОЗРОБЛЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВНОЇ ОРГАНІЗАЦІЇ

Олефіренко І. С.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Пєвнєв В. Я.

Актуальність. З посиленням цифровізації державного сектору та перенесенням критичних даних у цифрові екосистеми зростає ризик кібератак і несанкціонованого доступу до конфіденційної інформації та порушення її цілісності. Державні установи зберігають персональні дані громадян, фінансові і стратегічні записи, що робить їх привабливими цілями для атак. У контексті чинної нормативно-технічної бази ТЗІ необхідне поєднання інженерних заходів захисту й управлінських практик для забезпечення захищеності інформації [1].

Мета роботи. Дослідження, проєктування і розробка комплексної системи інформаційної безпеки для державної організації, яка відповідає вимогам нормативно-технічної бази ТЗІ і враховує сучасні архітектурні підходи як рекомендований логічний рівень реалізації.

Основні положення. Основні вектори атак на державні установи включають фішинг і соціальну інженерію, експлуатацію вразливостей у веб-та мережевих сервісах, компрометацію облікових записів і lateral movement всередині мережі. Галузеві звіти підтверджують високу частку інцидентів, пов'язаних із використанням вразливостей та компрометацією облікових даних [2].

Основні положення запропонованої системи:

1. Усі проєктні рішення узгоджуються з вимогами НД ТЗІ, міжнародних і національних стандартів для забезпечення юридичної та інженерної обґрунтованості захисту.
2. Рекомендовано застосовувати принципи Zero Trust – постійну верифікацію користувачів і пристроїв, оцінку стану, мінімізацію привілеїв і сегментацію доступу – як архітектурний підхід, сумісний із технічними вимогами ТЗІ [3].
3. Monitoring & Response. Впровадження централізованого збору логів і кореляції подій (SIEM), IDS/IPS та процесів управління вразливостями для оперативного виявлення й реагування на інциденти; відпрацювання процедур інцидент-менеджменту

4. Інженерні комплекси ТЗІ. Проєктування й атестація комплексів ТЗІ, побудова захищених каналів передачі, захист периметра та застосування фізичних і радіотехнічних заходів згідно з НД ТЗІ.

5. Організаційні заходи. Політики доступу, багатофакторна автентифікація, регулярні навчання персоналу й тренування сценаріїв інцидентного реагування; управлінські практики формуються з урахуванням підходів ISMS (ISO/IEC 27001) [4].

6. Криптографічний захист та ешелонована оборона. Технічна архітектура передбачає обов'язкову інтеграцію засобів криптографічного захисту інформації (КЗІ) та інфраструктури відкритих ключів (PKI) для забезпечення наскрізного шифрування трафіку та контролю цілісності транзакцій.

Висновки. Опираючись на НД ТЗІ та національні стандарти можна забезпечити необхідну нормативну основу і конкретні інженерні вимоги для захисту державної інформації. Поєднання принципів Zero Trust і елементів ISO/IEC 27001 на логічному та управлінському рівнях підвищує адаптивність і стійкість системи. Запропонований підхід інтегрує нормативну відповідність, технічні засоби й управлінські процеси для створення керованої і захищеної системи інформаційної безпеки в державному секторі

Список літератури

1. Пєвнєв В. Я. Моделі загроз і забезпеченння цілісності інформаціїї // Системи та технології – 2018. – №2 (56/1) –. С. 79-94. DOI: https://doi.org/10.32836/2521-6643-2018.2-56.6

2. 2024 Data Breach Investigations Report (DBIR 2024). Verizon. URL – https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf (дата звернення: 10.10.2025)

3. Zero Trust Architecture. NIST Special Publication 800-207 / NIST. URL – https://csrc.nist.gov/pubs/sp/800/207/final (дата звернення: 10.10.2025)

4. Information Security Management Systems. ISO/IEC 27001:2022 / International Organization for Standardization (ISO). URL – https://www.iso.org/standard/27001 (дата звернення: 10.10.2025)

Відомості про авторів

Олефіренко Іван Сергійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.s.olefirenko@student.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

ДОСЛІДЖЕННЯ ТА ВПРОВАДЖЕННЯ ІНСТРУМЕНТАЛЬНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У КОНВЕЄР БЕЗПЕРЕРВНОЇ ІНТЕГРАЦІЇ

Перетятько Р. С.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Узун Д. Д.

Актуальність. Розвиток DevOps-підходу в процесі розробки та розгортання програмного забезпечення дозволив зробити життєвий цикл розробки ПЗ (SDLC) більш автоматизованим, однак рівень загроз інформаційній безпеці зріс. Безпека у конвеєрі безперервної інтеграції (CI) стала критичним аспектом SDLC, оскільки компрометація на будь-якому етапі може призвести до втрати даних або порушення цілісності коду [1]. Вразливості в репозиторіях, відкриті секретні дані (токени, API-ключі тощо) в CI-скриптах та недостатній контроль доступу до середовища виконання є типовими проблемами сучасних DevOps-систем [2]. Інтеграція безпеки на ранніх етапах (DevSecOps) дозволяє зменшити витрати на виправлення помилок та підвищити довіру до кінцевого продукту [3]. Особлива актуальність цього була набута через підвищення популярності застосування контейнеризації та мікросервісної архітектури, де кожен елемент має свій життєвий цикл, що може стати вектором атаки.

Метою роботи є дослідження та впровадження інструментальних засобів забезпечення безпеки у конвеєр безперервної інтеграції з урахуванням принципів DevSecOps, а також оцінка їх ефективності у виявленні та запобіганні загрозам на етапах розробки, тестування та впровадження.

Основні положення. Для автоматизації контролю безпеки використовуються інструменти, що інтегруються в CI/CD конвеєр. До таких інструментів можна віднести:

– Secret Scanning інструменти, які шукають витоки приватних даних в репозиторіях [5];

– SCA (Software Composition Analysis), задача яких це пошук у відкритому коді залежностей із вразливостями [4];

– SAST (Static Application Security Testing), які перевіряють вихідник код на наявність вразливостей до його впровадження;

– DAST (Dynamic Application Security Testing), які аналізують поведінку вже працюючого застосунку.

Крім зазначених методів, архітектура захищеного конвеєра вимагає реалізації політик Quality Gates, які блокують просування артефактів при виявленні критичних вразливостей (CVE) із високим рейтингом CVSS. Важливим етапом є впровадження Container Security для сканування образів контейнерів на наявність вразливостей у базових шарах ОС та бібліотеках, а також перевірка конфігураційних файлів для мінімізації ризиків неправильного налаштування хмарного середовища.

Висновки. Інтеграція засобів забезпечення безпеки у конвеєр безперервної інтеграції дозволяє виявляти вразливості та зменшує ймовірність компрометації систем, застосунків тощо. Впровадження підходу DevSecOps сприяє формуванню культури безпеки серед розробників і адміністраторів. Однак, ефективність таких систем залежить від правильного налаштування інструментів, актуальності баз вразливостей і постійного моніторингу середовища CI/CD.

Список літератури

1. Савчук В. О., Цуранов М. В. Аналіз засобів безпеки хмарних платформ [Analysis of cloud platform security tools]. У кн.: Проблеми інформатизації: тези доп. 8-ї міжнар. наук.-техн. конф., 26-27 листопада 2020 р., м. Черкаси, м. Харків, м. Баку, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Черк. держ. технолог. ун-т [та ін.]. – Харків : Петров В. В., 2020. – 83 с

2. OWASP DevSecOps Guidelines. OWASP Foundation. URL – https://owasp.org/www-project-devsecops-guideline (дата звернення: 17.10.2025)

3. GitLab 2024 – Global DevSecOps Report. Gitlab. URL – https://about.gitlab.com/developer-survey (дата звернення: 17.10.2025)

4. Trivy – Simple and Comprehensive Vulnerability Scanner. Aqua Security. URL – https://aquasecurity.github.io/trivy/ (дата звернення: 17.10.2025)

5. GitGuardian Documentation. GitGuardian. URL – https://docs.gitguardian.com (дата звернення: 17.10.2025)

Відомості про авторів

Перетятько Роман Сергійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», r.s.peretiatko@student.khai.edu

Узун Дмитро Дмитрович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., d.uzun@csn.khai.edu

Section 1

ANALYSIS OF CYBERATTACKS ON NETWORK CLOUD STORAGE SYSTEMS USING ARTIFICIAL INTELLIGENCE

Andriy Piskovy
National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine
Scientific adviser: Heorhii Zemlianko

Relevance. The rapid migration of corporate and private data to cloud storage (Amazon S3, Azure Blob Storage, Google Cloud Storage) makes it a priority target for attackers. Traditional, signature-based defenses are proving ineffective against a new generation of cyberattacks that use artificial intelligence (AI) algorithms to automate exploration, exploit vulnerabilities, and bypass detection systems. This is due to the fact that AI attacks can dynamically change their vector and mimic legitimate behavior, making signal analysis practically useless. According to industry reports, by 2025 more than 60% of successful attacks on cloud infrastructures will use AI technologies [1]. However, there is not enough attention paid to studying the specifics of AI-attacks aimed at network protocols and cloud storage APIs. This gap in the studies creates a critical vulnerability, leaving confidential data without adequate cover.

The purpose of this work is to study and classify the vectors of cyberattacks on cloud storage using AI, as well as to analyze the mechanisms for countering such threats. The main threat is the ability of AI algorithms to analyze large volumes of traffic to detect incorrectly configured access rights, classified as Security Misconfiguration [2], and carry out complex attacks such as distributed denial of service (DDoS) attacks at the application level or targeted phishing for account theft.

Outline. For the timely detection and analysis of AI-attacks, a hybrid approach combining behavioral analysis (UEBA) and machine learning (ML) is proposed. The use of UEBA allows to form a dynamic profile of «normal» activity for each user and entity, immediately recording deviations. ML, in turn, directly analyzes the network traffic and API logs in real time to detect non-signature anomalies [3].

Recursive neural networks (RNN) and their architecture - long short-term memory networks (LSTM) are considered as bases for ML-models of attack prediction. Due to the ability to analyze time sequences, these models are effective for detecting complex patterns in access logs. They are able to identify suspicious transactions, such as atypical bulk downloading, enumeration

(«bucket» or anomalous data encryption attempts that often precede ransomware attacks) [3,4].

The implementation of protective measures is based on existing technological platforms. Analyzed SIEM-systems of new generation and platforms XDR (Extended Detection and Response), integrated with cloud providers. Their key advantage is the ability to aggregate telemetry directly from cloud APIs and run automatic response (SOAR) scenarios - for example, instantly block an attacker's IP address or suspend the rights of a compromised account [5].

Conclusions. The use of artificial intelligence by attackers fundamentally changes the threat landscape for cloud storage. The existing safeguards require adaptation and implementation of proactive AI models for detection. One of the most elusive threats is the use of generative competitive networks (GAN) to create realistic but malicious requests for APIs that bypass standard filters. The theses consider the main vectors of attacks using AI and propose methods for their detection, which is the basis for building layered cyber-protection systems.

List of references

1. 2024 State of Cloud Native Security Report. Palo Alto Networks. URL – https://www.paloaltonetworks.com/resources/research/state-of-cloud-native-security-2024 (date of access: 23.10.2025)

2. OWASP top 10 for large language model applications OWASP foundation. URL – https://owasp.org/www-project-top-10-for-large-language-model-applications (date of access: 23.10.2025)

3. Cyberattacks and security of cloud computing: a complete guideline / M. Dawood et al. Symmetry. 2023. Vol. 15, no. 11. P. 1981. DOI: https://doi.org/10.3390/sym15111981 (date of access: 23.10.2025)

4. Security threat analysis in cloud computing / M. Iqbal Fadillah et al. JATI (jurnal mahasiswa teknik informatika). 2024. Vol. 9, no. 1. P. 992–998. DOI: https://doi.org/10.36040/jati.v9i1.12528 (date of access: 23.10.2025)

5. Ikeoluwa K. Advancing u.s. national security with cloud computing: strengthening intelligence, cyber resilience, and homeland defense strategies. International journal of engineering technology research & management (ijetrm). 2025. Vol. 09, no. 02. DOI: https://doi.org/10.5281/zenodo.14937982 (date of access: 23.10.2025)

Information about the authors

Andriy Piskovy, a master`s student from the Department of Computer Systems, Networks and Cybersecurity, NAU «KhAI», a.piskovyi@student.csn.khai.edu

Heorhii Zemlianko, associate professor from the Department of Computer Systems, Networks and Cybersecurity, NAU "KhAI", PhD in Cybersecurity g.zemlynko@csn.khai.edu

Секція 1

АНАЛІЗ ТА ПРОТИДІЯ ІНСАЙДЕРСЬКИМ ЗАГРОЗАМ В ОРГАНІЗАЦІЯХ: ОЦІНКА ЕФЕКТИВНОСТІ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ

Подлас Я.О.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Брежнєв Є. В.

Актуальність Інсайдерські загрози є одними з найнебезпечніших для корпоративної безпеки, оскільки походять від осіб, що мають легітимний доступ до систем. У звіті IBM зазначено, що понад 35% інцидентів інформаційної безпеки спричинені діями або помилками співробітників [1]. У контексті переходу на віддалену роботу та використання хмарних сервісів традиційне захистове моделювання втрачає ефективність. Це зумовлює потребу у впровадженні Zero Trust-архітектури, поведінкової аналітики та систем моніторингу ризиків, орієнтованих на користувача [2].

Мета дослідження оцінити ефективність сучасних методів виявлення та запобігання інсайдерським загрозам, а також сформувати мінімальний набір заходів, що забезпечують найбільше зниження ризиків: UEBA, політика найменших привілеїв, багатофакторна автентифікація, DLP-рішення та моніторинг інцидентів через SIEM/SOAR [3].

Основні положення. Сучасні підходи до протидії інсайдерським загрозам включають поведінкову аналітику (UEBA), політику найменших привілеїв, багатофакторну автентифікацію, контроль доступу до даних і централізований моніторинг інцидентів через SIEM/SOAR [2,4]. Додатково проведено оцінку ефективності цих методів. Згідно з даними досліджень, UEBA дозволяє знизити кількість внутрішніх інцидентів на 40-50% завдяки виявленню аномальної поведінки користувачів [2]. Zero Trust-архітектура зменшує ризики успішних внутрішніх атак на 30-60%, оскільки забезпечує постійний контроль доступу на основі принципу «не довіряй нікому» [1]. DLP-рішення скорочують втрати від витоків конфіденційної інформації в середньому на до 38%, а використання SIEM/SOAR підвищує швидкість реагування на інциденти у 4-7 разів, що значно зменшує масштаб потенційних порушень [3,5]. Порівняльний аналіз показав, що найбільшу ефективність забезпечує комбіноване застосування кількох технологій – UEBA + Zero Trust + DLP + SIEM, що дозволяє знизити рівень інсайдерських ризиків на 40-60 %. У дослідженні запропоновано узагальнену модель управління інсайдерськими ризиками, що поєднує

технічні (UEBA, DLP, Zero Trust) та організаційні (контроль доступу, аудит, навчання) заходи. Новизна полягає у поєднанні поведінкової аналітики з динамічним контролем доступу, який адаптується до рівня ризику користувача. Такий підхід дозволяє виявляти загрози на ранніх етапах і мінімізувати людський фактор [2,4]. Реалізація Zero Trust-архітектури у поєднанні з поведінковою аналітикою користувачів та DLP-рішеннями дає змогу суттєво підвищити рівень захисту від інсайдерських дій. Запропонований підхід дозволяє знизити кількість внутрішніх інцидентів на 40-60 % і скоротити фінансові втрати, пов'язані з розслідуванням інцидентів і ліквідацією наслідків витоку даних [3,5].

Висновки. Протидія інсайдерським загрозам вимагає комплексного підходу, що поєднує технологічні, організаційні та поведінкові механізми. Перехід від реактивної моделі реагування до проактивної, яка базується на постійному моніторингу поведінки користувачів і динамічному управлінні ризиками, є ключовим напрямом розвитку корпоративної безпеки. Впровадження принципів Zero Trust, поведінкової аналітики та систем контролю даних забезпечує створення стійкої до внутрішніх загроз інформаційної інфраструктури.

Список літератури

1. Insider Threats Report 2024. IBM Security. URL – https://www. ibm.com/ reports/insider-threats-2024 (дата звернення: 28.10.2025)
2. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture: NIST SP 800-207.NIST, 2020. URL: https://nvlpubs.nist.gov/ nistpubs/ specialpublications/NIST.SP.800-207.pdf (дата звернення: 28.10.2025)
3. The State of Zero Trust Adoption 2024. Forrester Research. URL – https://www.forrester.com/report/the-state-of-zero-trust-adoption-2024 (дата звернення: 28.10.2025)
4. Yousef R., Jazzar M. Measuring the Effectiveness of User and Entity Behavior Analytics for the Prevention of Insider Threats.Journal of Xi'an University of Architecture & Technology, 2021, Vol. XIII (10), pp. 175–181. DOI: 10.37896/JXAT13.10/313918
5. Cost of Insider Threats 2024 Report. Ponemon Institute. URL – https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats(дата звернення: 28.10.2025)

Відомості про авторів

Подлас Ярослав Олександрович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.o.podlas @student.csn.khai.edu
Брежнєв Євген Віталійович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., с.н.с., e.brezhnev@csn.khai.edu

Секція 1

АНАЛІЗ РИЗИКІВ БЕЗПЕКИ ІНФРАСТРУКТУРИ «РОЗУМНОГО МІСТА» В МЕРЕЖАХ 5G: ВРАЗЛИВОСТІ ТА АТАКИ НА СИСТЕМИ ШІ

Приходько Д. С.
Харківського національного університету внутрішніх справ, м. Харків, Україна
Науковий керівник: Землянко Г. А.

Актуальність. Інфраструктура «Розумного міста» (Smart City) будується на двох фундаментальних технологіях: мережах 5G, що забезпечують наднадійний зв'язок з низькою затримкою (URLLC) для трильйонів IoT-пристроїв, і системах штучного інтелекту (ШІ), що керують критичними процесами. Ця синергія, будучи основою функціонування, одночасно формує нову, складну поверхню атаки. Вразливості більше не обмежуються традиційним мережевим периметром, а зміщуються в бік архітектури 5G і логіки самих ШІ-моделей [1].

Метою даної роботи є аналіз загроз безпеки наступного покоління, спрямованих на ключові технології «Розумного міста». Дослідження фокусується на двох основних векторах: 1) вразливості архітектури 5G, зокрема, пов'язані з віртуалізацією мережевих функцій (NFV), і 2) атаки на моделі ШІ (Data Poisoning і Adversarial Attacks), що використовуються в критичних підсистемах, таких як управління трафіком і відеоспостереження.

Основні положення. Архітектура 5G, заснована на програмно-визначених мережах (SDN) і NFV, переносить функції безпеки з апаратного на програмний рівень. Це створює ризики «некоректної конфігурації» (OWASP A05:2021) у складних віртуалізованих середовищах [2]. Вразливості в NFV Management and Orchestration (MANO) або в механізмах «нарізки» мережі (Network Slicing) можуть дозволити зловмиснику ізолювати цілий сектор міста або провести DoS-атаку на критичну інфраструктуру, наприклад, на служби екстреного реагування.

На рівні ШІ-систем найбільшу загрозу становлять атаки, спрямовані на статистичну природу моделей. Атаки типу «отруєння даних» (Data Poisoning) націлені на етап навчання. Зловмисник, впроваджуючи шкідливі дані в датасет (наприклад, у загальнодоступні дані про трафік), може таємно порушити логіку роботи ШІ-моделі управління світлофорами, провокуючи колапс або створюючи «зелений коридор» для порушників [3].

Інший вектор – «змагальні атаки» (Adversarial Attacks) – застосовується на етапі експлуатації (inference). Шляхом внесення мінімальних, непомітних для людини спотворень у фізичні об'єкти (наприклад, спеціальні наклейки на знаках дорожнього руху) або в цифрові потоки (піксельні спотворення у відео з камер), зловмисник може дезорієнтувати ШІ. Це може призвести до некоректної роботи системи розпізнавання облич або, в критичному випадку, до помилкової ідентифікації об'єктів автономним транспортом [4].

Висновки. Безпека «Розумного міста» в епоху 5G та ШІ – це комплексна проблема, де атаки на ШІ-моделі стають настільки ж критичними, як і мережеві вторгнення. Однією з неочевидних загроз є комбінована атака: використання вразливості 5G (наприклад, в NFV) для отримання доступу до каналу даних, який використовується для «отруєння» навчальної вибірки ШІ-моделі. У роботі запропоновано методи верифікації рішень ШІ і проактивного захисту, включаючи «суперечливе навчання» (adversarial training) моделей, як необхідні компоненти для забезпечення відмовостійкості міської інфраструктури.

Список літератури

1. Pevnev, V., Plakhteev, A., Tsuranov, M., Zemlianko, H., & Leichenko, K. (2022). “Smart city” technology: Conception, security issues and cases. Integrated computer technologies in mechanical engineering - 2021 (s. 207–218). Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-94259-5_19

2. Pevnev, V., Tsuranov, M., Zemlianko, H., & Amelina, O. (2021). Conceptual model of information security. *Lecture notes in networks and systems* (s. 158–168). Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-66717-7_14

3. Pevnev, V., Frolov, A., Tsuranov, M., & Zemlianko, H. (2022). Ensuring the data integrity in infocommunication systems. International Journal of Computing, 228–233. DOI: https://doi.org/10.47839/ijc.21.2.2591

4. Simulated adversarial attacks on traffic sign recognition of autonomous vehicles / H. Lin et al. *Ieee ecice 2024*. Basel Switzerland, 2025. P. 15. DOI: https://doi.org/10.3390/engproc2025092015

Відомості про авторів

Приходько Дмитро Сергійович, магістрант кафедри кібербезпеки та DATA-технологій ННІ № 5 Харківського національного університету внутрішніх справ

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

Секція 1

МЕТОДИ І ЗАСОБИ ШІ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ МЕДИЧНИХ ВЕБ-СИСТЕМ

Рябко І. Б.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Харченко В. С.

Актуальність. Медичні веб-системи (EHR/EMR, PACS/DICOMweb, телемедицина, портали пацієнта) працюють з високочутливими клінічними даними та критичними інтеграціями. Погрози включають фішинг, компрометацію облікових записів, інсайдерську активність, ін'єкції у веб-додатках, DDoS і витоки. Регуляторні вимоги (HIPAA, ISO/IEC 27001) підсилюють обов'язковість конфіденційності, цілісності та відстежуваності [1-3]. Класичні засоби захисту часто не встигають за складністю ландшафту. ШІ/ML-підходи допомагають виявляти аномалії, корелювати події, знижувати MTTD/MTTR та пріоритизувати інциденти [4]. Водночас застосування ШІ вимагає правильної архітектури (Zero-Trust [5], сегментація, RBAC/SSO, XDR/SOAR) і дисципліни MLOps (версіонування, моніторинг дрифту, аудит) [4].

Метою аналіз архітектурних патернів та практик MLOps для безпечного впровадження ШІ/ML у медичних веб-системах, зокрема принципів Zero-Trust, сегментації, автоматизації реагування (XDR/SOAR), а також методів версіонування моделей, моніторингу дрифту та керованого розгортання.

Основні положення. Архітектурні патерни базуються на принципі Zero-Trust [5], який передбачає перевірку кожного запиту та відсутність неявної довіри. Мікросегментація мережі ізолює критичні компоненти (PACS, EMR, веб-сервери) та обмежує поширення компрометації. Рольова модель доступу (RBAC/SSO) забезпечує мінімальні привілеї та централізоване управління автентифікацією. Кореляція подій та автоматизація реагування через XDR/SOAR знижують MTTD/MTTR. Повне журналювання та відстежуваність є обов'язковими для аудиту та відповідності регуляторним вимогам (HIPAA, ISO/IEC 27001) [2,3].Практики MLOps включають версіонування даних, моделей та пакетів ознак для відстеження змін та відкату до стабільних версій. Документування моделей через «model cards» забезпечує прозорість щодо їх поведінки та обмежень. Моніторинг дрифту та справедливості моделей

виявляє деградацію якості та зміщення в даних. Керовані релізи з гейтінгом, відкатом та канарейковими розгортаннями мінімізують ризики при впровадженні нових моделей у продакшн [4]. Інтеграція з клінічними системами вимагає повного аудиту всіх дій з даними, збереження відповідності регуляторним вимогам та мінімізації ризиків для пацієнтських даних [3].

Висновки. Архітектурні патерни та практики MLOps є критичними для безпечного впровадження ШІ/ML у медичних веб-системах. Zero-Trust архітектура та дисципліна MLOps забезпечують необхідний рівень контролю, відстежуваності та відповідності регуляторним вимогам, що дозволяє ефективно використовувати переваги ШІ/ML при мінімізації ризиків для клінічних даних. Подальші дослідження планується розгортати за напрямами: розробка специфічних архітектурних рішень для інтеграції ШІ/ML у критичні медичні системи та вдосконалення методів моніторингу та автоматизації реагування на загрози.

Список літератури

1. Web Application Security Risks 10:2021. OWASP Foundation. URL – https://owasp.org/Top10 (дата звернення: 10.11.2025)
2. ISO/IEC 27001:2022 Information security management systems – Requirements. ISO. – 2022
3. NIST SP 800-66 Rev. 2 HIPAA Security Rule: A Cybersecurity Resource Guide. NIST. URL – https://csrc.nist.gov/publications/detail/sp/800-66/rev-2/final (дата звернення: 10.11.2024)
4. NIST AI Risk Management Framework (AI RMF 1.0). NIST. URL – https://www.nist.gov/itl/ai-risk-management-framework (дата звернення: 10.11.2024)
5. Zero Trust Architecture. NIST SP 800-207. NIST. URL – https://csrc.nist.gov/publications/detail/sp/800-207/final (дата звернення: 10.11.2025)

Відомості про авторів

Рябко Іван Богданович, аспірант 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

УПРАВЛІННЯ ДОСТУПОМ ТА РОЛЬОВІ МОДЕЛІ В СИСТЕМАХ МОНІТОРИНГУ ОКЕАНУ

Рябчун М. А.
Дніпровський науковий українсько-американський ліцей Дніпровської міської ради, м. Дніпро, Україна
Науковий керівник: Кифорук Ю. М.

Актуальність. Системи моніторингу океану генерують величезні обсяги критично важливих даних, що вимагають надійного захисту та контрольованого доступу [1]. Управління доступом є ключовим елементом забезпечення конфіденційності, цілісності та доступності цієї інформації, особливо в умовах спільного використання даних різними науковими та державними установами. Прозорість та відповідність міжнародним стандартам безпеки (ISO/IEC 27001, NIST 800-162) є обов'язковою умовою для інтеграції вітчизняних систем моніторингу океану у світову наукову інфраструктуру.

Мета. Мета дослідження полягає у розробці та аналізі ефективних рольових моделей управління доступом (Role-Based Access Control, RBAC) для забезпечення гнучкого та безпечного розподілу прав користувачів у складних, багатокомпонентних системах моніторингу океану.

Основні положення. Пропонована рольова модель ґрунтується на принципі найменших привілеїв, адаптованому для специфіки океанографічних даних (наприклад, доступ до сирих даних, оброблених даних, моделей прогнозування) [2]. Запровадження ієрархії ролей (наприклад, «оператор сенсорів», «аналітик даних», «адміністратор системи») дозволяє мінімізувати ризики несанкціонованого доступу та помилок [3]. Розмежування прав доступу між науковими, державними та комерційними структурами сприяє безпечному обміну даними та розвитку міжнародних ініціатив у сфері сталого океанографічного моніторингу.

Для підвищення гранулярності контролю доцільним є застосування гібридного підходу, що інтегрує елементи атрибутивного управління (ABAC). Це дозволяє динамічно змінювати політики безпеки в реальному часі, враховуючи контекстуальні атрибути: геолокацію запиту, час доступу та поточний стан загроз кібербезпеці. Для забезпечення інтероперабельності в гетерогенних середовищах пропонується імплементація федеративних протоколів ідентифікації (SAML, OIDC), що спрощує наскрізну автентифікацію користувачів з різних наукових

інституцій без компрометації периметру безпеки. Модель реалізована на мікросервісній архітектурі з окремим сервісом авторизації, що інтегрується через API Gateway. Захист телеметрії від атак типу Man-in-the-Middle забезпечується протоколом DTLS 1.3 з взаємною автентифікацією на рівні Edge Computing.

Розмежування прав доступу між науковими, державними та комерційними структурами сприяє безпечному обміну даними та розвитку міжнародних ініціатив у сфері сталого океанографічного моніторингу.

Висновки. Розроблені рольові моделі управління доступом (Role-Based Access Control, RBAC) значно підвищують безпеку даних у складних, багатокомпонентних системах моніторингу океану. Впроваджуючи ці моделі, що ґрунтуються на принципі найменших привілеїв, вдається ефективно мінімізувати ризики несанкціонованого доступу та помилок. Це забезпечується завдяки чіткій ієрархії ролей (наприклад, «оператор сенсорів», «аналітик даних») та адаптації моделі під специфіку океанографічних даних (сирі, оброблені, моделі прогнозування). Таким чином, забезпечується конфіденційність, цілісність та доступність величезних обсягів критично важливої інформації.

Список літератури

1. Lisitsky D., et al. The evolution of mapping: from geodata to geoinformation and geoknowledge // SGEM Conference Proceedings. – 2021

2. Geospatial knowledge infrastructure. Geospatial Media and Communications. URL – https://www.geospatialworld.net (дата звернення: 08.11.2025)

3. Arcuser. Supporting the science that saves the ocean // ArcUser Magazine. – ESRI, 2023

4. Kyforuk Yu. M., Petrosyan P. A., Kravchenko K. S., Puchenina M. R., Kondrachuk S. S., Andreev S. M. Creation of aerospace monitoring of pollution of oceans and seas by plastic emissions // Dnipro Orbit – 2025: materials of the XX scientific readings (October 22–24, 2025). – Dnipro, 2025. – С. 213–214

Відомості про авторів

Рябчун Максим Андрійович, студент Дніпровського наукового українсько-американського ліцею Дніпровської міської ради, ryabchun.maksim@gmail.com

Кифорук Юрій Миколайович, вчитель інформатики Дніпровського наукового українсько-американського ліцею Дніпровської міської ради, kiforuk.yury@gmail.com

Section 1

PROTECTION OF REAL-TIME TELEMETRY FLOWS FROM DOS/MANIPULATIONS

Kateryna Savchenko
Municipal Extracurricular Educational Institution, Junior Academy of Sciences for Schoolchildren of the Dnipropetrovsk Regional Council, Dnipro, Ukraine
Scientific advisor: Yurii Kyforuk

Relevance. In modern conditions of digitalization, the majority of critical infrastructures depend on the continuous transmission of telemetry data in real time. Telemetry flows ensure the collection and processing of information about the state of objects, which enables systems to work stably and safely. However, the increase in the number of connected devices and the use of open networks, in particular the Internet, increases the risks of DoS-type cyber attacks and data manipulation aimed at violating the integrity or availability of telemetry information. Such attacks can lead to incorrect functioning of monitoring systems.

Purpose. The purpose of the study is to identify effective approaches to ensuring the integrity, reliability and availability of telemetry streams transmitted in real time, as well as creating mechanisms for detecting and neutralizing DoS attacks and data manipulation.

Basic provisions. The main provisions of this report are based on the analysis of threats that pose a danger to telemetry flows and the determination of complex means of their countermeasures. Telemetry streams can be subject to DoS and DDoS-type attacks, where attackers overload network resources, causing data outages, as well as manipulation attacks in which telemetry information is distorted or swapped. An important aspect is also the danger of replay attacks and injections of false data injecting false information into the system. To counter such threats, adaptive traffic filtering systems, network segmentation, are used load balancing between nodes. Furthermore, the implementation of behavioral anomaly detection algorithms based on statistical analysis or machine learning is crucial for identifying low-rate DoS attacks that evade traditional threshold-based filters. To ensure strict data integrity and prevent replay attacks, the communication protocol must incorporate Hash-based Message Authentication Codes (HMAC) combined with precise timestamping or nonce verification. The defense architecture should integrate Software-Defined Networking (SDN) to dynamically isolate compromised segments, implement mutual TLS (mTLS) for bidirectional authentication, and apply Long

Short-Term Memory (LSTM) networks to detect subtle cyber-attacks disguised as normal operational anomalies. For time-critical telemetry, optimizing the DTLS 1.3 handshake process and utilizing lightweight cryptographic primitives (e.g., ChaCha20-Poly1305) allows minimizing latency without compromising the security posture. Equally important is cryptographic protection, which includes encryption, digital signatures, certificate-based authentication.

Conclusions. As a result of the preparation of the report, it was summarized information on the main threats affecting the safety of telemetry flows and ways to prevent them are considered. The most effective approach to protection is a combination of encryption, authentication, QoS and communication channel reservation and the deployment of intelligent intrusion detection systems (IDS) capable of analyzing telemetry packet headers and payloads in real-time to block malicious traffic patterns instantly.

List of references

1. Shen, W., & Zhang, Y. (2024). Secure Telemetry Data Transmission for Satellite Networks under DDoS Conditions. IEEE Transactions on Aerospace and Electronic Systems. DOI: 10.1109/TAES.2024.3298764.

2. Liu, H., et al. (2023). QoS-based Resilient Communication Framework for Spaceborne Telemetry Systems. Journal of Network and Computer Applications, 220, 103656.

3. Mitigating Microplastics Risks to Advance Ocean Health. Geospatial World. URL – https://www.geospatialworld.net (date of access: 03.11.2025)

4. Kyforuk Yu.M., Petrosyan P.A., Kravchenko K.S., Puchenina M.R.Kondrachuk S.S., Andreev S.M. Creation of aerospace monitoring of pollution of oceans and seas by plastic emissions // Dnipro Orbit - 2025: materials of the XX scientific readings (October 22-24, 2025) / National Center for Aerospace Education of Youth named after O.M.Makarov, SE "Design Bureau" Yuzhnoye "named after M.K. Yangel", National Museum of Cosmonautics named after S.P. Korolev, Dnipro National University named after O. Honchar. - Dnipro, 2025. - P. 213-214

Information about the authors

Kateryna Savchenko, student member of the «Fundamentals of Electronics» club Municipal extracurricular educational institution Small Academy of Sciences for Schoolchildren of the Dnipropetrovsk Regional Council, katya2009.savchenko@gmail.com

Yurii Mykolayovych Kyforuk, head of the «Fundamentals of Electronics» club, Municipal Extracurricular Educational Institution, Junior Academy of Sciences for Schoolchildren of the Dnipropetrovsk Regional Council, kiforuk.yury@gmail.com

Секція 1

ДОСЛІДЖЕННЯ ІНСТРУМЕНТІВ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ У ЗАЛЕЖНОСТЯХ JAVASCRIPT-ПРОЄКТІВ ТА РОЗРОБКА РОЗШИРЕННЯ ДЛЯ VISUAL STUDIO CODE

Семенець О. Ю.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Тецький А. Г.

Актуальність. Сучасні веб-додатки значною мірою покладаються на зовнішні бібліотеки та залежності, що створює додаткові ризики для безпеки. Значна частина вразливостей виникає не у власному коді розробника, а саме у сторонніх пакетах, які імпортуються через менеджери залежностей (npm, Yarn тощо) [1]. Згідно з OWASP, вразливості, що походять від сторонніх пакетів та компонентів, становлять критичну загрозу для організацій [5]. Складність полягає в тому, що розробник часто не має інструментів для оперативної перевірки залежностей прямо під час роботи над проєктом. Стандартні методи аналізу, такі як статичний аналіз коду чи динамічне тестування, не охоплюють проблему небезпечних залежностей, які можуть містити відомі CVE або потенційно небезпечні версії пакетів [1-3].

Метою даної роботи є дослідження інструментів автоматизованого виявлення вразливостей у залежностях JavaScript-проєктів та розробка розширення для Visual Studio Code, яке виконує перевірку зовнішніх бібліотек із використанням декількох джерел даних про вразливості.

Основні положення. У ході роботи було проаналізовано інструменти та підходи до виявлення вразливих залежностей: npm audit [1], Snyk Open Source Scanner, GitHub Security Advisory, а також існуючі автоматизовані засоби CI/CD-перевірок [2,3]. Встановлено, що кожен з цих інструментів має власні недоліки: npm audit обмежений своєю базою, Snyk потребує інтеграції з API, GitHub Advisory не завжди містить деталізовані рекомендації. Для підвищення ефективності було розроблено розширення для Visual Studio Code, яке:

- автоматично зчитує залежності з package.json;
- запускає npm audit у робочому середовищі розробника;
- надсилає запити до Snyk API та GitHub Advisory API для перехресної перевірки кожного пакета;

– агрегує та нормалізує результати з різних джерел;

– відображає їх у вигляді інтерактивних поп-апів та панелі VS Code з рекомендаціями: оновити, замінити пакет, перевірити ланцюг залежностей [4].

Розширення дозволяє отримати більш точні результати, оскільки поєднує кілька незалежних баз даних, тим самим зменшуючи ймовірність пропуску критичних вразливостей. Було проведено тестування на типових JavaScript-проєктах і підтверджено здатність інструменту виявляти вразливості, які не розпізнаються стандартним npm audit.

Висновки. Виявлення вразливих залежностей у JavaScript-проєктах є важливим етапом забезпечення кібербезпеки, оскільки значна частина атак здійснюється через ланцюги постачання. Розроблене розширення для Visual Studio Code демонструє ефективність підходу, який об'єднує кілька джерел інформації про вразливості та надає розробнику результати безпосередньо в процесі роботи. Це дозволяє своєчасно виявляти ризики та приймати рішення щодо оновлення або заміни небезпечних компонентів. Запропонований підхід та реалізований інструмент можуть бути використані як частина процесу безпечної розробки (SSDLC) та інтегровані у практики DevSecOps.

Список літератури

1. npm-audit. NPM. URL – https://docs.npmjs.com/cli/v10/commands/npm-audit (дата звернення 17.10.2025)

2. Snyk. Open Source Security Scanning. Snyk. URL – https://snyk.io/product/open-source-security-scanning (дата звернення: 23.10.2025)

3. Advisories: GitHub Security Advisory Database. GitHub Docs. URL – https://docs.github.com/en/code-security/supply-chain-security/keeping-your-dependencies-updated-automatically/about-github-advisory-database (дата звернення: 20.10.2025)

4. Visual Studio Code Extension API. Microsoft Docs. URL – https://code.visualstudio.com/api (дата звернення: 28.10.2025)

5. OWASP Dependency-Check. OWASP Foundation. URL – https://owasp.org/www-project-dependency-check/ (дата звернення: 03.11.2025)

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

КІБЕРБЕЗПЕКА РОБОТІВ: АНАЛІЗ ВРАЗЛИВОСТЕЙ ТА НАСЛІДКИ ЇХ ВИКОРИСТАННЯ

Сіроклин О. В.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Клюшніков І. М.

Актуальність. Сучасний світ переживає нову промислову революцію, що базується на масовому впровадженні робототехнічних систем у ключові сектори економіки. Ця трансформація, попри значне зростання ефективності та продуктивності, створює новий, складний ландшафт загроз. Ключова проблема полягає у тому, що сучасний робот є складною кіберфізичною системою, яка успадковує вразливості як з інформаційного, так і з операційного світів. На відміну від традиційних IT-систем, наслідки кібератаки на робота можуть бути не лише цифровими, а й кібер-кінетичними, що призводить до фізичних руйнувань та становить загрозу життю і здоров'ю людини. Забезпечення кібербезпеки роботів грунтується на сучасніх методах забезпечення цілісності інформації [1].

Метою даної роботи є системний аналіз загроз кібербезпеці, притаманних сучасним робототехнічним системам, та обґрунтування необхідності застосування проактивних підходів до їх захисту. Це включає:

– огляд архітектури роботів для ідентифікації поверхонь атаки;

– класифікацію вразливостей на апаратному, програмному та комунікаційному рівнях;

– оцінку потенційних наслідків експлуатації цих вразливостей.

Основні положення. У доповіді наведено аналіз архітектури сучасного робота передбачає його дослідження як багаторівневої структури, що складається з апаратного, програмного та комунікаційного шарів. Розглянуто основні класи робототехнічних систем, зокрема промислові, колаборативні, сервісні та автономні, і визначено специфічні для них вектори загроз.

Проаналізовано існуючі інциденти безпеки, такі як вразливість UniPwn у роботах Unitree, що дозволяє перехопити повний контроль над рухами, злам промислових роботів, що дозволив обійти фундаментальні механізми безпеки та кібератаки на хірургічні системи, що продемонстрували можливість перехоплення команд хірурга [2-4].

Розроблено класифікацію вразливостей за основними доменами:

– програмним (незахищеність Robotic Operating System, ROS [5]);
– мережевим (небезпека протоколів Bluetooth, CAN);
– сенсорним (GPS-спуфінг, атаки на машинний зір);
– апаратним (незахищені діагностичні порти).

Висновки. Результати дослідження, які наведено у доповіді, підтверджують, що загрози кібербезпеці роботів не є гіпотетичними та несуть пряму небезпеку.

Наслідки експлуатації вразливостей виходять за межі цифрового простору, спричиняючи фізичну шкоду, економічні збитки, промислове шпигунство та навіть перетворення роботів на зброю. Кожен новий тренд у робототехніці, такий як інтеграція зі штучним інтелектом та хмарними платформами, ускладнює завдання захисту. Це вимагає розробки комплексного підходу до безпеки, що враховує загрози на всіх рівнях архітектури – від проектування до експлуатації – для запобігання кібер-кінетичним інцидентам.

Список літератури

1. Пєвнєв В. Я. Моделі загроз і забезпеченння цілісності інформаціїї // Системи та технології – 2018. – №2 (56/1) –. С. 79- 94. DOI: https://doi.org/10.32836/2521-6643-2018.2-56.6
2. Найпопулярніші людиноподібні роботи отримали дивний Bluetooth вірус. Noworries. URL: https://noworries.news/najpopulyarnishi-lyudynopodibni-roboty-otrymaly-dyvnyj-bluetooth-virus (дата звернення: 13.10.2025)
3. IOActive Finds Rampant Security Vulnerabilities in Home, Business and Industrial Robots. IOActive. URL: https://www.ioactive.com/article/ioactive-finds-rampant-security-vulnerabilities-in-home-business-and-industrial-robots/ (дата звернення: 13.10.2025).
4. ECE professors hack surgical robot in Motherboard special // University of Washington. URL: https://www.ece.uw.edu/spotlight/ee-professors-hack-surgical-robot-in-motherboard-special (дата звернення: 13.10.2025)
5. About ROS. ROS.org. URL: https://www.ros.org/about-ros/ (дата звернення: 13.10.2025)

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, НАУ «ХАІ», к.т.н., с.н.с., i.kliushnikov@csn.khai.edu

Секція 1

ДОСЛІДЖЕННЯ СТАНУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ДЕРЖАВНИХ ВЕБ-САЙТАХ УКРАЇНИ

Соколовський В. Б.
Харківського національного університету внутрішніх справ, м. Харків, Україна
Науковий керівник: Землянко Г. А.

Актуальність. В умовах цифрової трансформації та розвитку E-Government, веб-сайти державних органів стають ключовими агрегаторами персональних даних (ПДн) громадян. Зберігання великих обсягів цієї інформації робить такі ресурси пріоритетною ціллю для кібератак, у тому числі з боку APT-груп у гібридній війні [1]. Витік ПДн несе прямі фінансові збитки, підриває довіру до державних інституцій та створює загрозу національній безпеці. Тому аудит відповідності цих сайтів законодавству та міжнародним стандартам є критичним науково-практичним завданням.

Метою даної роботи є аналіз стану захисту персональних даних на державних веб-ресурсах України, систематизація типових векторів атак та виявлення поширених вразливостей. Дослідження фокусується на загрозах, класифікованих у OWASP Top 10, зокрема: «Неправильна конфігурація безпеки» (A05:2021), «Вразливі та застарілі компоненти» (A06:2021) та «Небезпечний дизайн» (A04:2021) [2].

Основні положення. Методологія дослідження базувалася на аналізі відкритих даних (OSINT) та ненав'язливому скануванні конфігурацій безпеки транспортного і прикладного рівнів. Аудит транспортної безпеки (TLS) виявив значну неоднорідність: хоча ключові портали (служби «Дія», сайти міністерств) використовують стійкі протоколи (TLS 1.2/1.3), значна частина регіональних сайтів все ще підтримує застарілі та вразливі версії (SSLv3, ранні TLS), що робить їх сприйнятливими до атак ПУДЕЛЬ або ЗВІР [3].

На прикладному рівні проаналізовано реалізацію HTTP-заголовків безпеки, що захищають від атак на стороні клієнта. Встановлено, що на багатьох відомчих сайтах ці заголовки відсутні або налаштовані некоректно. Зокрема, відсутність суворої Політики безпеки вмісту (CSP) робить ресурси вразливими до XSS-атак, що є основним вектором для крадіжки сесійних cookie та перехоплення ПДн.

Крім того, аналіз конфігурації виявив часті випадки вразливості A05:2021 – «Неправильна конфігурація безпеки» [2]. Це проявляється в

публічному доступі до службових файлів (наприклад, nv, we onfig), розкритті версій програмного забезпечення в HTTP-відповідях і використанні CMS (Content Management Systems) з відомими, але невиправленими вразливостями. Ця недбалість значно зменшує витрати зловмисників на дослідження та використання вразливостей «Вразливі та застарілі компоненти» (A06:2021).

Висновки. Стан захисту персональних даних на держсайтах України неоднорідний: високий рівень критичних сервісів нівелюється вразливістю регіональних сайтів, що використовуються як точки входу, та загрозами «ланцюга поставок». Вирішення проблеми вимагає спільної державної політики, обов'язкових регулярних аудитів та впровадження автоматизованих сканерів (DAST/SAST) для всіх без винятку веб-ресурсів влади.

Список літератури

1. Pevnev, V., Tsuranov, M., Zemlianko, H., & Amelina, O. (2021). Conceptual model of information security. *Lecture notes in networks and systems* (s. 158–168). Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-66717-7_14 (дата звернення: 23.10.2025)

2. A05 security misconfiguration - OWASP top 10:2021. *OWASP Foundation*. URL – https://owasp.org/Top10/A05_2021-Security_Misconfiguration (дата звернення: 23.10.2025)

3. Yavor O., Piddubna V., Ruban O. Legal concerns regarding the protection of minors' personal data in compliance with national legislation and GDPR requirements. *ScienceRise: juridical science*. 2023. No. 3(25). P. 23–34. DOI: https://doi.org/10.15587/2523-4153.2023.286647

4. Zhang Z., Yong F. Study on the security of government portal websites. *Applied mechanics and materials*. 2013. Vol. 380-384. P. 2534–2538. DOI: https://doi.org/10.4028/www.scientific.net/amm.380-384.2534

Відомості про авторів

Соколовський Вадим Борисович, магістрант кафедри кібербезпеки та DATA-технологій ННІ № 5 Харківського національного університету внутрішніх справ

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

Секція 1

НЕДОЛІКИ ТЕСТУ СОЛОВЕЯ-ШТРАССЕНА НА ПРОСТОТУ ЧИСЛА

Стадніченко М. С.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Пєвнєв В. Я.

Актуальність. Перевірка простоти чисел залишається однією з ключових задач сучасної криптографії та теорії чисел. Незважаючи на появу нових досконалих алгоритмів, зокрема детермінованих та прискорених ймовірнісних методів, пошук і аналіз інших можливостей перевірки чисел на простоту й досі залишається актуальним.

Метою роботи є формування загальної характеристики тесту Соловея-Штрассена та у порівнянні з тестом Мілера-Рабіна.

Основні положення. Основною частиною доповід є аналіз і порівняння основних та загальних характеристик двох тестів. Теоретична межа помилки, для окремих випадків сягає 1/2. Для k ітерацій це $(1/4)^{\cdot}$, що у два рази більше за тест Мілера-Рабіна. Складність обох тестів однакова для однієї перевірки, а саме O(log n M(n)), але тест Соловея-Штрассена потребує більше раундів, тому його загальна складність вище мінімум на 1 раунд [1]. Алгоритм не має завчасних виходів та «легких» випадків. Для кожної перевірки має бути обраховано символ Якобі[1]. Слід підкреслити, що обчислення символу Якобі, на відміну від модульного експоненціювання, базується на алгоритмі, подібному до алгоритму Евкліда, що важко піддається розпаралелюванню та векторизації на сучасних процесорах через залежність даних у ітераціях. Тест Соловея-Штрассена загалом вкрай залежний від структури числа, що перевіряється, від його факторизації. Для $N = P \times Q$ це може частка брехунів <1/4для $N = P^2 \times Q \approx 0\%$ для спеціальних чисел Кармайкла частка наближається до верхньої межі [1,2]. Числа Кармайкла та спецальні псевдопрості числа Ейлера є двома множинами, що перетинаються. Такі числа називаються special Carmichael (1729, 2465, 15841, 41041, 46657, 75361) [2]. Псевдопрості числа Ейлера зустрічаються набагато частіше за числа Кармайкла (наприклад кількість чисел Кармайкла- $< 10^{10}$: 1547, чисел Ейлера до основи $2 < 10^{10}$: 8664) [3,4]. Символ Якобі має непросту оцінку за О-символікою, яка вкрай сильно залежить від числа, що оцінюється. Це додає алгоритму більше непередбачуваності та зростання часу виконання

при роботі з великими числами, також це залежить від структури цього числа. Тест, через свою структуру (використання символу Якобі) не піддається узагальненням та розширенням. Якщо тест Мілера-Рабіна не впорався з перевіркою числа n з базою a, то і тест Соловея-Штрассена на це не здатен. Алгоритм загалом має вкрай низьку використовуваність, навіть у навчальних цілях. Він не міститься у найпоширеніших криптографічних бібліотеках (OpenSSL, GMP/MPIR).

Висновки. Аналіз показує, що тест Соловея-Штрассена поступається тесту Міллера-Рабіна за практичною ефективністю. Імовірність хибного прийняття складеного числа є гіршою, обчислення символу Якобі довше і менш стабільне за модульні множення, а структура самого тесту гірше масштабується і комбінується з іншими методами та загальними базами. Тест Міллера-Рабіна забезпечує нижчу ймовірність помилки на один раунд, швидше виконується та краще оптимізується та загалом більш доступний у сучасних криптографічних бібліотеках. Тому в реальних криптографічних застосуваннях саме тест Міллера-Рабіна вважають стандартом ймовірнісних тестів числа на простоту.

Список літератури

1. Monier L. Evaluation and comparison of two efficient probabilistic primality testing algorithms. Theoretical Computer Science 12 -1980. – P. 97 – 108. DOI: https://doi.org/10.1016/0304-3975(80)90007-9

2. Di Biagio, Lorenzo. Euler Pseudoprimes for Half of the Bases Integers, vol. 12, no. 6, 2012, pp. 1231-1237. DOI: https://doi.org/10.1515/integers-2012-0037

3. Grantham, Jon. “Frobenius pseudoprimes”. Math. Comput. 70 (2001): P. 873-891. DOI: https://doi.org/10.1090/S0025-5718-00-01197-2

4. The On-Line Encyclopedia of Integer Sequences. Number of Carmichael numbers less than 10^n. URL: https://oeis.org/A055553 (дата звернення: 01.11.2025)

5. The On-Line Encyclopedia of Integer Sequences. Number of base-2 Euler pseudoprimes.–URL: https://oeis.org/A006970 (дата звернення: 03.11.2025)

Відомості про автора

Стадніченко Максим Сергійович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.s.stadnichenko@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

РОЛЬ ПРИМАНОК У КІБЕРБЕЗПЕЦІ

Тецький А. Г.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна

Актуальність. Звіт Державної служби спеціального зв'язку та захисту інформації України за перше півріччя 2025 року свідчить про зростання кількості та складності кібератак [1]. Активний розвиток методів штучного інтелекту та використання цих методів у всіх галузях людської діяльності відкриває нові можливості і для тих, хто атакує мережеві ресурси, так і для тих, хто їх захищає. В умовах розвиненої сталої загрози (Advanced persistent threat, APT) штучний інтелект стає серйозним помічником для модифікації добре відомих векторів атак [2].

Цікавим напрямком у кібербезпеці є створення та використання приманок (honeypots) [3]. Це спеціально підготовлений об'єкт (застосунок, сервер чи навіть ціла інфраструктура), що спонукає до вторгнення та несанкціонованого використання. Оскільки використовуються підроблені бази даних, файли та інші дані, то атака на такі приманки не має впливати на основні мережеві ресурси, що містять важливі кіберактиви. З іншого боку під час таких атак можуть вивчатися інструменти та інші особливості атак, отримані дані можуть бути використані для захисту реальних мережевих ресурсів від існуючих загроз.

Метою даної роботи є визначення можливостей застосування приманок для дослідження інструментальних засобів, що використовуються під час атак на мережеві ресурси.

Основні положення. Використання приманок дає змогу дослідникам спостерігати за поведінкою атакуючих. Їхня цінність полягає в тому, що кожен дотик до приманки є за визначенням підозрілим, тому аналітик отримує інформацію про спосіб атаки. Окремо слід виділити доцільність застосування гібридних архітектур, що поєднують приманки з високим рівнем взаємодії (High-interaction) для глибокого аналізу поведінки зловмисника та емулятори сервісів (Low-interaction) для масштабування периметра захисту. Такий підхід дозволяє отримувати унікальні індикатори компрометації (IoC) та TTPs (Tactics, Techniques, and Procedures), які неможливо виявити класичними сигнатурними методами. Завдяки таким об'єктам можна досліджувати техніки сканування, методи проникнення, шаблони атак перебору грубої сили, послідовності команд

зловмисника, експлуатацію вразливостей нульового дня [4], роботу ботнетів, звички конкретних APT-груп, їхні інструменти та ланцюжки доставки шкідливого коду. Приманки дають можливість збирати зразки шкідливого програмного забезпечення, аналізувати мережевий трафік атаки, виявляти повторювані техніки соціальної інженерії, досліджувати поведінку зловмисних скриптів і збагачувати власні моделі виявлення аномалій. На рівні інфраструктури приманки дозволяють зрозуміти, як саме нападник рухається між вузлами, які привілеї намагається підвищити, які інструменти завантажує, яку інформацію шукає.

Висновки. Таким чином приманки стають не лише способом раннього виявлення інцидентів, а й повноцінною дослідницькою платформою, що відкриває доступ до реальної картини загроз, дає змогу моделювати атаки та покращувати ефективність захисту на основі емпіричних даних. Отримані дані можуть бути використані для навчання систем штучного інтелекту, які можуть стояти на захисті реальних об'єктів мережевої інфраструктури.

Список літератури

1. Звіт за І півріччя. Державна служба спеціального зв'язку та захисту інформації України. URL – https://cip.gov.ua/services/cm/api/attachment/download?id=71278 (дата звернення: 12.11.2025)
2. Ukraine sees surge in AI-Powered cyberattacks by Russia-linked Threat Actors. Security Affiars. URL – https://securityaffairs.com/183222/apt/ukraine-sees-surge-in-ai-powered-cyberattacks-by-russia-linked-threat-actors.html (дата звернення: 12.11.2025)
3. Honeypots in Cybersecurity: Their Analysis, Evaluation and Importance. URL – https://www.preprints.org/manuscript/202408.0946 (дата звернення: 12.11.2025)
4. Zero-Day Exploit Statistics: The 2025 Threat Report for Defenders. URL – https://deepstrike.io/blog/zero-day-exploit-statistics-2025 (дата звернення: 12.11.2025)

Відомості про авторів

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

Секція 1

ПРОЕКТУВАННЯ БЕЗПЕЧНОЇ АРХІТЕКТУРИ ІНТЕЛЕКТУАЛЬНОГО ШІ-ПОМОЧНИКА ДЛЯ ОСВІТНЬОГО ПРОЦЕСУ

Федоренко Д. Д.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Землянко Г.А.

Актуальність. Інтеграція інтелектуальних помічників (ІП) на базі ШІ в університетський освітній процес кардинально підвищує доступність та персоналізацію освіти. Однак це створює нову, складну поверхню атаки. Виникають значні ризики для конфіденційності академічних даних (оцінки, ексклюзивні навчальні матеріали) та цілісності критичних функцій, таких як прокторинг, оцінювання та управління розкладами [1]. Традиційні моделі безпеки не повною мірою враховують специфіку загроз для ШІ, що зумовлює актуальність розробки комплексної безпечної архітектури [2].

Метою даної роботи є проектування та обґрунтування архітектури інтелектуального ШІ-помічника, що інтегрує вимоги кібербезпеки та функціональної безпеки, для забезпечення конфіденційності, стійкості та відмовостійкості критичних освітніх сервісів.

Основні положення. В основі запропонованого рішення лежить модульна архітектура, що включає інтерфейс користувача, API для інтеграції з навчальним контентом (LMS), ядро ШІ-моделей (NLU/NLG) і виділений модуль логування та моніторингу [2]. Особлива увага приділяється аналізу потоків даних (data flow) між компонентами та визначенням критичних функцій (наприклад, доступ до екзаменаційних матеріалів, зміна оцінок). Для цих функцій визначаються рівні важливості (Safety Integrity Levels) у контексті функціональної безпеки [3,4].

Комплекс заходів кіберзахисту включає сувору автентифікацію (MFA) та авторизацію на основі ролей (RBAC) для розмежування доступу студентів, викладачів та адміністраторів. Всі канали (data-in-transit) та сховища (data-at-rest) піддаються шифруванню. Ключовим елементом є захист ШІ-моделі від специфічних атак: ін'єкцій у промпти (Prompt Injection) та атак на дані (Data Poisoning), які можуть маніпулювати відповідями помічника або порушити процес навчання моделі [1,4].

Задля більшої функціональної безпеки пропонується система предиктивной діагностики відмов. Вона використовує механізми health checks та ML-аналіз телеметрії для раннього виявлення деградації сервісу. Розроблено алгоритми автоматичного переходу до безпечного стану (Automatic Safe State, APS) при інцидентах. Це включає режими обмеженої функціональності (degradation modes), відключення функції оцінювання при виявленні аномалії та процедури безпечного відновлення (graceful shutdown) для мінімізації втрат даних [1,4].

Висновки. У роботі формалізовано архітектуру ШІ-асистента, збалансовану між функціональністю та вимогами безпеки. Запропоновані механізми (RBAC, захист моделей) протидіють специфічним загрозам університетського середовища, таким як витік оціночних даних та маніпуляція відповідями. Однією з неочевидних загроз є компрометація даних телеметрії, які використовуються передиктивної діагностики. Очікувані результати включають прототипи процедур APS для критичних функцій та набір верифікаційних тестів для оцінки стійкості системи до змодельованих атак та збоїв..

Список літератури

1. Pevnev, V., Tsuranov, M., Zemlianko, H., & Amelina, O. (2021). Conceptual model of information security. Lecture notes in networks and systems (pp. 158–168). Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-66717-7_14

2. OWASP Top 10 for Large Language Model Applications. *OWASP Foundation*. URL – https://owasp.org/www-project-top-10-for-large-language-model-applications (дата звернення: 23.10.2025)

3. Pevnev, V., Frolov, A., Tsuranov, M., & Zemlianko, H. (2022). Ensuring the data integrity in infocommunication systems. International Journal of Computing, 228–233. DOI: https://doi.org/10.47839/ijc.21.2.2591

4. Kumar Y., Kumar V. A systematic review on intrusion detection system in wireless networks: variants, attacks, and applications. *Wireless personal communications*. 2023. DOI: https://doi.org/10.1007/s11277-023-10773-x

Відомості про авторів

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

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

Секція 1

ДОСЛІДЖЕННЯ СТАТИСТИКИ ВРАЗЛИВОСТЕЙ ГЛОБАЛЬНО РОЗПОДІЛЕНИХ РЕПЛІКОВАНИХ СИСТЕМ ЗБЕРІГАННЯ ДАНИХ

Хроненко Я. Є.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Карпенко А.С.

Актуальність. Глобально розподілені системи зберігання даних (DSS) є основою сучасної цифрової інфраструктури, забезпечуючи цілісність, масштабованість, доступність і стійкість до відмов. Водночас їхня складна архітектура підвищує ризики безпеки. Реплікація та використання гібридних хмар створюють нові вектори атак, що потребують системного аналізу вразливостей [1,2].

Метою роботи провести дослідження статистики відомих вразливостей у глобально розподілених реплікованих системах зберігання даних, визначити їхню класифікацію, динаміку появи та вплив на безпеку інформаційних інфраструктур.

Основне положення. Глобально розподілені системи зберігання даних ґрунтуються на принципі реплікації – створенні копій даних у різних географічних регіонах для підвищення надійності та швидкодії. Попри це, саме механізми синхронізації, керування репліками та аутентифікації користувачів часто стають джерелом критичних вразливостей.

Під час дослідження використовувалася база даних CVE (Common Vulnerabilities and Exposures) за останні 5 років, що охоплює понад 2000 записів, пов’язаних із базами даних типу Cassandra, MongoDB, Redis, Amazon S3, Google Cloud Storage та ін [1, 3].

Було проведено статистичну класифікацію за типами вразливостей [3]:

- 45% помилки автентифікації та авторизації (ACL misconfiguration, token leakage);
- 27% уразливості в мережевих протоколах реплікації (data desynchronization, man-in-the-middle);
- 18% вразливості конфігураційного рівня (відкриті порти, слабкі політики безпеки);
- 10% апаратно-залежні атаки (cache poisoning, speculative execution flaws).

Виявлено тенденцію до зростання вразливостей у компонентах cloud-based replication та multi-region orchestration, що свідчить про посилення ризиків при інтеграції хмарних і локальних вузлів. Виявлено критичну кореляцію між використанням моделей Eventual Consistency та вразливістю до Race Condition. Аналіз також показав, що незахищені механізми серіалізації в протоколах Gossip/Raft створюють вектори для RCE-атак на рівні оркестрації контейнерів. Для оцінки впливу кожної категорії використовувалися показники CVSS (Common Vulnerability Scoring System) [4].

Середній рівень критичності склав 7,6 із 10, що вказує на високу небезпеку експлуатації таких систем у корпоративному середовищі без належного моніторингу безпеки [5].

Висновки. У роботі було проведено аналіз статистики вразливостей у реплікованих розподілених системах зберігання даних, визначено найпоширеніші категорії атак і виявлено загальну тенденцію до зростання кількості критичних інцидентів у хмарних середовищах. Отримані результати можуть бути використані для побудови моделей ризиків і розробки адаптивних систем виявлення вторгнень, орієнтованих на специфіку глобально розподілених баз даних.

Список літератури.

1. CVE – Common Vulnerabilities and Exposures Database. MITRE Corporation. URL – https://www.cve.org (дата звернення: 12.10.2025)
2. Пєвнєв В. Я. Моделі загроз і забезпеченння цілісності інформаціїї Системи та технології №2 (56/1). 2018. С. 79-94. DOI: https://doi.org/10.32836/2521-6643-2018.2-56.6
3. OWASP Top 10 for Cloud and Distributed Systems. Open Web Application Security Project. URL – https://owasp.org (дата звернення: 12.10.2025)
4. Common Weakness Enumeration (CWE). MITRE Corporation. URL – https://cwe.mitre.org (дата звернення: 12.10.2025)
5. Google Cloud Security Best Practices for Distributed Storage. Google Cloud. URL – https://cloud.google.com/security (дата звернення: 12.10.2025)

Відомості про авторів

Хроненко Ярослав Євгенович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.khronenko@student.csn.khai.edu
Карпенко Андрій Сергійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», PhD з кібербезпеки, a.karpenko@csn.khai.edu

Секція 1

МОДЕЛЬ ВИЯВЛЕННЯ БОТНЕТ-АТАК У БЕЗДРОТОВИХ МЕРЕЖАХ НА ОСНОВІ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Чорногор Д. А.
Харківський національний університет імені В.Н.Каразіна Харків, Україна
Науковий керівник: Олійников Р. В.

Актуальність розробки системи виявлення ботнет-атак у бездротових мережах та захисту вебресурсів зумовлена кількома факторами. По-перше, зростання кількості IoT-пристроїв і широке використання Wi-Fi мереж створюють нові можливості для зловмисників, які використовують ці мережі для створення ботнетів [1,2]. По-друге, вебресурси залишаються критично важливими для бізнесу, державних установ та суспільства, а зростання складності кібератак вимагає нових підходів до їх захисту. По-третє, методи машинного навчання дозволяють значно підвищити ефективність виявлення загроз у реальному часі, що є необхідним у динамічних і масштабних інформаційно-комунікаційних системах.

Метою роботи є розробка ПЗ для виявлення ботнет-атак у бездротових мережах та захисту вебресурсів на основі методів машинного навчання. Основними завданнями є створення моделі класифікації мережевого трафіку для ідентифікації ботнет-активності, імітація атак для тестування системи, а також розробка інтерфейсу користувача для моніторингу та аналізу результатів. Результати роботи можуть бути застосовані в таких галузях:

- кібербезпека: для захисту корпоративних і домашніх Wi-Fi мереж від ботнет-атак;
- захист вебресурсів: для запобігання DDoS-атакам, спаму та крадіжці даних на вебсерверах;
- спеціальні інформаційно-комунікаційні системи: для забезпечення безпеки в державних і військових мережах;
- дослідження: як інструмент для тестування нових алгоритмів виявлення кіберзагроз.

Основні положення. Дана робота спирається на результати попередніх досліджень у галузі аналізу мережевого трафіку та захисту інформаційних систем. Використання датасету CTU-13 як основи для навчання моделі ґрунтується на роботах С. Гарсії та інших, які довели його ефективність для моделювання ботнет-атак. Алгоритми машинного навчання, такі як Random Forest та нейронні мережі, обрані з урахуванням їх успішного застосування в роботах М. Фейлі, А. Зуева та інших. У той же час, робота

вносить новизну через фокус на бездротових мережах, де враховуються специфічні характеристики Wi-Fi трафіку, такі як канали передачі, MAC-адреси та динамічність топології [3-5]. Крім того, інтеграція захисту вебресурсів через аналіз трафіку, пов'язаного з HTTP, DNS та іншими протоколами, доповнює традиційні підходи до кібербезпеки, створюючи комплексне рішення. Систему захисту і систему атаки реалізовано в одній програмі, моделі тренуються на реальному датасеті, атаки імітують реальні пакети, всі атаки ідуть через бездротовий адаптер. Поведінка бот-нета це імітація, оскільки створювати та користуватися реальними бот-нетами не законно. Система реагує, як на імітовану атаку, так і на реальну.

Висновки. Розроблене програмне забезпечення поєднує в собі можливості моделювання атак, аналізу даних у реальному часі та візуалізації результатів, що відповідає сучасним вимогам до систем кібербезпеки. Таким чином, робота є логічним продовженням і розвитком існуючих досліджень, спрямованих на підвищення безпеки інформаційно-комунікаційних систем у сучасних умовах.

Список літератури

1. Bhadauria A., Sanyal S. Botnet detection and mitigation using machine learning techniques // International Journal of Information Security. – 2023. – Vol. 22. – P. 123–135. DOI: 10.1007/s10207–022–00615–3

2. Alothman A., Alotaibi A. A comprehensive review of botnet attacks and defense mechanisms // IEEE Access. – 2022. – Vol. 10. – P. 45678–45690. DOI: 10.1109/ACCESS.2022.3172345

3. Li X., Zhang Q. Artificial intelligence–driven botnet detection in IoT networks // IEEE Internet of Things Journal. – 2024. – Vol. 11, No. 3. – P. 4567–4578. DOI: 10.1109/JIOT.2023.3298765

4. Yang Q., Liu X. Synthetic data generation for botnet detection in IoT networks // IEEE Access. – 2024. – Vol. 12. – P. 56789–56798. DOI: 10.1109 ACCESS.2024.3389012

5. Singh A., Jain R. Automated response mechanisms for botnet attacks in enterprise networks // Journal of Network and Computer Applications. – 2022. – Vol. 198. – P. 103289. DOI: 10.1016/j.jnca.2021.103289

Відомості про авторів

Чорногор Дмитро Анатолійович, магістрант кафедри кібербезпеки інформаційних систем, мереж і технологій, ХНУ ім. В.Н. Каразіна, dmytro.chornohor@student.karazin.ua

Олійников Роман Васильович, професор кафедри безпеки інформаційних систем і технологій, ХНУ ім. В.Н. Каразіна, д.т.н., професор, roman.oliynykov@karazin.ua

Секція 1

ВИБІР ЗАСОБІВ ТА БЕЗПЕЧНИХ СЕРВІСІВ ПЕНТЕСТУВАННЯ: АНАЛІЗ, ІНФОРМАЦІЙНА МОДЕЛЬ ТА АЛГОРИТМИ

Шашкін М. А.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Харченко В.С.

Актуальність. Зростання кіберзагроз та складність сучасних IT-інфраструктур підвищують попит на безпечні сервіси пентестування (penetration testing as a service, або PtaaS). Для забезпечення захисту інформаційних систем, організації потребують ефективних і спеціалізованих засобів для оцінки вразливостей. Неправильний вибір інструментів або сервісів пентестування може призвести до недосконалого виявлення вразливостей та збільшення ризиків. За останні роки кіберінциденти внаслідок неоптимальних рішень для тестування безпеки зросли на 30%, що підтверджує необхідність обґрунтованого вибору таких засобів [1].

Метою дослідження є розроблення моделі вибору інструментів і сервісів для проведення пентестування на основі алгоритмів аналізу потреб, а також створення рекомендацій для підвищення безпеки та ефективності процесу пентестування. Дослідження фокусується на критеріях для вибору інструментів, відповідно до типів вразливостей, потреб організації, масштабів її IT-інфраструктури та бюджету.

Основні положення. Оптимізація вибору інструментів та сервісів пентестування можлива завдяки комплексному підходу, що включає аналіз факторів ризику, характеру вразливостей та бізнес-вимог клієнта. Для цього розроблена інформаційна модель, яка базується на алгоритмі рекомендацій, що охоплює:

- оцінювання потреб клієнта, коли враховуються специфікації, масштабність мережі, рівень захищеності та ресурси [2];
- ідентифікацію вразливостей, що включає класифікацію вразливостей за критеріями ризику та впливу на бізнес [3];
- вибір оптимальних інструментів, коли на основі попередніх аналізів система надає рекомендації щодо інструментів, таких як Nessus, Burp Suite, Nmap тощо, а також PtaaS платформ для безперервного моніторингу та тестування [4].

Використання запропонованої інформаційної моделі підтримується спеціальною анкетною формою, що дозволяє ефективно визначити потреби клієнта та забезпечити точне налаштування процесу пентестування.

Висновки. Розроблена інформаційна модель та алгоритм вибору засобів пентестування надають змогу покращити точність вибору та зменшити ризик недооцінки кіберзагроз. Рекомендований підхід сприяє ефективному використанню ресурсів та підвищенню загального рівня безпеки інформаційної системи. Важливими аспектами для впровадження моделі є адаптивність до потреб клієнта та здатність масштабуватися відповідно до змін у кіберсередовищі.

Для підвищення ефективності моделі необхідне регулярне оновлення даних про уразливості та сервіси, що забезпечить своєчасне реагування на загрози. Постійний моніторинг інструментів зберігає актуальність моделі, дозволяючи інтегрувати нові методи захисту у пентестування.

Таким чином, модель вибору інструментів пентестування підвищує якість та швидкість виявлення вразливостей, оптимізує витрати, зменшує ризики кібератак і підвищує кіберстійкість організацій.

Список літератури

1. Brian Carlson: Top cybersecurity statistics, trends, and facts. Csoonline. URL – https://www.csoonline.com/article/571367/top-cybersecurity-statistics-trends-and-facts.html (дата звернення: 13.11.2024)
2. SMART POWER: Розуміння потреб клієнта – основа ефективного пентесту. Spart Power. URL – https://www.smartpower.com.ua/pentest/ (дата звернення: 13.11.2024)
3. OWASP Top 10. OWASP. URL – https://owasp.org/www-project-top-ten/ (дата звернення: 13.11.2024)
4. Selecting the Perfect Tools for Effective Penetration Testing: A Comprehensive Guide. Eurofins Digitaltesting. URL – https://www.eurofins-digitaltesting.com/ selecting-the-perfect-tools-for-effective-penetration-testing-a-comprehensive-guide/ (дата звернення: 13.11.2024)

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 кібербезки, НАУ «ХАІ», д.т.н., професор, v.kharchenko@csn.khai.edu

Section 1

THE IMPACT OF PARAMETERS IN RSA CRYPTOSYSTEM ON THE FEASIBILITY OF KEY COMPROMISE VIA FACTORIZATION

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

Relevance. For many years, the RSA public-key cryptosystem has served as a foundational element of modern cryptographic infrastructures, ensuring both secure information exchange within communication networks and providing a reliable basis for digital signature mechanisms. Its security model relies on the assumption that the integer factorization problem lies outside the class P and that no efficient polynomial-time classical algorithms exist for solving it, thereby reducing the chance of key compromise [1].

However, the continuous growth in computing power, along with emerging theoretical appearance insights and the development of more sophisticated algorithms – including those originating from quantum computing research – necessitate a systematic and forward-looking reassessment of RSA's security stability. At present, a 2048-bit modulus is widely regarded as an industry standard. Although such key sizes substantially elevate the computational effort required for cryptanalytics attacks and currently remain resistant to classical sub-exponential factorization techniques under proper parameter selection, algorithms like the General Number Field Sieve still leave open the possibility of future advances capable of undermining these security guarantees [2].

In addition, the ongoing progress in quantum computing – most notably Shor's algorithm, which theoretically enables polynomial-time factorization – poses the most significant strategic threat to RSA in the long term [3,4]. This situation shows the needs to explore and design cryptographic mechanisms that offer stronger resilience [5].

The purpose of this work is to analyze the principal classical and modern factorization algorithms applicable to RSA, with particular emphasis on their computational complexity and practical relevance.

Principal provisions. The work provides a structured classification of factorization algorithms based on their computational complexity and domains. Within the context of RSA cryptanalysis, these algorithms can be grouped into several major categories: classical deterministic methods, stochastic techniques, lattice-based approaches, algebraic algorithms, and quantum methods. The work also includes comparative efficiency plots illustrating how the performance of

different factorization strategies varies with respect to RSA parameter choices and algorithmic implementations.

Conclusions. The analysis reaffirms that the security of RSA is intrinsically dependent on the computational difficulty of the integer factorization problem. Attacks on RSA-based systems employ both exponential-time algorithms (such as Fermat's method and Pollard's ρ algorithm) and sub-exponential techniques (including the Quadratic Sieve and the General Number Field Sieve), with the selection of a particular method determined by the bit-length of the modulus N and the relative sizes of its prime factors.

List of references

1. O. Illiashenko and V. Pevnev, "Development of large numbers factorization algorithm", in 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, Sep. 18–21, 2019. IEEE, 2019. DOI: https://doi.org/10.1109/idaacs.2019.8924341
2. V. Pevnev, O. Yudin, P. Sedlaček, and N. Kuchuk, "Method of testing large numbers for primality", Advanced Information Systems, vol. 8, no. 2, pp. 99–106, Jun. 2024. DOI: https://doi.org/10.20998/2522-9052.2024.2.11
3. Abbasi, M.; Cardoso, F.; Váz, P.; Silva, J.; Martins, P. A Practical Performance Benchmark of Post-Quantum Cryptography Across Heterogeneous Computing Environments. Cryptography 2025, 9, 32. https://doi.org/10.3390/cryptography9020032
4. Teşeleanu G. Partial Exposure Attacks Against a Family of RSA-like Cryptosystems. Cryptography. 2025; 9(1): 2. DOI: https://doi.org/10.3390/cryptography9010002
5. Mehta J, Rana H. Safest-Value of the Number of Primes in RSA Modulus and an Improvised Generalized Multi-Moduli RSA. Mathematics. 2025; 13(10):1690. DOI: https://doi.org/10.3390/math13101690

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

Секція 1

ДОСЛІДЖЕННЯ ПРОТОКОЛІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БЕЗДРОТОВИХ МЕРЕЖ З РОЗРОБКОЮ ПОЛІТИКИ БЕЗПЕКИ МЕРЕЖЕВОГО АДМІНІСТРАТОРА

Яковлєв О. Г.
Харківський національний університет внутрішніх справ, м. Харків, Україна
Науковий керівник: Цуранов М. В.

Актуальність. Сучасну людську цивілізацію важко уявити без доступу до глобальних мереж. До глобальної мережі Інтернет підключені більшість побутових пристроїв смартфони, комп'ютери, телевізори, розумні будинки, колонки, лампи, пилососи, пральні машини, відеокамери, автомобілі. Усім цим пристроям необхідно постійне оновлення програмного забезпечення, комунікація між пристроями, віддаленого керування та авторизації процесів.

Wi-Fi є найпоширенішою технологією доступу до мережі через зручність, мобільність і можливість підключення безлічі пристроїв одночасно без прокладання кабелів. Технологія забезпечує бездротовий доступ до Інтернету в межах зони покриття, що дозволяє користувачам переміщатися та використовувати мережу всюди. Кількість пристроїв котрі використовують технологію Wi-Fi постійно зростає на 2025 рік вона складає приблизно 75,44 мільярдів, Значна частина цих пристроїв відноситься до «Інтернету речей» (IoT), що відображає зростаючу інтеграцію розумних технологій [1].

Метою даної роботи є дослідження протоколів забезпечення кібербезпеки бездротових мереж.

Основні положення. Wi-Fi є радіо протоколом, що забезпечує бездротову передачу даних у відкритому середовищі, через це будь-який користувач, який перебуває в зоні дії мережі, потенційно може спробувати підключитися до неї або перехопити інформацію, що передається між клієнтом і точкою доступу. Тому найрозповсюдженими атаками на мережу є: MITM та Evil Twin [2].

Людина по середині це атака коли зловмисник перехоплює або підмінює трафік через фальшиву точку доступу або шляхом перехоплення сесій. Evil Twin створюється підроблена точка доступу Wi-Fi з таким самим іменем мережі (SSID), щоб користувачі підключилися саме до неї. Через це він може перехоплювати або підмінювати передані дані [2].

Для протидії MITM застосування протоколи TLS, VPN та протокол OWE. Для протидії Evil Twin потрібно впровадження WPA3-Enterprise з автентифікацією 802.1X (EAP-TLS) та використання WIDS/WIPS-систем для виявлення несанкціонованих точок доступу.

Різниця між WPA3-Personal та WPA3-Enterprise в тому що WPA3-Personal призначений для домашніх і малих мереж, використовуючи спільний пароль використовує протокол SAE це захищає від атаки brute-force, а WPA3-Enterprise призначений для корпоративних та урядових мереж, де потрібна строга аутентифікація кожного користувача через сервер (наприклад, RADIUS-сервер або EAP-TLS), а не загальний пароль, тому WPA3-Enterprise більш захищений. Також WPA3-Enterprise підтримує більший розмір ключів шифрування в алгоритмі AES, що висуває додаткові вимоги до обладнання, проте робить канал з'єднання більш захищеним.

Висновки. Wi-Fi став невід'ємною частиною повсякденного життя і постійно розвивається від стандарту 802.11 до 802.11be (Wi-Fi 7) демонструє постійне вдосконалення як швидкості передачі даних, та рівня безпеки. Із розвитком стандартів зростає і потреба у надійному захисті даних. Для запобігання несанкціонованому доступу необхідно застосовувати сучасні протоколи. Безпека бездротової мережі постійний процес, який вимагає оновлення технологій та підвищення обізнаності користувачів, адже саме від цього залежить стабільність і захищеність інформаційних систем у цифровому світі.

Список літератури

1. Alam Tanweer. A Reliable Communication Framework and its Use in Internet of Things. May 1, 2018. CSEIT1835111. Vol (3)5 : 450-456, Available at SSRN: https://ssrn.com/abstract=3619450 (дата звернення: 31.10.2025)

2. Що таке атака Evil Twin у Wi-Fi та як від неї захиститися? Securew. URL – https://www.securew2.com/blog/what-is-an-evil-twin-attack-in-wi-fi-and-how-can-i-protect-against-it (дата звернення: 31.10.2025)

Відомості про авторів

Яковлєв Олександр Геннадійович, магістрант кафедри кібербезпеки та DATA-технологій ННІ № 5 Харківського національного університету внутрішніх справ, yakovlev.alex02@gmail.com

Цуранов Михайло Віталійович, ст. викладач кафедри кібербезпеки та DATA-технологій ННІ № 5 Харківського національного університету внутрішніх справ, ukrear2006@gmail.com

ТЕЗИ ДОПОВІДЕЙ

Секція 2. Функційна безпека

ABSTRACTS OF REPORTS

Section 2. Functional safety

Секція 2

МІНІМІЗАЦІЯ РИЗИКІВ НЕПРАВИЛЬНОГО ВСТАНОВЛЕННЯ ПАРАМЕТРІВ ФІЛЬТРІВ ДЛЯ ПОКРАЩЕННЯ ЯКОСТІ РСА-ЗОБРАЖЕНЬ

Аль-Сенайх Р.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Рубель О. С.

Актуальність. Неправильний вибір параметрів фільтра Lee для пригнічення спекл-шуму в SAR-зображеннях призводить до втрати важливих деталей та неточного визначення меж об'єктів, що створює серйозні ризики для безпеки при картографуванні, де необхідно коректно приховувати об’єкти [1-3].

Традиційні підходи до вибору параметрів фільтрів базуються на емпіричних правилах або вичерпному пошуку, що вимагає значних обчислювальних ресурсів і не підходить для автоматизованих систем обробки даних у реальному часі.

Метою даної роботи є розробка методу мінімізації ризиків неправильного встановлення параметрів фільтрів для обробки SAR-зображень Sentinel-1 шляхом апріорного прогнозування оптимальних параметрів з використанням методів глибокого навчання.

Основні положення. Запропонований метод формулює задачу вибору оптимального розміру вікна фільтра Lee як пряму багатокласову класифікацію з використанням трансферного навчання. На відміну від існуючих підходів, заснованих на регресійному прогнозуванні метрик якості з подальшим вибором максимуму, запропонований метод автоматично витягує релевантні ознаки зі зображень і безпосередньо прогнозує оптимальний розмір вікна як клас [2,3]. Модель базується на архітектурі MobileNetV2, попередньо навченій на наборі даних ImageNet. Архітектура адаптована для обробки одноканальних SAR-зображень та класифікації оптимальних розмірів вікон фільтра. Використовується стратегія повного fine-tuning, при якій всі шари мережі навчаються спільно. Автоматизація процесу вибору параметрів фільтра значно знижує ризики людської помилки та забезпечує стабільну якість обробки зображень, що критично важливо для забезпечення безпеки при визначенні меж об’єктів та їх приховуванні на картографічних зображеннях. Метод протестовано на прикладі фільтра Lee та дозволяє забезпечити точне визначення меж

об’єктів для їх коректного приховування, що критично важливо для забезпечення безпеки при картографуванні.

Висновки. Запропонований метод на основі трансферного навчання MobileNetV2 дозволяє мінімізувати ризики неправильного встановлення параметрів фільтрів для SAR-зображень Sentinel-1 шляхом автоматизованого прогнозування оптимальних розмірів вікон фільтра Lee, що забезпечує точне визначення меж об’єктів для їх коректного приховування. Автоматизація процесу значно знижує ймовірність помилок, пов’язаних з ручним підбором параметрів, та забезпечує стабільну якість обробки в різних умовах зйомки. Метод придатний для оперативної інтеграції у виробничі конвеєри обробки SAR-даних та може бути використаний для забезпечення безпеки при картографуванні та аналізі територій.

Список літератури

1. Lee J. S. Digital image enhancement and noise filtering by use of local statistics / J. S. Lee // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1980. – Vol. 2, № 2. – P. 165–168. DOI: https://doi.org/10.1109/TPAMI.1980.4766994

2. Rubel O. Selection of Lee filter window size based on despeckling efficiency prediction for Sentinel SAR images / O. Rubel, V. Lukin, A. Rubel, K. Egiazarian // Remote Sensing. – 2021. – Vol. 13, № 10. – P. 1887. DOI: https://doi.org/10.3390/rs13101887

3. Lukin V. An Approach to Prediction of Signal-Dependent Noise Removal Efficiency by DCT-Based Filter / V. Lukin, S. Abramov, A. Rubel, S. Krivenko, A. Naumenko, B. Vozel, K. Chehdi, K. Egiazarian, J. Astola // Telecommunications and Radio Engineering. – 2014. – Vol. 73, № 18. – P. 1645–1659. DOI: https://doi.org/10.1615/TelecomRadEng.v73.i18.40

Відомості про авторів

Аль-Сенайх Раед, аспірант кафедри інформаційно-комунікаційних технологій ім О.О. Зеленського, НАУ «ХАІ», r.z.alsenaikh@khai.edu

Рубель Олексій Олександрович, доцент кафедри інформаційно-комунікаційних технологій ім О. О. Зеленського, НАУ «ХАІ», к.т.н., o.rubel@khai.edu

Секція 2

ДОСЛІДЖЕННЯ І РОЗРОБКА СИСТЕМИ ОЦІНЮВАННЯ ЯКОСТІ ІНТЕРФЕЙСІВ ДОПОВНЕНОЇ РЕАЛЬНОСТІ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Асєєв Д.О.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Орєхов О.О.

Актуальність. Сучасні інтерфейси доповненої реальності (AR) активно інтегруються у медицину, освіту, індустріальний дизайн та розважальні технології [1]. Зі зростанням їх популярності виникає потреба у стандартизованій та об'єктивній оцінці ефективності AR-взаємодії. Традиційні методи, що базуються на ручному аналізі та невеликих вибірках користувачів, не забезпечують масштабованість і не дозволяють оперативно отримувати якісні аналітичні висновки.

Штучний інтелект відкриває можливість автоматизувати опрацювання опитувань, агрегувати дані та формувати аналітику в режимі реального часу. Таким чином, питання розробки інтелектуальної системи аналізу якості AR-інтерфейсів є актуальним для сучасних UX-досліджень та цифрового продуктового дизайну [2-4].

Метою дослідження є розробка веб-системи, яка забезпечує збір, аналіз та інтелектуальне формування висновків щодо якості інтерфейсів доповненої реальності на основі користувацьких опитувань і алгоритмів штучного інтелекту.

Основні положення. У межах роботи створено веб-систему для оцінювання якості інтерфейсів доповненої реальності, що поєднує інтерактивне опитування, статистичний аналіз та автоматичне формування текстових висновків за допомогою штучного інтелекту. Адміністратор формує структуру питань у Strapi CMS, визначає аспекти оцінювання та керує даними опитувань [5]. Після заповнення анкети результати автоматично агрегуються, обчислюються середні показники за аспектами та генеруються оновлені аналітичні звіти.

Під час розробки системи враховано базові вимоги кібербезпеки: використання HTTPS, токенізованого доступу до API, ролей і прав у CMS, захисту персональних даних респондентів, ізоляції бази даних та фільтрації вхідної інформації для запобігання ін'єкціям. Технологічна архітектура включає React + Next.js для фронтенду, Strapi CMS (Node.js) для бекенду та

PostgreSQL як основне сховище, що забезпечує надійність, масштабованість і безпечну обробку даних.

Висновки. Розроблена система оцінювання AR-інтерфейсів демонструє ефективність у поєднанні інструментів опитування та штучного інтелекту. Вона дозволяє автоматизувати рутинні етапи UX-дослідження, підвищити об'єктивність аналізу та забезпечити наочність результатів завдяки візуалізаціям. Система є гнучкою, розширюваною та придатною для використання як у навчальних, так і в комерційних дослідженнях AR-рішень.

Список літератури

1. Azuma, R. T. A Survey of Augmented Reality. Presence: Teleoperators and Virtual Environments. URL – https://www.cs.unc.edu/~azuma/ARpresence.pdf (дата звернення: 14.11.2025)
2. Caruso, G., et al. User-Centered Evaluation Framework to Support the Interaction Design for Augmented Reality Applications. Multimodal Technologies and Interaction, 8(5) (2024). URL – https://www.mdpi.com/2414-4088/8/5/41 (дата звернення: 14.11.2025)
3. National Institute of Standards and Technology (NIST). Augmented Reality (AR) Usability Evaluation Framework. NIST Interagency/Internal Report (NISTIR) 8422. URL – https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8422.pdf (дата звернення: 14.11.2025)
4. ISO 9241-210:2019. Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems. URL – https://www.iso.org/standard/77520.html (дата звернення: 14.11.2025)
5. Strapi 5 Docs – Headless CMS Documentation. Strapi. URL – https://docs.strapi.io/ (дата звернення: 14.11.2025)

Відомості про авторів

Асєєв Данило Олегович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.asieiev@student.csn.khai.edu
Орєхов Олександр Олександрович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., доцент, a.orehov@csn.khai.edu

Секція 2

МУЛЬТИМОДАЛЬНА ІНФОРМАЦІЙНА СИСТЕМА КВАНТИФІКАЦІЇ РИЗИКІВ ПОВІТРЯНИХ ЗАГРОЗ

Астраханцев О. А.
Київський національний університет імені Тараса Шевченка Науковий, Київ, Україні
Науковий керівник: Заславський В. А.

Актуальність. Сучасні системи оповіщення про повітряні загрози працюють переважно за бінарним принципом «Тривога/Відбій», що не забезпечує оцінку рівня небезпеки у реальному часі. Для цивільного населення, військових структур і критичної інфраструктури це створює ризики перевантаження інформаційними сигналами та зниження довіри до сповіщень [1].

Дослідження у сфері OSINT-технологій показують, що відкриті дані можуть значно підвищити точність оцінювання загроз, якщо їх поєднати з аналітичними алгоритмами та методами машинного навчання. Тому важливим завданням є створення інформаційної системи, яка поєднує офіційні джерела, відкриті повідомлення та аналітичні індикатори для розрахунку кількісного рівня ризику. Такі рішення підвищують точність прогнозування загроз і допомагають швидше ухвалювати рішення у критичних ситуаціях [2].

Метою роботи є проєктування та розробка архітектури і створення інформаційно- аналітичної системи, що визначає рівень ризику повітряних загроз за допомогою обробки даних з різних джерел та алгоритмів машинного навчання [1,2].

Основні положення. Запропонована система об'єднує три типи даних: офіційні повідомлення (M_1), OSINT-джерела (M_2) та аналітичні показники (M_3). Кожному з них надається ваговий коефіцієнт довіри $W_i(t)$, який змінюється відповідно до достовірності інформації. Для зменшення впливу помилкових сигналів застосовується алгоритм Random Forest [3], який коригує ваги на основі попередніх результатів. Інтегральний рівень ризику для регіону визначається за формулою:

$$R_L(t) = \sum_{i=1}^{3} A_i \times W_i(t) \quad ,$$

де A_i – нормалізовані показники активності кожної модальності $M_i, i = \overline{1,3}$. Отримані результати використовуються для побудови теплової карти ризиків, яка показує зміну небезпеки у просторі та реальному часі [3].

Для забезпечення коректної інтерпретації результатів усі нормалізовані показники задовольняють умову, тобто їх сума дорівнює одиниці, а кожен окремий показник належить інтервалу від 0 до 1,

$$\sum_{i=1}^{3} A_i = 1, A_i \in [0,1]$$

.Такий підхід дозволяє оцінювати реальний стан загроз, виявляти критичні зони та допомагає приймати своєчасні рішення [1].

Висновки. Розроблена система кількісного оцінювання ризиків підвищує точність прогнозування, дозволяє використовувати відкриті та офіційні дані разом, а також зменшує кількість хибних тривог. Інтеграція машинного навчання, OSINT та аналітичних моделей забезпечує більш достовірну оцінку ситуаційної небезпеки, що є важливим для підвищення ефективності систем цивільного захисту та національної безпеки.

Список літератури

1. Hwang Y.-W., Lee I.-Y., Kim H., Lee H., & Kim D. Current Status and Security Trend of OSINT. // *Wireless Communications and Mobile Computing*, 2022. – С. 14. DOI: https://doi.org/10.1155/2022/12901291

2. Gaivoronski A.A., Knopov P.S., Zaslavskyi V.A. (eds.). *Modern Optimization Methods for Decision Making Under Risk and Uncertainty*. CRC Press Taylor Francis Group, 2023. – P. 388

3. Resende P.A.A., Drummond A.C. A Survey of Random Forest Based Methods for Intrusion Detection Systems. // *ACM Computing Surveys (CSUR)*, 2018, Vol. 51, Issue 3, Article 48, P. 1–36

Відомості про авторів

Астраханцев Олексій Андрійович, магістр кафедри математичної інформатики, факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка, alexeiastrakh@knu.ua

Заславський Володимир Анатолійович, професор кафедри математичної інформатики факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка, д.т.н., професор, zaslavskiy.volodymyr@knu.ua

Секція 2

АНАЛІЗ ЗАСТОСУВАННЯ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ У СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ РОЗПІЗНАВАННЯ ОБЛИЧ

Ахтирська С. В.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Куланов В. О.

Актуальність. Біометричні системи контролю доступу зручні, надійні та безпечні тим, що носії інформації завжди знаходяться у користувача та не можуть бути втрачені чи вкрадені. Одним зі способів біометричної автентифікації є технологія сканування обличчя, що набирає все більшу популярність протягом останніх років. Ринок технологій розпізнавання облич у 2022 році становив 5 мільярдів доларів, і очікується, що до 2032 року він зросте до 19 мільярдів доларів зі середньорічним темпом зростання 14% [1]. Точна ідентифікація за допомогою біометричних рішень безпеки дозволяє підприємствам забезпечити надійний доступ до важливих ресурсів та інформації, уникнувши ризику несанкціонованого доступу та забезпечивши швидкий а безконтактний доступ без запам'ятовування паролів або використання карток доступу [2].

Метою даної роботи є дослідження та аналіз технології сканування обличчя, що базуються на методах комп’ютерного зору.

Основні положення. Face Recognition (технологія сканування обличчя) використовує аналіз унікальних рис обличчя: форма, розміщення очей, ніздрів та рота для ідентифікації особи. Ця технологія заснована на використанні алгоритмів комп’ютерного зору, які дозволяють точно розпізнати особу за допомогою відео- або фотозображення [2].

Системи розпізнавання обличчя виконують чотирьох етапний процес:

1. Захоплення: Камера збирає зображення або відео обличчя людини у 2D або 3D форматі, залежно від можливостей пристрою.
2. Аналіз: Програмне забезпечення визначає ключові орієнтири обличчя, такі як очі, ніс і рот.
3. Порівняння: Ці орієнтири перетворюються на числовий код (підпис обличчя) та порівнюються з існуючими шаблонами в базі даних.
4. Верифікація: Якщо дані відповідають існуючому профілю, надається доступ або верифікація [3].

Одним із ключових методів, що забезпечують високу ефективність в обробці та аналізі зображень у межах таких систем, є згорткові нейронні мережі (Convolutional Neural Networks, CNN). Архітектура CNN включає в себе три основних шари: згорткові шари для формування карти ознак, шар пулінгу, який зменшує розмір карти ознак за допомогою фільтру, та повнозв'язний шар, який є результуючим. CNN відіграють ключову роль у підвищенні точності та надійності біометричних систем контролю доступу. Вони дозволяють автоматично виділяти та аналізувати важливі риси обличчя без необхідності ручного налаштування параметрів. CNN навчаються на великих наборах даних, що містять тисячі зразків облич різних людей, і здатні розпізнавати індивідуальні відмінності навіть за змінених умов освітлення, положення голови або міміки.

Системи контролю доступу, що базуються на розпізнаванні облич за допомогою CNN, мають низку потенційних ризиків і обмежень:

- проблеми конфіденційності та зберігання біометричних даних;
- атаки типу «spoofing» (імітаційні атаки);
- упередженість даних (bias) у навчанні нейронних мереж;
- високі вимоги до обчислювальних ресурсів;
- можливість зловживання технологією.

Висновки. Використання технології комп'ютерного зору у системах контролю доступу сприяє підвищенню рівня інформаційної безпеки, зручності користування та ефективності управління доступом у різних сферах діяльності - від корпоративних структур до побутових пристроїв, хоча все ще й має за собою певні ризики.

Список літератури

1. Facial recognition statistics and facts (2025). Market.us Scoop. URL – https://scoop.market.us/facial-recognition-statistics (дата звернення: 07.11.2025)
2. Біометричні рішення безпеки. Biosol. URL – https://biosol.ua (дата звернення: 07.11.2025)
3. Facial recognition: what it is & how it works | signicat. Signicat. URL – https://www.signicat.com/blog/face-recognition (date of access: 07.11.2025)

Відомості про авторів

Ахтирська Софія Вячеславівна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», s.v.akhtyrska@student.csn.khai.edu
Куланов Віталій Олександрович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., v.kulanov@csn.khai.edu

Секція 2

TAILSCALE ЯК ОСНОВА ДЛЯ ZERO TRUST МЕРЕЖ

Ахтирська С. В.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Лейченко К. М.

Актуальність. Традиційна модель захисту мереж запобігає зовнішнім загрозам завдяки використанню брандмауерів та систем виявлення вторгнень, проте всередині такої мережі рівень безпеки зазвичай набагато слабший, тож зловмиснику достатньо лише потрапити у саму мережу для того, щоб отримати доступ до даних в ній. Щоб прибрати таку вразливість варто встановити брандмауер навколо кожного пристрою та переконатися, що сеанси завжди шифруються між кожною парою кінцевих точок [1].

Метою даної роботи є дослідження принципів моделі Zero Trust та аналіз можливостей використання Tailscale як інструменту для створення захищеної приватної мережі. Розроблення мережевої директорії для зберігання персональних документів з використанням сервісу Paperless [4].

Основні положення. Zero Trust – це модель побудови інформаційних систем, що виходить з того, що систему вже зламано, і тому довіряти не можна нікому. Кожен доступ до даних і програм потребує підтвердження, користувачі отримують лише мінімально необхідні привілеї протягом обмеженого часу [2].

Tailscale – це mesh-сервіс VPN, який створює безпечну приватну мережу між вашими пристроями, незалежно від їхнього місцезнаходження, використовуючи протокол WireGuard з відкритим кодом [3].

Використовуючи разом ці дві технології – отримуємо надійно захищену приватну мережу, в якій Tailscale забезпечить:

- наскрізне шифрування трафіку;
- контроль доступу;
- ідентифікацію та автентифікацію користувачів;
- незалежність від місцезнаходження.

Особливу увагу слід приділити реалізації політик безпеки через механізм списків контролю доступу (ACL), які дозволяють детерміновано обмежувати мережеву взаємодію на рівні окремих вузлів, унеможливлюючи латеральне переміщення загроз (lateral movement). Архітектура рішення передбачає криптографічне розділення площини

управління (control plane) та площини даних (data plane), гарантуючи конфіденційність навіть у разі компрометації координаційного сервера.

Для створення такої мережі необхідно мати сервер, що буде виконувати роль хоста для сервісу Paperless та забезпечить безперебійний доступ до документів. Для захищеності системи встановлюємо та налаштовуємо Tailscale. Лише власник може додавати користувачів до мережі, також власник має можливість переглядати IP-адреси підключених пристроїв та їхній статус. Tailscale дозволяє налаштувати права доступу користувачів, відстежувати їхню активність за допомогою логів та загалом надає всі інструменти контролю над мережею та повну інформацію про те, що відбувається у ній.

Висновки. Tailscale може виступати ефективною основою для побудови Zero Trust мереж, особливо для малих і середніх організацій, яким важлива як безпека, так і простота впровадження. Поєднання цих технологій дозволяє значно знизити ризики зовнішніх та внутрішніх загроз, а також зробити інфраструктуру більш стійкою до кіберзагроз.

З використанням Tailscale вдалося розгорнути невелику приватну Zero Trust мережу для зберігання персональних документів з використанням сервісу Paperless та надати до неї доступ кільком користувачам, права яких були обмежені, а активність відстежена завдяки інструментам Tailscale.

Список літератури

1. Zero trust networking. Tailscale. URL – https://tailscale.com/kb/1123/zero-trust (дата звернення: 16.10.2025)

2. Модель з нульовою довірою. Вікіпедія. URL – https://uk.wikipedia.org/wiki/Модель_з_нульовою_довірою (дата звернення: 18.10.2025)

3. Pennarun A. Tailscale: how it works. Tailscale Best VPN Service for Secure Networks. Tailscale. URL – https://tailscale.com/blog/how-tailscale-works (дата звернення: 18.10.2025)

4. Paperless-ngx documentation. Paperless-ngx. URL – https://docs.paperless-ngx.com (дата звернення: 18.10.2025)

Відомості про авторів

Ахтирська Софія Вячеславівна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», s.v.akhtyrska@student.csn.khai.edu

Лейченко Кирило Миколайович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», PhD, k.leychenko@csn.khai.edu

Секція 2

ДОСЛІДЖЕННЯ ВПЛИВУ ТОЧНОСТІ НЕЙРОМЕРЕЖ НА ФУНКЦІЙНУ БЕЗПЕЧНІСТЬ СИСТЕМ ДІАГНОСТУВАННЯ НЕВРОЛОГІЧНИХ ЗАХВОРЮВАНЬ

Байда В. Р.
Національний аерокосмічний університет
«Харківський авіаційний інститут»,
м. Харків, Україна
Науковий керівник: Клюшніков І. М.

Актуальність. Аналіз томографічних зображень є важливим етапом діагностики патологій головного мозку, зокрема пухлин. Згідно з даними дослідження, опублікованого у 2025 році, кожен місяць затримки діагностики, підвищує ризик смертності на 18–28% [1].

Традиційні методи аналізу знімків значною мірою залежать від досвіду радіолога та значних часових ресурсів, що підвищує ризик затримок при постановці діагнозу або навіть пропуску патології, особливо у великих медичних закладах або в регіонах з обмеженим доступом до спеціалістів.

Відомий випадок, коли патологія залишалася непоміченою протягом багатьох років, попри її наявність на знімках [2]. Використання штучного інтелекту для автоматизованого аналізу МРТ-зображень дозволяє зменшити вплив людського фактора, прискорити діагностику та підвищити точність оцінки стану пацієнта.

Метою даної роботи є дослідження впливу точності аналізу томографічних знімків з використанням згорткових нейронних мереж (CNN) на функційну безпечність процесу встановлення діагнозу.

Процес аналізу знімків з використанням згорткових нейронних мереж здійснюється з використанням розробленого застосунку, який дозволяє виявляти та класифікувати пухлини, відображати патологію за допомогою теплової карти (heatmap), а також зберігати історію обробки з можливістю експорту результатів у форматі PDF для подальшого аналізу.

Основні положення. У ході роботи було розроблено веб-застосунок для автоматизованого аналізу МРТ-зображень головного мозку з використанням CNN. Досліджено вплив класичної та зваженої крос-ентропії як функції втрат на точність класифікації CNN за умов дисбалансу класів.

Використано відкритий набір даних Brain Tumor for 14 classes (4456 знімків) [3], що пройшов попередню обробку даних. Для навчання було

використано декілька архітектур CNN: AlexNet, VGG-16, ResNet-18, DenseNet-121, EfficientNet-B0.

Всі моделі навчалися з використанням оптимізатора Adam, планувальника CosineAnnealingLR для регулювання швидкості навчання. Окрім того, застосовано transfer learning з fine-tuning, early stopping та dropout для запобіганню перенавчанню. Найкращі результати показала модель EfficientNet-B0 без використання модифікації функції втрат, яка досягла точності 97,16 % на тренувальному наборі даних при мінімальній кількості хибнонегативних класифікацій (FN=7).

Висновки. Отримані результати показують, що найбільш ефективною моделлю є EfficientNet-B0, яка використовує класичну функцію втрат. Хоча зважена функція втрат може бути ефективним засобом для моделей, чутливих до дисбалансу, проте її застосування слід адаптувати до конкретної архітектури та специфіки поставленої задачі. Таким чином, реалізація глибоких CNN у поєднанні з веб-інтерфейсом забезпечує створення ефективного та функційно безпечного інструменту підтримки медичної діагностики.

Список літератури

1. Scott, R. Larger Tumor Size Linked to Higher Mortality Risk in Brain Cancer. CURE Today. URL – https://www.curetoday.com/view/larger-tumor-size-linked-to-higher-mortality-risk-in-brain-cancer (дата звернення: 09.09.2025)
2. Whitehead J. Father-of-three diagnosed with brain tumour claims doc-tors missed it for 12 years. The Independent. URL – https://www.the-independent.com/life-style/health-and-families/brain-tumour-missed-doctors-wales-b2171899.html (дата звернення: 09.09.2025)
3. Hennes W. N. Brain Tumor for 14 Classes. Kaggle. URL – https://www.kaggle.com/datasets/waseemnagahhenes/brain-tumor-for-14-classes/data (дата звернення: 29.09.2025)

Відомості про авторів

Байда Валерія Романівна, магістрантка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», v.baida@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@csn.khai.edu

Секція 2

ЗАХИЩЕНЕ СТИСНЕННЯ ОДНОВИМІРНИХ АКУСТИЧНИХ СИГНАЛІВ КОДЕРОМ НА ОСНОВІ НЕЙРОМЕРЕЖІ

Брисін П. В.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Лукін В.В.

Актуальність. У багатьох випадках виникає необхідність передавати одновимірні сигнали з високим ступенем стиснення, задовільною якістю та захищеністю інформації. Існують відомі методи, але бажано звернути увагу й на новітні підходи до стиснення, яке базується на нещодавно запропонованих рішеннях та програмних засобах кодування та декодування, які можуть бути відомим вузькому колу користувачів та бути доступними лише на передавальній та прийомній сторонах [1]. Одна з таких технологій нещодавно розроблена Ф. Беларом та його колегами, вона базується на використанні навчених нейромереж і забезпечує характеристики, що суттєво відрізняють її в кращий бік у порівнянні з відомими (традиційними) методами [2]. Кодер TSAC базується на модифікованій версії аудіокодека Descript, розширеній для стерео, та моделі Transformer для подальшого збільшення коефіцієнта стиснення [3].

Модель Transformer оцінюється детермінованим та відтворюваним способом. Тому результат не залежить від точної моделі графічного процесора чи процесора, а також від кількості налаштованих потоків. Це гарантує, що стиснутий файл можна розпакувати за допомогою іншої апаратної або програмної конфігурації. Основні переваги кодера продемонстровані для акустичних сигналів високої якості.

Метою даної роботи є дослідження здатності кодера стискати з втратами акустичні (музикальні та мовні) сигнали, що мають відносно низьке відношення сигнал-шум [2,3]. Доцільність такого аналізу зумовлена двома факторами. По-перше, зареєстровані сигнали можуть бути суттєво спотворені завадами [4]. По-друге, відомо що деякі методи стиснення даних, спотворених шумом, можуть дещо придушувати його [5].

Основні положення. Спочатку були розраховані значення коефіцієнтів стиснення (КС) для кількох музикальних файлів формату wav. Для сигналів без завад значення КС лежать в інтервалі від 120 до 156, для сигналів із вхідним відношенням сигнал-шум (ВСШ) 20 дБ – від 120 до 158, для ВСШ=10 дБ – від 116 до 148, для ВСШ=0 – від 111 до 129, тобто присутність інтенсивних завад загалом погіршує КС, але не дуже суттєво. Для ВСШ>15

дБ спостерігається деяке придушення завад внаслідок стиснення із втратами, тому пост-фільтрація після декомпресії не має сенсу. А для ВСШ в межах 0-10 дБ пост-фільтрація із використанням фільтрів на основі дискретного косинусного перетворення (ДКП) виявилась корисною, де виграш для вихідного ВСШ у порівнянні з вхідним ВСШ може сягати 8-10 дБ для версій із використанням як жорсткого порогу, так і комбінованого. Таким чином, вдається не тільки стиснути дані з КС>100, але й підвищити їх якість після декомпресії, якщо рівень шума в зареєстрованому сигналі є високим.

Аналогічні дані отримані і для випадку стиснення мовних сигналів, що спотворені адитивним білим гаусовим шумом. Для низьких вхідних ВСШ вдається підвищити метрику ESTOI за рахунок вибору оптимальних порогів – приблизно 3σ для жорсткого порогу та приблизно 5σ для комбінованого, де σ – середньоквадратичне відхилення шуму, що повинно бути апріорно відомим або точно оціненим.

Висновки. Завдяки новітнім методам стиснення одновимірних акустичних даних можна досягти значень КС, що перевищують 100. Для ситуацій, коли відношення сигнал-шум є малим, можливо суттєве покращення якості завдяки пост-фільтрації даних після декомпресії.

Список літератури

1. Юрх Н.Г., Петченко М.В., Іванченко І.С. (2025). Аналіз методів захисту системи передавання мовної інформації. Сучасний захист інформації, 2(62), 107–113. DOI: 10.31673/2409-7292.2025.026026

2. Bellard F. (2024) TSAC, Very Low Bitrate Audio Codec, URL – https://bellard.org

3. Kumar R., Seetharaman P., Luebs A. (2023). High-Fidelity Audio Compression with Improved RVQGAN. DOI: 10.48550/arXiv.2306.06546

4. Brysin P., Lukin V., DCT-based Denoising of Speech Signals, Herald of Khmelnytskyi National University. Technical sciences, No 4, 2024 (339), pp. 301-309. DOI: 10.31891/2307-5732-2024-339-4-4.

5. V. Lukin, M. Zriakhov, A. Popov, O. Pogrebnyak, Preliminary Processing and Lossy Compression of Multichannel Information Data, Industrial Informatics, Research in Computing Science, Vol. 31, 2007, pp. 105-114.

Відомості про авторів

Брисін Петро Володимирович, аспірант кафедри інформаційно-комунікаційних технологій ім О.О. Зеленського, НАУ «ХАІ», p.v.brysin@khai.edu

Лукін Володимир Васильович, завідувач кафедри інформаційно-комунікаційних технологій ім О.О. Зеленського, НАУ «ХАІ», д.т.н., v.lukin@khai.edu

Секція 2

АНАЛІЗ І ЗАБЕЗПЕЧЕННЯ ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ HMI-LLM-СИСТЕМ

Васик Д. В.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Харченко В. С.

Актуальність. Сучасні людино-машинні системи (human-machine interaction, HMI) із взаємодією через великі мовні моделі (LLM) забезпечують не лише збір і обробку даних, але й керування пристроями (рівень операційних технологій).

Інтеграція LLM у HMI-системи призводить до безпекових ризиків: модель може неправильно інтерпретувати природно-мовну команду, формувати некоректне рішення при керуванні, створюва-ти ситуацію, коли пристрій діє непередбачено і порушується цілісність чи доступ до даних. Тому виникає потреба у аналізі загроз та механізмів захисту безпеки HMI-систем, які включають LLM (HMI-LLM-систем).

Метою дослідження підвищення функційної безпечності HMI-LLM-систем шляхом:

по-перше, аналізу специфічних загроз та наслідків атак на LLM-активи;

по-друге, обґрунтування вибору контрзаходів щодо їх запобігання в контексті управління пристроями, збору телеметрії та людино-машинної взаємодії в HMI-LLM-системах.

Аналіз існуючих рішень виконано за напрямами:

– HMI-LLM-системи як об’єкти регулювання функційної безпечності та кібербезпеки (з урахуванням NIST AI RMF) [1];

– методи оцінювання функційної безпечності, зокрема формальні й напівформальні підходи, засновані на Security Informed Safety [2], моделях якості штучного інтелекту та кібербезпеки LLM [3];

– контрзаходи для забезпечення безпеки та критерії їх вибору.

Виявлено, що наявні методи оцінювання ризиків і контролю AI-модулів мають обмеження й не гарантують повної відповідності стандартам безпеки.

Основні положення. Запропоновано кілька принципів, які формують системну модель безпеки, і рекомендації щодо їх реалізації шляхом:

– чіткого архітектурного розділення між HMI/LLM і критичними пристроями;

– застосування принципу найменших прав і людського контролю при ключових рішеннях;

– моніторинг дій системи з автоматизованою верифікацією та можливістю ручного втручання.

Описано таксономічну модель безпеки та метод оцінювання контрзаходів за метриками: частота небезпечних дій і хибних спрацювань, витрати ресурсів та вплив на продуктивність і реактивність системи керування.

Висновки. Основним науковим результатом дослідження є сукупність принципів та метрик для оцінювання функційної безпечності та вибору контрзаходів для забезпечення вимог до безпеки HMI-LLM-систем. Подальші кроки досліджень можуть бути пов'язані із створенням відповідної системи підтримки прийняття рішень при їх розробленні.

Список літератури

1. M. Harter, "LLM Assisted No-code HMI Development for Safety-Critical Systems: Insights of a Short Empirical Study",(CENTRIC 2023), Valencia, Spain, Nov. 13-17, 2023, pp. 8-18

2. O. Illiashenko, V. Kharchenko, I. Babeshko, H. Fesenko, F. Di Giandomenico, Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection. *Entropy.* 25.8, 1123. 2023. P.1-35. DOI:10.3390/e25081123

3. V. Kharchenko, H. Fesenko, O. Illiashenko, Quality Models for Artificial Intelligence Systems: Characteristic-Based Approach, Development and Application, *Sensors*, 22.13, 4865(2022). P. 1-32. DOI: 10.3390/s22134865.

4. O. Neretin, V. Kharchenko. A model of ensuring LLM cybersecurity. Radioelectronic and Computer Systems, 2025 (2) p. 201–215, DOI: https://doi.org/10.32620/reks.2025.2.13

Відомості про авторів

Васик Дмитро Володимирович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.v.vasyk@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

ПИТАННЯ ІНТЕГРАЦІЇ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ПРИНЦИПІВ ЦИРКУЛЯРНОЇ ЕКОНОМІКИ В УПРАВЛІННІ ВІДХОДАМИ

Васильчук М. В.
Київський національний університет імені Тараса Шевченка, Київ, Україна
Науковий керівник: Заславський В. А.

Актуальність. Глобальне виробництво відходів зростає і, за прогнозами, досягне 3.8 мільярдів тонн до 2050 року. У відповідь світовим трендом стає циркулярна економіка, що розглядає відходи як цінні вторинні ресурси [1].

Однак малі та середні підприємства стикаються з серйозними перешкодами при впровадженні цих принципів. Ключовими бар'єрами є брак знань про циркулярну економіку та відсутність технічних навичок у персоналу.

Цей інформаційний розрив є критичним: відсутність інформації щодо можливостей утилізації та наступної переробки створює загрози функціональній безпеці, призводячи до промислових інцидентів, та екологічній безпеці через забруднення, що суперечить принципам зеленої економіки.

Паралельно ці ж прогалини у знаннях унеможливлюють ефективне використання вторинних ресурсів на підприємствах [2].

Мета. Розробити інформаційно аналітичний прототип цифрового інтерактивного засобу, здатного на основі текстового запиту користувача агрегувати та структурувати складні нормативні вимоги. Кінцевою метою є надання чітких, практичних рекомендацій, що поєднують протоколи безпечного поводження з можливостями вторинного використання відходів.

Основні положення. В основі прототипу лежить репрезентативна вибірка тестових знань, що ілюструє агрегацію національних, міжнародних стандартів та галузевих протоколів безпеки[3]. Система аналізує текстовий запит користувача відносно цієї бази даних та формує комплексний аналітичний документ, що включає:

- класифікацію відходу та опис пов'язаних небезпек;
- рекомендації з функціональної безпеки (зберігання, поводження, транспортуваннят відходів);

– аналіз потенціалу в рамках циркулярної економіки (сфери використання);

– ідентифікацію потенційних партнерів або галузей, зацікавлених у даному вторинному ресурсі.

Висновки. Розроблено програмний прототип цифрового інтерактивного засобу, що структурує складні нормативні дані у практичні рекомендації, інтегруючи аналіз ризиків функціональної безпеки з ідентифікацією економічних можливостей циркулярної економіки. Такий підхід надає інструмент для мінімізації ризику людської помилки та підтримує впровадження безпечних і сталих практик поводження з відходами.

Список літератури

1. Global Waste Management Outlook 2024: Beyond an age of waste – Turning rubbish into a resource / United Nations Environment Programme (UNEP). Nairobi: UNEP, 2024. P. 196. URL: https://wedocs.unep.org/bitstream/handle/20.500.11822/44939/global_waste_management_outlook_2024.pdf?sequence=3 (дата звернення: 23.10.2025)

2. Implementation of Circular Economy Business Models by Small and Medium-Sized Enterprises (SMEs): Barriers and Enablers / V. Rizos та ін. // Sustainability. 2016. Vol. 8, no. 11. Art. 1212. DOI: https://doi.org/10.3390/su8111212

3. Volkovitch V., Zaslavsky V., Franchuk O. A decision making support system for marketing "SPRUT" // Information Infrastructure for free Market Societies in Transition Eds. V.M. Shalamanov and T.D. Tagarev Proc. AFCEA-Europe (Sofia Seminar 26-28 April, 1995) - P.55-56

Відомості про авторів

Васильчук Микола Володимирович, магістр кафедри математичної інформатики факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка, nikolay_vsk@knu.ua

Заславський Володимир Анатолійович, професор кафедри математичної інформатики факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка, д.т.н., професор, zaslavskiy.volodymyr@knu.ua

Секція 2

МОБІЛЬНИЙ ЗАСТОСУНОК ДЛЯ НАДІЙНОГО ТА БЕЗПЕЧНОГО УПРАВЛІННЯ КРИПТОВАЛЮТНИМ ПОРТФОЛІО

Закладний О. О.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Клюшніков І. М.

Актуальність. Криптовалюти сьогодні займають важливе місце у світовій фінансовій системі [1]. Вони використовуються не лише як інвестиційний актив, але й для розрахунків у різних сферах. Попри зростання популярності, управління криптовалютним портфелем залишається складним завданням через високу волатильність ринку. Більшість існуючих мобільних застосунків для відстеження портфеля мають перевантажений функціонал, рекламу або надмірну кількість сервісів, що ускладнює роботу користувача. Це обумовлює потребу у простому, зручному та функціональному інструменті для моніторингу ринку та аналізу інвестиційної доходності вкладень, щоб забезпечити функційну надійність та безпечність операцій.

Метою даної роботи є забезпечення надійного та та безперебійного доступу до даних криптовалютного ринку для зменшення імовірності фінансових втрат.

На даний момент більшість фінансових проєктів, що працюють із цифровими активами, передбачають отримання, обробку та збереження даних у межах централізованих або децентралізованих платформ, тоді як користувацьке програмне забезпечення виступає інтерфейсом взаємодії із цими системами. Реалізація мобільних застосунків для моніторингу та управління криптовалютним портфоліо стала одним із сегментів фінансових технологій, оскільки вони забезпечують постійний доступ користувача до ринку та дозволяють оперативно приймати інвестиційні рішення.

Основні положення. Розвиток ринку криптовалют супроводжується постійним збільшенням обсягів даних, що потребують обробки та зберігання. Для мобільних застосунків, які забезпечують управління портфелем та моніторинг курсів популярних монет, критично важливо гарантувати швидкий доступ до інформації, відмовостійкість і безпеку даних користувачів. Хмарні технології дозволяють інтегрувати масштабовану обробку даних у реальному часі. Інформація про курси

валют, обсяги торгів, ринкові індекси та новинні стрічки надходить через API, а хмарна інфраструктура забезпечує її зберігання, агрегацію та синхронізацію. Мобільний додаток при цьому виконує роль клієнтського інтерфейсу. Водночас використання хмарних сервісів має виклики: ризик залежності від одного провайдера (vendor lock-in), правові аспекти обробки фінансових даних та потенційне збільшення витрат при різкому зростанні навантажень. Таким чином, хмарні провайдери є ключовим елементом мобільних додатків для управління криптовалютним портфоліо, забезпечуючи швидкий доступ до даних, надійність і безпеку, а розробникам – можливість зосередитися на інтерфейсі та аналітичних функціях для користувачів.

Було проведено аналіз існуючих рішень (Binance, CoinStats, Delta) [2, 3, 4], що виявив перевантаженість застосунків другорядним функціоналом. На основі цього обрано концепцію мінімалістичного застосунку. Для реалізації використано трирівневу архітектуру, що включає клієнтську частину (мобільний застосунок), сервер (отримання та обробка даних з API) та базу даних (збереження інформації про користувачів, портфелі та транзакції). Це рішення дозволяє масштабувати систему, забезпечу надійність, гнучкість і підвищує рівень функціональної безпеки.

Висновки. Використання мобільних застосунків для управління криптовалютним портфоліо дозволяє реалізувати баланс між зручністю інтерфейсу та ефективністю роботи з даними, забезпечуючи надійність, актуальність і високу швидкість обробки інформації.

Список літератури

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. 9 p. DOI: http://dx.doi.org/10.2139/ssrn.3440802
2. Track All Your Wallets & Exchanges From One Place. CoinStats. URL – https://coinstats.app (дата звернення: 18.11.2025).
3. Binance App. *Binance*. URL – https://www.binance.com (дата звернення: 18.11.2025)
4. Delta Investment Tracker. Delta. URL – https://delta.app (дата звернення: 18.11.2025)

Відомості про авторів

Закладний Олег Олексійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.zakladnyi@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@csn.khai.edu

Section 2

USING MACHINE LEARNING METHODS TO PREDICT FAILURES AND ENSURE THE FUNCTIONAL SAFETY OF SMART HOME SUBSYSTEMS WHEN CLIMATIC CONDITIONS CHANGE

Danylo Kirichenko
University of Duisburg-Essen, Duisburg, Germany
Scientific adviser: Heorhii Zemlianko

Relevance. The introduction of smart home technologies is growing rapidly, integrating complex interconnected subsystems (HVAC, power supply, lighting) into everyday life, but these systems are focused on comfort and efficiency, remain critically vulnerable to natural disasters and extreme climate events, highlighting the need for adaptive modelling to improve system resilience [1]. Functional safety remains a key concern, and traditional methods of reliability analysis often prove insufficient in dynamic and unpredictable conditions [2]. This provides significant opportunities for machine learning to analyse large flows of system data and transition from reactive maintenance to predictable security measures aimed at reducing vulnerability to global climate change [3,4].

The purpose of this work is to develop and validate a predictive failure model using machine learning techniques. The primary goal is to enhance the functional safety of critical smart home subsystems, such as heating and energy supply. This model is specifically designed to forecast subsystem failures by correlating operational data with changing climatic conditions, thereby addressing a significant safety and reliability gap noted in recent studies [1].

Principal provisions. The study focuses on analyzing the reliability and operational continuity of essential life-support subsystems (heating, ventilation, energy supply). The core methodology involves collecting and integrating a combined dataset, featuring internal system logs (e.g., sensor readings, error codes) and external climatic data (e.g., temperature, humidity, storm warnings). Machine learning models – potentially including LSTMs for time-series analysis or federated learning frameworks for privacy – are then trained on this data [5]. These models are designed to identify subtle patterns and correlations that precede failures and to predict their probability in real-time. The key contribution is the development of robust algorithms that leverage these failure predictions. When the model forecasts a high probability of failure, it automatically triggers a pre-defined safety protocol, such as transitioning the subsystem into a safe-fail state or alerting occupants, thus preventing catastrophic failure and ensuring resident well-being. This approach provides the dynamic adaptability and resilience that current smart home systems often lack [1,2].

Conclusions. This research demonstrates that machine learning offers a viable and powerful solution to the significant vulnerabilities of modern smart homes, particularly in the context of emergency situations and climate-driven stress. By proactively identifying and predicting failures linked to external climatic data, the proposed framework can significantly enhance functional safety. It ensures the resilience and continuous operation of essential home services when they are needed most. This proactive, data-driven approach is a critical step toward developing the next generation of truly adaptive and safe smart homes, which are capable of anticipating risks and protecting occupants from new climate-related challenges.

List of references

1. D. Kirichenko and H. Zemlianko, "Smart home subsystems during emergency situations", *Proceedings of the International Scientific Conference "Modern Trends in the Development of Science and Society"*, 2023. DOI: https://doi.org/10.64076/iedc251023.02

2. N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments", in *IEEE Access*, vol. 9, pp. 121975-121995, 2021, DOI: 10.1109/ACCESS.2021.3109886

3. A. A. Saleem, M. M. Hassan and I. A. Ali, "Smart Homes Powered by Machine Learning: A Review", 2022 International Conference on Computer Science and Software Engineering (CSASE), Duhok, Iraq, 2022, pp. 355-361, DOI: 10.1109/CSASE51777.2022.9759682

4. Bazazzadeh, H. ., Nadolny, A. ., & Safaei, S. S. H. . (2021). Climate Change and Building Energy Consumption: A Review of the Impact of Weather Parameters Influenced by Climate Change on Household Heating and Cooling Demands of Buildings. *European Journal of Sustainable Development*, *10*(2), 1. DOI: https://doi.org/10.14207/ejsd.2021.v10n2p1

5. N. Pape and C. Mansour, "Edge Machine Learning to Detect Malicious Activity in IoT Devices through System Calls and Traffic Analysis," *2023 International Conference On Cyber Management And Engineering (CyMaEn)*, Bangkok, Thailand, 2023, pp. 123-127, DOI: 10.1109/CyMaEn57228.2023.10051091

Information about the authors

Danylo Kirichenko, a master`s student from the Department of General Computer Science, danylo.kirichenko@stud.uni-due.de

Heorhii Zemlianko, associate professor from the Department of Computer Systems, Networks and Cybersecurity, NAU «KhAI», PhD in Cybersecurity, g.zemlynko@csn.khai.edu

Секція 2

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ПРОТОКОЛІВ ОБМІНУ ДАНИМИ В СИСТЕМАХ IIOT

Любченко М. С.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Бабешко Є. В.

Актуальність. Сучасний розвиток Промислового Інтернету речей (IIoT) характеризується конвергенцією інформаційних (IT) та операційних (OT) технологій. Історично промислові протоколи розроблялися для ізольованих мереж, де захист базувався на принципі фізичної ізоляції («повітряний зазор» або «air gap»). Однак підключення OT-систем до глобальних мереж виявило фундаментальну вразливість класичних протоколів, таких як Modbus та IEC 60870-5-104, які є «небезпечними за задумом» (insecure-by-design) [1]. Конфлікт пріоритетів тріади безпеки (CIA) в IT та OT вимагає перегляду підходів до захисту даних, оскільки стандартні IT-рішення не завжди застосовні до критичної інфраструктури.

Метою є аналіз сучасних технологій безпеки основних протоколів обміну даними в IIoT (Modbus, IEC 60870-5-104, MQTT, OPC UA) та визначення ефективних методів їх захисту в умовах гетерогенних систем.

Основні положення. У ході роботи було проаналізовано еволюцію підходів до безпеки промислових протоколів. Виявлено, що протоколи Modbus TCP та IEC 60870-5-104 не мають вбудованих механізмів шифрування та автентифікації, передаючи дані у відкритому вигляді. Це робить їх вразливими до атак типу Man-in-the-Middle та ін'єкцій команд. Сучасним рішенням для них є підхід «Security-by-Encapsulation» (безпека через інкапсуляцію). Наприклад, стандарт Modbus Security (2018) пропонує інкапсуляцію PDU в тунель TLS (порт 802) з використанням сертифікатів X.509 [2]. Аналогічно, для IEC 104 застосовується стандарт IEC 62351-3, що забезпечує шифрування транспортного рівня та автентифікацію повідомлень [3]. Протокол MQTT використовує модель «Secure-by-Implementation». Безпека не є вбудованою, а залежить від реалізації брокера та використання транспортного шифрування (MQTTS/TLS) разом зі списками контролю доступу (ACL) для авторизації на рівні топіків [4]. Найвищий рівень захисту демонструє OPC UA, побудований за принципом «Secure-by-Design». Він пропонує багаторівневу модель безпеки, яка включає окремі шари для автентифікації додатків (SecureChannel) та

користувачів (Session), а також гранулярну авторизацію доступу до кожного вузла адресної моделі [5].

Висновки. Забезпечення безпеки в IIoT вимагає диференційованого підходу. Для застарілих протоколів (Modbus, IEC 104), які неможливо модернізувати на рівні кінцевих пристроїв через обмежені ресурси, доцільним є використання комунікаційних шлюзів. Такі шлюзи виконують роль бар'єру безпеки, термінуючи незахищені з'єднання в локальному сегменті та передаючи дані на верхній рівень через захищені протоколи (OPC UA або MQTTS). Це підтверджує необхідність розроблення спеціалізованих шлюзів, здатних не лише конвертувати дані, а й забезпечувати їх цілісність та конфіденційність.

Список літератури

1. A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities. MDPI. 2023. URL – https://www.mdpi.com/1424-8220/23/17/7470 (дата звернення: 11.11.2025).
2. Enhanced Modbus/TCP Security Protocol: Authentication and Authorization Functions Supported. PubMed Central. 2022. URL – https://pmc.ncbi.nlm.nih.gov/articles/PMC9607043 (дата звернення: 11.11.2025)
3. IEC 62351: Secure communication in the energy industry. COPA-DATA Blog. URL – https://blog.copadata.com/iec-62351-secure-communication-in-the-energy-industry (дата звернення: 11.11.2025)
4. Authorization in MQTT: Using ACLs to Control Access to MQTT Messaging. EMQX. URL – https://www.emqx.com/en/blog/authorization-in-mqtt-using-acls-to-control-access-to-mqtt-messaging (дата звернення: 11.11.2025)
5. Practical Security Recommendations for building OPC UA Applications. OPC Foundation. URL – https://opcfoundation.org/wp-content/uploads/2017/11/OPC-UA-Security-Advise-EN.pdf (дата звернення: 11.11.2025)

Відомості про авторів

Любченко Максим Сергійович, магістрант кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.liubchenko@student.csn.khai.edu
Бабешко Євген Васильович, доцент кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., e.babeshko@csn.khai.edu

Секція 2

ЗАСТОСУВАННЯ СІАМСЬКИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ПІДВИЩЕННЯ НАДІЙНОСТІ СИСТЕМ ВИЯВЛЕННЯ МАНІПУЛЯЦІЙ ІЗ ЗОБРАЖЕННЯМИ

Нікітін А. О.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Шостак А. В.

Актуальність. Швидке зростання кількості атак, пов'язаних із підміною візуального контенту, зокрема за допомогою deepfake-технологій, створює серйозні ризики для безпеки інформаційних систем. Фальсифіковані зображення можуть використовуватися для кібершантажу, підриву репутації, створення фальшивих доказів, а також обходу систем автентифікації, що базуються на біометричних даних. Тому зростає потреба у методах, здатних точно вимірювати ступінь схожості зображень і виявляти штучні модифікації. Перспективним підходом для вирішення цього завдання є використання сіамських нейронних мереж (Siamese Neural Networks, SNN), які дозволяють порівнювати пари зображень та визначати факт підміни із високою точністю [1-3].

Метою роботи є дослідження можливостей застосування сіамських нейронних мереж для автоматичного виявлення підроблених або модифікованих зображень у контексті забезпечення кібербезпеки, включно з аналізом метричних просторових ознак, побудовою стійких embedding-представлень та оцінкою ефективності SNN у протидії сучасним атакам, таким як deepfake-генерація, локальні маніпуляції та підміна візуальних даних.

Основні положення. У роботі розглянуто побудову обчислювального ядра SNN, що складається з двох ідентичних CNN-енкодерів, які генерують векторні представлення зображень. Для порівняння отриманих embedding-векторів застосовано функцію контрастивної відстані, що дозволяє кількісно оцінити рівень схожості та визначати наявність маніпуляцій. Використання функції втрат Triplet Loss підвищує стабільність навчання моделі за рахунок формування семантичних кластерів «оригіналів» та «підробок» [4]. Експериментальна частина роботи передбачала розроблення та навчання моделі з використанням датасетів, що містять пари автентичних та підроблених зображень, у тому числі deepfake-матеріалів. Результати показали, що SNN демонструє значно вищу точність при виявленні маніпуляцій порівняно з класичними підходами, які використовують порогові значення або ручні ознаки. Високий рівень узагальнення забезпечує можливість застосування моделі в реальних умовах, включаючи моніторинг соцмереж, юридичний аналіз цифрових доказів та захист облікових записів. Наукова новизна полягає у

застосуванні глибоких сіамських архітектур для задач кібербезпеки, зокрема для виявлення добудованих або штучно модифікованих зображень. Комбінація CNN-енкодера, порівняльної підмережі та Triplet Loss дозволила отримати стійку модель, здатну визначати навіть мінімальні спотворення, характерні для сучасних deepfake-систем [2]. Сіамські нейронні мережі здатні підвищувати надійність процесів цифрової криміналістики, зокрема у завданнях ідентифікації джерела зображення, виявлення локальних маніпуляцій та оцінки ступеня схожості між оригінальними й модифікованими зразками. Крім того, SNN можуть застосовуватися в автоматизованих системах контролю доступу для перевірки автентичності фотографій користувачів або попередження підміни облікових записів.

Висновки. Сіамські нейронні мережі є ефективним інструментом для виявлення маніпуляцій із зображеннями та протидії deepfake-атакам. Завдяки здатності моделі порівнювати високорівневі семантичні ознаки та генерувати стійкі векторні представлення, SNN забезпечують високий рівень точності та надійності при класифікації зображень за ознакою автентичності. Отримані результати підтверджують доцільність інтеграції SNN у сучасні системи кіберзахисту, зокрема у підсистеми моніторингу контенту, автоматичного виявлення візуальних підробок та цифрової криміналістики.

Список літератури

1. S. Chopra, R. Hadsell and Y. LeCun, "Learning a similarity metric discriminatively, with application to face verification," 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), San Diego, CA, USA, 2005, pp. 539-546 vol. 1, DOI: 10.1109/CVPR.2005.202

2. F. Schroff, D. Kalenichenko and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering", in 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 2015, pp. 815-823, DOI: 10.1109/CVPR.2015.7298682

3. Goodfellow I. et al. Deep Learning. MIT Press, 2016. URL – http://www.deeplearningbook.org (дата звернення: 04.11.2025)

4. Omkar M. Parkhi, Andrea Vedaldi and Andrew Zisserman. Deep Face Recognition. In Xianghua Xie, Mark W. Jones, and Gary K. L. Tam, editors, Proceedings of the British Machine Vision Conference (BMVC), pages 41.1-41.12. BMVA Press, September 2015. DOI: https://dx.doi.org/10.5244/C.29.41

Відомості про авторів

Нікітін Андрій Олексійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.nikitin@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

АНАЛІЗ КІБЕРБЕЗПЕКОВИХ ВИКЛИКІВ В ЗАСТОСУВАННІ БПЛА У ЦИВІЛЬНІЙ ТА БЕЗПЕКОВІЙ СФЕРАХ

Олейников Є. О.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Харченко В. С.

Актуальність. Сучасний етап розвитку безпілотних літальних апаратів (БПЛА) характеризується швидким переходом від військового до цивільного застосування. Дрони активно використовуються у сферах моніторингу навколишнього середовища, логістики, пошуково-рятувальних операцій, спостереження за інфраструктурою, а також у забезпеченні громадської безпеки. Завдяки здешевленню технологій та розвитку штучного інтелекту, БПЛА стали ключовими інструментами у підвищенні ситуаційної обізнаності, оперативності реагування та зниженні ризиків для персоналу. Водночас, розширення зон використання дронів створює нові загрози у сфері кібербезпеки, що потребують комплексного аналізу та розробки єдиних підходів до захисту систем керування [1-3].

Метою даної роботи є дослідження кібербезпекових ризиків, пов'язаних із функціонуванням систем БПЛА у цивільних та державних сферах, а також аналіз методів захисту від сучасних кіберзагроз, що впливають на конфіденційність, цілісність і доступність даних безпілотних систем.

Основні положення. Розширення функціональності БПЛА супроводжується збільшенням кіберзалежності та кількості можливих точок атаки. Згідно з дослідженнями, найпоширенішими є три категорії кібератак: перехоплення – спрямовані на порушення конфіденційності переданих даних; модифікація або фальсифікація – порушують цілісність системи; порушення доступності – спричиняють відмову або зупинку сервісів [4]. Для протидії цим загрозам застосовуються методи криптографічного захисту, захищеної маршрутизації та підвищення стійкості мережевих зв'язків. Перспективними напрямами є використання технологій блокчейну та машинного навчання для створення адаптивних механізмів кіберзахисту. Водночас, як показує огляд, інтеграція БПЛА у цивільні сфери (моніторинг, пошук і рятування, логістика) створює необхідність одночасного врахування питань безпеки польотів, надійності систем зв'язку та інформаційної безпеки [5]. Формування уніфікованих

методологій аналізу ризиків сприятиме розвитку кіберстійких дронових систем у майбутньому.

Висновки. БПЛА стали невід'ємною частиною сучасних безпекових і цивільних інфраструктур. Однак із зростанням рівня автономності та мережевої взаємодії підвищуються ризики кібератак, здатних паралізувати роботу систем або скомпрометувати дані. Комплексний підхід до кіберзахисту, заснований на принципах криптографії, машинного навчання та розподілених технологій, є необхідною умовою для забезпечення надійності та стійкості безпілотних платформ.

Список літератури

1. Ruslan Demura, Vyacheslav Kharchenko, Vitaly Levashenko, "Cybersecurity of UAV Swarm Communication using VPN and RIS Technologies Integration: Protected Assets, IMECA Analysis and Countermeasures", DESSERT 2024, December 2024, pp. 1. DOI: https://doi.org/10.1109/DESSERT65323.2024.11122116

2. Heorhii Zemlianko, Vyacheslav Kharchenko, "Cybersecurity Risk Analysis of Multifunctional UAV Fleet Systems: A Conceptual Model and IMECA-Based Technique", Radioelectronic and Computer Systems, December 2023. DOI: https://doi.org/10.32620/reks.2023.4.11

3. Niyonsaba S., Konate K., & Soidridine M. M. A Survey on Cybersecurity in Unmanned Aerial Vehicles: Cyberattacks, Defense Techniques and Future Research Directions. International Journal of Computer Networks and Applications, 2023, vol. 10, no. 5, pp. 688-701

4. Illiashenko O., Kharchenko V., Babeshko I., Fesenko H., & Di Giandomenico F. Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection. Entropy, 2023, vol. 25, article no. 1123

5. Pevnev V. Ya., Toryanyk V. V., & Kharchenko V. S. Cybersecurity of Wireless Smart Systems: Interference Channels and Radio Frequency Vulnerabilities. Radioelectronic and Computer Systems, 2020, no. 4, pp. 79-92. DOI: https://doi.org/10.32620/reks.2020.4.07

Відомості про авторів

Олейников Єгор Євгенійович, аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.oleinykov@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

ВИКОРИСТАННЯ НЕТИПОВИХ DCT-КОДЕРІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ МЕДИЧНИХ ЗОБРАЖЕНЬ

Пліско О. О.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Кривенко С. С.

Актуальність. Розвиток телемедицини і збільшення обсягів медичних даних породжують нові виклики щодо гарантування конфіденційності зображень пацієнтів. Медичні діагностичні зображення (КТ, МРТ, рентген та ін.) містять чутливу інформацію і потребують надійного захисту. Стандартні методи стиснення, такі як JPEG або JPEG2000, забезпечують ефективне зменшення обсягів інформації, але їх відкрита технічна документація та доступність декодерів дозволяють будь-кому відтворити вихідне зображення [1]. Це створює потенційні ризики несанкціонованого доступу до конфіденційної медичної інформації. Тому важливо шукати такі методи стиснення, які не просто ефективно зменшують обсяг даних, але й додають рівень безпеки. Цього можна досягти, наприклад, за рахунок складної структури самого алгоритму або того, що він не є загальновідомим.

Метою даної роботи є дослідження здатності деяких DCT-кодерів стискати медичні зображення, одночасно забезпечуючи високу візуальну якість декомпресованих зображень та підвищений рівень конфіденційності даних. Для оцінки ефективності обраних кодерів використовується метрика PSNR-HVS-M, оскільки вона враховує особливості людського сприйняття візуальних спотворень [2].

Основні положення. Для аналізу було розглянуто стандартні та нестандартні підходи до стиснення медичних зображень. Стандартні методи, такі як JPEG і JPEG2000, широко застосовуються в медичних інформаційних системах через простоту інтеграції та сумісність з форматами DICOM. Але їхня відкритість дозволяє легко відтворити зображення, що підвищує ризики витоку даних. На відміну від них, DCT-кодери, такі як ADCTC та AGU/AGU-MHV, використовують удосконалені алгоритми обробки блоків, побітового кодування та контекстного моделювання, що дозволяє досягати кращого співвідношення між ступенем стиснення та якістю відновлення [1]. Дослідження показали, що

кодери ADCT та AGU можуть стискати медичні зображення набагато ефективніше, ніж добре відомий формат JPEG2000, не втрачаючи при цьому їхньої візуальної якості. Результати, підтверджені на медичних наборах даних [3], доводять значний потенціал цих кодерів. Метрика PSNR-HVS-M продемонструвала свою ефективність як інструмент оцінки якості, оскільки враховує властивості зорової системи людини та корелює із суб'єктивним сприйняття [2]. Таким чином, використання маловідомих (але ефективних) або внутрішніх форматів може виступати додатковим рівнем технічного захисту медичних даних поряд із традиційними криптографічними методами [3,4].

Висновки. Використання нестандартних DCT-кодерів, таких як ADCT, AGU та їх модифікацій, є перспективним напрямом для підвищення безпеки та ефективності зберігання медичних зображень. Ці кодери чудово стискають дані та забезпечують високу візуальну якість. Водночас вони самі по собі слугують захистом, адже ті, хто не мають декодерів, не в змозі декодувати такий файл. В подальшому, щоб забезпечити великий рівень безпеки в системах зберігання медичних зображень можна поєднати ці методи з традиційними криптографічними засобами захисту, такими як шифрування файлів та метаданих. Це дозволить не тільки зменшити обсяг даних, а й підвищити рівень конфіденційності, що особливо важливо для медичних систем.

Список літератури

1. Ponomarenko N. N., Lukin V. V., Egiazarian K., Astola J. ADCTC: Advanced DCT-based image coder. Proc. of LNLA, 2008. – P. 83–94

2. PSNR-HVS-M: Peak Signal-to-Noise Ratio taking into account HVS masking. Ponomarenko N. N. URL – http://www.ponomarenko.info/psnrhvsm.htm (дата звернення: 05.11.2025)

3. Lukin V., Kryvenko L., et al. *Visually lossless compression of dental images. Advanced Optical Technologies (Frontiers)*, 2024, Article 1306142. DOI: https://doi.org/10.3389/aot.2024.1306142

4. Krivenko S. *Smart lossy compression of images based on distortion prediction*. KNMU Technical Report, 2018. DOI: 10.1615/TelecomRadEng.v77.i17.40

Відомості про авторів

Пліско Олег Олегович, аспірант кафедри інформаційно-комунікаційних технологій ім О.О. Зеленського, НАУ «ХАІ», o.o.plisko@student.khai.edu

Кривенко Сергій Станіславович, старший науковий співробітник кафедри інформаційно-комунікаційних технологій ім О.О. Зеленського, НАУ «ХАІ», к.т.н., s.kryvevnko@khai.edu

Секція 2

РОЗРОБКА ВЛАСНОГО ЕКСПОРТУ ТА ПОСТОБРОБКИ ДАНИХ OPENSTREETMAP ДЛЯ ГЕОПРОСТОРОВОГО ЗІСТАВЛЕННЯ АДРЕС

Сатановський Д. В.
Київський національний університет імені Тараса Шевченка Науковий, м. Київ, Україна
Науковий керівник: Заславський В. А.

Актуальність. Адресні дані є ключовим елементом геоінформаційних систем, що забезпечують роботу навігаційних, муніципальних та логістичних сервісів, які необхідні для бізнесу та кінцевих клієнтів. Вони відіграють центральну роль у прийнятті рішень, плануванні маршрутів, реагуванні на надзвичайні ситуації та функціонуванні критичних систем[1], де навіть незначна похибка в адресі може призвести до значних наслідків для безпеки та ефективності роботи. Відкриті дані OpenStreetMap (OSM) дають змогу створювати просторові бази, однак їх якість і консистентність залежать від активності спільноти [2]. Це призводить до дублювання назв, помилкових координат і неузгодженості форматів. Тому актуальною є побудова надійного процесу власного експорту, що забезпечить їх структурованість і валідність.

Метою є розробка програмного рішення для експорту й постобробки даних OSM, який включає відбір лише адресних сутностей, збереження геометрії, побудову адміністративної ієрархії, нормалізацію назв і валідацію змін. Рішення орієнтоване на застосування в системах геоматчингу та автоматичного зіставлення даних з різних джерел [3].

Основні положення. Програмне рішення реалізоване за допомогою інструментів Imposm і PostGIS, що забезпечують повний цикл експорту, трансформації й контролю якості. Imposm виконує фільтрацію дампів OSM (.pbf) за тегами addr:*, building=*, highway=*, boundary=administrative. Дані завантажуються у PostGIS, де через функції ST_Contains і ST_Within формується ієрархія «будинок → вулиця → населений пункт → область». Нормалізація виконується Python-модулями libpostal та unidecode, що уніфікують формат написання, виправляють скорочення та дублікати [4]. Для забезпечення функціональної безпеки система аналізує журнали редагувань (changesets), виявляючи масові перейменування, зміни геометрії чи видалення об’єктів, що можуть свідчити про потенційно некоректні правки. Запропонована архітектура є модульною: етапи експорту, нормалізації, перевірки та формування адресної бази реалізовано

як незалежні компоненти. Подальший розвиток передбачає інтеграцію алгоритмів машинного навчання – моделей BERT для семантичного зіставлення назв і підвищення точності геоматчингу [5].

Висновки. Розроблене рішення забезпечує структуровану й перевірену бази адресних даних на основі OpenStreetMap. Поєднання процедур фільтрації, нормалізації й контролю змін формує основу для точного геопросторового зіставлення та підвищує надійність використання відкритих даних у критичних інформаційних системах. Запропонована архітектура забезпечує відтворюваність процесу, масштабованість і можливість розширення під специфіку будь-якої країни чи міста. Подальші дослідження спрямовуватимуться на інтеграцію моделей глибинного навчання для семантичного зіставлення назв.

Список літератури

1. Alexei A. Gaivoronski, Pavel S. Knopov, Vladimir I. Norkin, Volodymyr A. Zaslavskyi. Stochastic Modeling and Optimization Methods for Critical Infrastructure Protection. ISTE Ltd, London, UK; John Wiley&Sons, Inc.Hoboken, USA, 2025, 261 p

2. Li D., Gamage D., Peng S. Mapping the Completeness and Positional Accuracy of OpenStreetMap Road Data at the County Level in the Contiguous United States // Transactions in GIS. – 2025. – DOI: 10.1111/tgis.70077

3. Kilic B., Hacar M., Gülgen F. Effects of reverse geocoding on OpenStreetMap tag quality assessment // Transactions in GIS. – 2023. – Vol. 00. – P. 1–15. DOI: 10.1111/tgis.13089

4. Hristov E., Petrova-Antonova D., De Paoli F. Geospatial Data Enrichment through Address Geocoding: Challenges and Solutions // The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. – 2024. – XLVIII-4. – С. 239–245. DOI: 10.5194/isprs-archives-XLVIII-4-2024-239-2024

5. Devlin J., Chang M.-W., Lee K., Toutanova K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. arXiv:1810.04805, 2019. URL: https://arxiv.org/abs/1810.04805

Відомості про авторів

Сатановський Дмитро Володимирович, аспірант факультету комп'ютерних наук та кібернетики, Київський національний університет імені Тараса Шевченка, satandmytro@gmail.com

Заславський Володимир Анатолійович, професор кафедри математичної інформатики факультету комп'ютерних наук та кібернетики, Київський національний університет імені Тараса Шевченка, д.т.н., професор, zaslavskyi.volodymyr@knu.ua

Секція 2

ДОСЛІДЖЕННЯ ТА РОЗРОБЛЕННЯ ВЕБСИСТЕМИ ОБРОБКИ ЗАЯВОК СЛУЖБИ ПІДТРИМКИ З АВТОМАТИЧНОЮ КЛАСИФІКАЦІЄЮ ТА КОНТРОЛЕМ SLA

Сорокін В. В.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Клюшніков І.М.

Актуальність. У сучасних інформаційних системах кількість користувацьких звернень постійно зростає, що ускладнює своєчасне реагування та підтримання високої якості обслуговування й забезпечення функційній надійності. Традиційні help desk-рішення, засновані на ручній класифікації заявок і відсутності автоматизованого контролю SLA (Service Level Agreement), характеризуються низькою масштабованістю, залежністю від людського фактору та ризиком порушення термінів виконання [1]. Це знижує стабільність роботи сервісу, ефективності процесів технічної підтримки та може призводити до переривання бізнес-процесів.

Функційна надійність системи технічної підтримки визначається її здатністю забезпечувати безперервну та надійну роботу навіть за умов підвищеного навантаження.

Використання методів машинного навчання для автоматичної класифікації звернень у поєднанні з моніторингом SLA дозволяє підвищити надійність, стійкість і контрольованість програмно-технічних комплексів служби підтримки [2,3].

Мета. Розроблення вебсистеми обробки заявок служби підтримки, що реалізує автоматичну класифікацію звернень користувачів і контроль показників SLA для підвищення функційної надійності, безпечності, стабільності та ефективності процесів технічної підтримки.

Основні положення. Проведено аналіз предметної області та виявлено недоліки традиційних help desk-систем: відсутність автоматичного контролю SLA, обмежена масштабованість і висока залежність від людського фактору [1,4].

Для усунення цих проблем запропоновано архітектуру інтелектуальної вебсистеми, що поєднує модуль автоматичної класифікації звернень з контролем SLA-дедлайнів.

У системі застосовано методи системного аналізу, програмної інженерії та машинного навчання. Для класифікації використано модель TF-IDF у поєднанні з алгоритмами Logistic Regression та Support Vector Machine (SVM), що забезпечує високу точність розпізнавання категорій [4]. Контроль SLA реалізовано за допомогою Quartz/Hangfire, які перевіряють

статуси заявок та надсилають сповіщення при порушенні термінів. Аналітичний модуль Chart.js відображає ключові показники ефективності роботи операторів[5].

Розроблена система автоматизує процеси технічної підтримки, скорочує кількість ручних операцій і підвищує точність та швидкість реагування, забезпечуючи стабільність і контроль виконання SLA.

Висновки. У результаті дослідження розроблено концепцію вебсистеми служби підтримки, що поєднує методи машинного навчання з автоматизованим контролем SLA. Запропоноване рішення підвищує функційну надійність, безпечність, стабільність і ефективність обробки звернень користувачів.

Запропонована система сприяє оптимізації процесів технічної підтримки та забезпечує безперервність обслуговування відповідно до вимог SLA.

Список літератури

1. Al-Hawari F., Barham H. A Machine Learning Based Help Desk System for IT Service Management. Journal of King Saud University - Computer and Information Sciences, Vol. 33, No. 6, 2019, pp. 702 -718
2. Why implement multi-level SLA in ITSM? Mint Service Desk. URL – https://www.mintsd.com/blog/why-implement-multi-level-sla-in-itsm (дата звернення: 18.10.2025)
3. Інтелектуальні системи підтримки прийняття рішень у сфері обслуговування клієнтів. Nauka Online. URL – https://nauka-online.com/article/intelligent-systems-helpdesk-ml (дата звернення: 12.10.2025)
4. Мельник А. В., Кулик О. В. Використання методів машинного навчання у вебсистемах технічної підтримки користувачів. // Вісник Національного університету «Львівська політехніка». Серія: Комп'ютерні науки. - 2022. - № 4(1083). - С. 45-52.
5. Ren M., Cao K., Betz V. Large Language Models for Hardware Design: Opportunities and Challenges in HDL Generation and Verification // IEEE Access. – 2023. – Vol. 11. – P. 56745–56759. DOI: https://doi.org/10.1109/ACCESS.2023.3264910

Відомості про авторів

Сорокін Владімір Володимирович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», v.v.sorokin@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@csn.khai.edu

Секція 2

УДОСКОНАЛЕНИЙ ПРОЦЕС ВЕРИФІКАЦІЇ ТА ВАЛІДАЦІЇ FPGA МОДУЛІВ НА ОСНОВІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Стряпунін А.О.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Брежнєв Є.В.

Актуальність. Безпілотні літальні апарати (БПЛА), що діють у небезпечних середовищах потребують високого рівня функціональної безпеки, відмовостійкості та кіберзахисту. Критичні функції таких систем часто реалізуються у вигляді програмованої логіки (FPGA), яка забезпечує детерміноване виконання алгоритмів та низьку затримку обробки сигналів [1].

Використання засобів штучного інтелекту (ШІ) відкриває можливості автоматизації аналізу, формалізації вимог, перевірки властивостей і виявлення аномалій у логіці FPGA [2-4].

Мета. Запропонувати концепцію методу верифікації та валідації основаного на засобах ШІ, спрямованого на підвищення гарантоздатності FPGA-модулів у складі безпілотних літальних апаратів.

Основні положення. Враховуючи дослідження, у роботі частково спираємося на концепцію багатоетапної верифікації та гарантоздатності програмованих платформ, запропоновану проф. В.С. Харченком, розширюючи її засобами ШІ для аналізу, формальної перевірки та динамічної валідації FPGA-модулів [1-5]. Запропонована концепція передбачає створення ШІ агента, який здійснює семантичний аналіз вимог, виявляє потенційні невідповідності та формує формальні властивості для перевірки HDL-коду.

Модель машинного навчання класифікує типові шаблони логіки та контролює їх відповідність вимогам. У розробці концепції також варто врахувати тенденції впровадження ML-алгоритмів безпосередньо на FPGA для енергоефективної обробки даних та підвищення стійкості систем керування БПЛА [5]. Верифікація з використанням засобів ШІ повинна забезпечувати безперервний контроль відхилень і своєчасне оновлення перевіреної логіки.

Висновки. Враховуючи вищевикладене, використання методів і засобів ШІ у процесах верифікації та валідації FPGA-модулів є актуальним

напрямом дослідження і потенційно ефективним напрямом підвищення автоматизації розробки, а також функціональної та кібербезпеки БПЛА. FPGA-технології, поєднані із інтеграцією засобів штучного інтелекту, підвищують гарантоздатність і безпеку систем, забезпечуючи їх ефективну роботу у небезпечних просторах.

Подальші дослідження планується зосередити на побудові основаного на інструментах ШІ прототипу процесу верифікацій HDL-коду і розробленні метрик оцінки гарантоздатності.

Список літератури

1. Kharchenko V, Illiashenko O, Sklyar V. Invariant-Based Safety Assessment of FPGA Projects: Conception and Technique. Computers. 2021; 10(10):125. DOI: https://doi.org/10.3390/computers10100125

2. Харченко В.С., Стряпунін А.О. Application of AI Tools in Requirements Engineering: Analysis of Capabilities and a Chatbot for Validation // Aviation and Space Technology. – 2024. – № 3(58). – С. 48–56. DOI: https://doi.org/10.32620/aktt.2024.2.10

3. Li L., Zhang J., Chen Y. Machine Learning-Assisted Hardware Design and Verification: A Survey // ACM Transactions on Design Automation of Electronic Systems (TODAES). – 2024. – Vol. 29, No. 1. – P. 1–42. DOI: https://doi.org/10.1145/3661308

4. Ren M., Cao K., Betz V. Large Language Models for Hardware Design: Opportunities and Challenges in HDL Generation and Verification // IEEE Access. – 2023. – Vol. 11. – P. 56745–56759. DOI: https://doi.org/10.1109/ACCESS.2023.3264910

5. Léonard C., Stober D., Schulz M. FPGA-Enabled Machine Learning Applications in Earth Observation: A Systematic Review // arXiv preprint arXiv:2506.03938. – Technical University of Munich, DLR, 2025. DOI: https://doi.org/10.48550/arXiv.2506.03938

Відомості про авторів

Стряпунін Антон Олександрович, аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.o.striapunin@csn.khai.edu

Брежнєв Євген Віталійович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, e.brezhnev@csn.khai.edu

Секція 2

ФУНКЦІОНАЛЬНА БЕЗПЕКА ІНТЕРФЕЙСІВ ДОПОВНЕНОЇ РЕАЛЬНОСТІ ДЛЯ БЕЗПІЛОТНИХ СИСТЕМ МОНІТОРИНГУ

Суходольський М. О.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Орєхов О.О.

Актуальність. Швидке впровадження безпілотних літальних апаратів (БПЛА) у сферах цивільного, промислового та оборонного моніторингу висуває підвищені вимоги до операторських інтерфейсів. Зростання обсягів телеметрії, відеоданих і просторової інформації призводить до збільшення когнітивного навантаження на оператора, що створює ризики помилок та небезпечних ситуацій. Технології доповненої реальності (AR) дозволяють інтегрувати всі критично важливі дані в єдине інформаційне поле. Проте питання функціональної безпеки AR-інтерфейсів, відповідності стандартам [1-3] та мінімізації операторських помилок залишаються актуальними та малодослідженими.

Метою даної роботи є підвищення рівня функціональної безпеки інтерфейсів доповненої реальності для систем моніторингу БПЛА шляхом аналізу вимог, розроблення структурної моделі AR-панелі оператора та оцінювання її якості методом експертної верифікації.

Основні положення. Традиційні інтерфейси керування БПЛА є інформаційно перевантаженими та розділяють відеопотік, карту й телеметрію між окремими зонами, що збільшує час обробки даних і підвищує ризик операторських помилок. До ключових викликів належать несвоєчасне виявлення небезпечних подій, втрата просторової орієнтації, збільшення кількості помилкових дій та затримка прийняття рішень. Використання AR дозволяє інтегрувати всі критичні дані в єдиний простір сприйняття [4], накладаючи телеметрію, мапу та індикатори стану безпосередньо на відеопотік. Це зменшує когнітивне навантаження, прискорює реакцію оператора, забезпечує контекстну візуалізацію та дозволяє використовувати тривимірні попередження для підвищення безпеки.

Розроблена модель AR-інтерфейсу включає відеопотік з HUD-елементами (курс, висота, швидкість), телеметричні блоки стану, мінікарту, панель вибору дронів і систему аварійних повідомлень відповідно до NUREG-0700. Архітектура орієнтована на AR-шоломи та

мобільні пристрої. Верифікація інтерфейсу за критеріями ISO 25010, NUREG-0700 та IEEE P2048.1 показала високу якість рішення: читабельність – 9.4/10, ефективність попереджень – 9.3/10, функційна повнота – 9.2/10, естетична узгодженість – 9.0/10. Інтегральний показник 8.8/10 підтвердив відповідність системи вимогам функціональної безпеки та ефективності операторської роботи.

Висновки. Розроблений підхід до побудови AR-інтерфейсу підвищує рівень функціональної безпеки систем моніторингу БПЛА завдяки поєднанню телеметрії, карти та попереджень у єдиному візуальному просторі. Експертна верифікація підтвердила його відповідність міжнародним стандартам та ефективність у зниженні операторських помилок. Отримані результати формують основу для подальших досліджень у напрямку масштабування інтерфейсу на багатодронові системи, інтеграції AI-аналітики та впровадження адаптивних механізмів під рівень підготовки оператора.

Список літератури

1. ISO/IEC 25010:2011. Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE). ISO. URL – https://www.iso.org/standard/35733.html (дата звернення: 14.11.2025)
2. U.S. Nuclear Regulatory Commission. NUREG-0700, Rev. 3. HumanSystem Interface Design Review Guidelines. Washington, DC: NRC, 2020. DOI: https://doi.org/10.2172/1644018
3. IEEE P2048.1. Standard for Virtual and Augmented Reality: Device Taxonomy and Definitions. IEEE. URL – https://sagroups.ieee.org/2048wg/ (дата звернення: 14.11.2025)
4. Milgram, P., Kishino, F. A taxonomy of mixed reality visual displays. IEICE Transactions on Information and Systems, E77-D, № 12, pp. 1321– 1329 (1994). URL – https://www.alice.id.tue.nl/references/milgram-kishino1994.pdf (дата звернення: 14.11.2025)

Відомості про авторів

Суходольський Марк Олексійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.sukhodolskyi@student.csn.khai.edu
Орєхов Олександр Олександрович, професор кафедри комп'ютерних систем, мереж і кібербезпеки НАУ «ХАІ», к.т.н., доцент, a.orehov@csn.khai.edu

Секція 2

АРХІТЕКТУРА ЗБОРУ ПОВЕДІНКОВИХ ДАНИХ: БАЛАНС МІЖ ПЕРСОНАЛІЗАЦІЄЮ ТА БЕЗПЕКОЮ КОРИСТУВАЧА

Тітов Б. О.
Національний аерокосмічний університет
«Харківський авіаційний інститут»
м. Харків, Україна
Науковий керівник: Бабешко Є. В.

Актуальність. Розроблення систем персоналізованої дієтології вимагає оброблення значних масивів чутливих даних, що включають антропометричні показники, медичні дані та детальні поведінкові патерни. З одного боку, глибина аналізу цих даних визначає точність рекомендацій, а з іншого – створює суттєві ризики для приватності користувача та інформаційної безпеки системи.

Використання виключно клієнтського трекінгу (Client-Side Tracking) робить систему вразливою до блокувальників контенту, ін'єкцій шкідливого коду та перехоплення даних, що ускладнює відповідність регламентам GDPR.

Розроблення гібридної архітектури збору даних, яка забезпечує валідність інформації без компрометації конфіденційності, є актуальним завданням у сфері кібербезпеки веб-застосунків.

Метою є обґрунтування архітектури збору та оброблення поведінкових даних у веб-застосунку для дієтології, яка забезпечує баланс між ефективністю персоналізації та захистом інформаційних активів користувача.

Основні положення. У ході дослідження було проаналізовано таксономію даних для нутриціології, яку розділено на медико-біологічні (об'єктивні) та поведінкові (суб'єктивні/контекстуальні). Встановлено, що покладання виключно на клієнтський трекінг несе загрози цілісності та конфіденційності даних. Натомість серверний трекінг (Server-Side) забезпечує контроль над даними у захищеному периметрі [1]. Запропоновано гібридний підхід до архітектури системи, який базується на розмежуванні потоків даних.

Критично важливі події, такі як збереження прийому їжі, медичні показники та транзакції, обробляються виключно на стороні сервера, що дозволяє застосовувати суворі політики валідації та шифрування перед записом у базу даних. Водночас дані про UX-взаємодію (кліки, скроли), які

не несуть критичних ризиків приватності, збираються на клієнтській стороні для покращення інтерфейсу, але не використовуються для прийняття медичних рішень. Для мінімізації ризиків зберігання чутливої інформації рекомендовано використання API платформ здоров'я (Health Connect, HealthKit).

Це дозволяє агрегувати дані з IoT-пристроїв без необхідності їх повної передачі на сервери застосунку, залишаючи контроль за дозволами на стороні користувача [2,3]. Такий підхід дозволяє нівелювати ризики, пов'язані з блокувальниками реклами та вразливістю клієнтських скриптів, забезпечуючи цілісність даних для алгоритмів машинного навчання.

Висновки. Запропонована гібридна архітектура вирішує проблему дихотомії між зручністю використання та безпекою даних у системах e-health.

Використання серверної сторони як єдиної точки верифікації критичних даних у поєднанні з федеративними протоколами обміну інформацією дозволяє створити стійку до маніпуляцій систему. Це забезпечує захист персональних даних користувача при формуванні інтелектуальних дієтичних рекомендацій.

Список літератури

1. Server-Side vs Client-Side Tracking: A Simple Guide. Snowplow Blog. URL – https://snowplow.io/blog/server-side-vs-client-side-tracking (дата звернення: 14.11.2025)
2. Health Connect data types. Android Developers. URL – https://developer.android.com/health-and-fitness/guides/health-connect/plan/data-types (дата звернення: 14.11.2025)
3. NestJS Documentation. Security Best Practices: Authentication, CORS, CSRF, and HTTPS. URL: https://docs.nestjs.com/security (дата звернення: 09.11.2025)

Відомості про авторів

Тітов Богдан Олегович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», b.titov@student.csn.khai.edu
Бабешко Євген Васильович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки НАУ «ХАІ», к.т.н, e.babeshko@csn.khai.edu

Секція 2

ДОСЛІДЖЕННЯ ТА РОЗРОБЛЕННЯ СИСТЕМИ КОНТРОЛЮ ВИКОРИСТАННЯ ОРЕНДОВАНОГО АВТОМОБІЛЯ

Ткаченко І. Д.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Желтухін О. В.

Актуальність. В сучасному світі широкої популярності набуло явище у час відпустки, подорожування світом для знайомства з різноманітними куточками нашої планети. Сучасні туристи вирушають у мандрівку містами минулих великих цивілізацій, де зараз мешкають звичайні люди. Сучасні туристичні агенції пропонують безліч різноманітних турів, але туристи замовивши такі тури стають заручниками стандартних екскурсій і не мажуть як правило змінити програму придбаного турне, але для цих користувачів існує легке вирішення цієї проблеми – наймання персонального водія з власним транспортним засобом, але послуги водія будуть коштувати занадто дорого, що не кишені переважної більшості туристів, інший спосіб вирішення цієї проблеми – здійснити подорож використовуючи власний транспортний засіб, але тут також є велика купа проблем, пов’язана з доставкою автомобіля, є ще можливість використання орендованого транспортного засобу.

Метою даної роботи є дослідження безпеки керування орендатором орендованого транспортного засобу, для запобігання прискореного зносу автомобіля, що знаходиться в оренді, і звільнення власника орендованого автомобіля від сплати штрафів оформлених в режимі автоматичної фіксації порушень правил дорожнього руху.

Основні положення. Каршерінг це автомобільний сервіс, який дає можливість орендувати автомобіль на короткий час з по хвилинною або по годинною оплатою. Найчастіше він використовується для коротких поїздок в межах міста. А наявність великої кількості пунктів, де можна залишити автомобіль після використання, дає можливість вибирати між громадським транспортом або автомобілем. Тож користувачі стають власниками авто тільки у той час, коли їм це дійсно необхідно [1].

Каршерінг дозволяє вирішити безліч питань, які, пов'язани з традиційною орендою автомобіля:

Каршерінг дозволяє вирішити всі ці проблеми і робить оренду чимось середнім між звичною орендою авто, громадським транспортом і таксі [2].

Каршерінг незважаючи на свою привабливість для клієнта має і певні недоліки такі як – ризики частого пошкодження і виходу з ладу автомобілів (також взявши в оренду автомобіль і не помітивши порушень, що вже були, але не прописані в договорі та не зафіксовані заздалегідь, є ризик, що компанія може зажадати відшкодування збитків) [3].

Саме пошкодження транспортного засобу може бути спричинено як в наслідок дорожньо транспортної пригоди – ДТП, так і в наслідок неналежної експлуатації цього транспортного засобу орендарем. Збитки спричинені у першому випадку майже очевидні і зазвичай фіксуються дорожньою поліцією, або страховим інспектором і як правило мають пояснення від другої сторони цього ДТП.

У випадку неналежної експлуатації транспортного засобу орендарем збитки спричинені орендарем майже не можна довести, тому ці можливі збитки майже сто відсотково будуть закладені у вартість оренди транспортного засобу який використовується у системі каршерінгу.

Висновки. Розробка контролера, що дозволяє контролювати основні параметри використання орендованого транспортного транспортного засобу, збереження параметрів функціонування означеного транспортного засобу і разі можливості обмежувати використання його у екстремальних режимах є актуальним.

Список літератури

1. Каршерінг. Fra.org. URL – https://fra.org.ua/uk/an/publikatsii/analitika/karshieringhova-ievropieis-ka-istoriia (дата звернення 10.10.2025)

2. Проблеми, що вирішує каршерінг. Getmancar. URL – https://getmancar.com/ru/blogs/carsharing-in-europe (дата звернення 12.10.2025)

3. Недоліки каршерінгу. Inventure. URL – https://inventure.com.ua/uk/analytics/investments/rinok-karsheringu-v-ukrayini (дата звернення 14.10.2025)

Відомості про авторів

Ткаченко Ігор Дмитрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.tkachenko@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

ПІДХОДИ ДО АДАПТАЦІЇ МОДЕЛЕЙ ЗОРУ ТА МОВИ У ЗАДАЧАХ З ОБМЕЖЕНИМИ ДАНИМИ

Туз А. В.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Морозова О. І.

Актуальність. З розвитком штучного інтелекту та глибокого навчання зросла кількість атак, спрямованих на підробку або спотворення даних: від фішингових зображень до deepfake-відео, які здатні обманювати як людей, так і автоматизовані системи захисту. Традиційні методи виявлення загроз вимагають великої кількості маркованих даних і швидко застарівають через постійне оновлення типів атак. У цьому контексті модель CLIP (Contrastive Language-Image Pretraining) набуває особливої актуальності, адже поєднує аналіз зображень і текстових описів, що дозволяє проводити zero-shot детекцію аномалій – розпізнавати нові або невідомі типи загроз без попереднього навчання [1]. Використання CLIP у сфері кібербезпеки відкриває можливості для створення інтелектуальних систем, здатних автоматично виявляти підроблений контент, фішингові сторінки та інші прояви візуальних атак.

Метою роботи є дослідження можливостей застосування мультимодальної моделі PACKETCLIP для підвищення безпеки сучасних Docker-контейнерів шляхом виявлення аномалій у мережевому трафіку [2]. Основними задачами дослідження є: аналіз архітектури CLIP та принципів її роботи; оцінка здатності zero-shot детекції аномалій; порівняння продуктивності базової моделі CLIP та її модифікацій, таких як AA_CLIP і PACKETCLIP, у протидії adversarial-атакам; визначення перспектив інтеграції мультимодальних моделей у системи моніторингу загроз та SOC-платформи [3].

Основні положення. Мультимодальна модель PACKETCLIP поєднує представлення мережевих пакетів та текстових описів у єдиному семантичному просторі, що дозволяє здійснювати аналіз трафіку навіть у зашифрованих контейнерних середовищах. Для детекції аномалій використовуються методи zero-shot, які не потребують додаткового маркування даних, що є особливо важливим при швидко змінюваних типах атак у Docker-контейнерах. Архітектура моделі включає графові нейронні мережі, що дозволяють враховувати взаємозв'язки між пакетами та

підвищують точність класифікації аномалій [2]. Інтерпретованість результатів забезпечується завдяки можливості відстежувати, які текстові чи пакетні характеристики вплинули на рішення моделі. Використання PACKETCLIP дозволяє автоматично виявляти підозрілу активність у мережевому трафіку, зменшувати кількість хибнопозитивних спрацьовувань та підвищувати ефективність моніторингу безпеки Docker-контейнерів [2].

Висновки. Використання мультимодальної моделі PACKETCLIP у сфері кібербезпеки дозволяє підвищити ефективність автоматичного виявлення аномалій у мережевому трафіку Docker-контейнерів. zero-shot підхід забезпечує можливість розпізнавати нові або невідомі типи загроз без необхідності додаткового маркування даних, що особливо важливо для швидко змінюваних атак. Архітектура з графовими нейронними мережами підвищує точність класифікації, а інтеграція текстових описів з даними пакетів дозволяє підвищити інтерпретованість рішень. Результати дослідження свідчать про високий потенціал мультимодальних моделей для інтеграції у системи моніторингу та SOC-платформи (комплексні програмні рішення для операційних центрів безпеки), що дозволяє ефективно захищати контейнерні середовища і зменшувати ризики від нових кіберзагроз.

Список літератури

1. Radford, Alec, et al. "Learning transferable visual models from natural language supervision". International conference on machine learning. PmLR, 2021. DOI: https://doi.org/10.48550/arXiv.2103.00020

2. Masukawa, Ryozo, et al. "PacketCLIP: Multi-Modal Embedding of Network Traffic and Language for Cybersecurity Reasoning". arXiv preprint arXiv: 2503.03747. 2025.

3. Ma, Wenxin, et al. "Aa-clip: Enhancing zero-shot anomaly detection via anomaly-aware clip". Proceedings of the Computer Vision and Pattern Recognition Conference. 2025. DOI: https://doi.org/10.48550/arXiv.2503.06661

Відомості про авторів

Туз Аліна Володимирівна, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.tuz@student.csn.khai.edu

Морозова Ольга Ігорівна, доктор технічних наук, професор, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.morozova@khai.edu

Секція 2

БЕЗПЕКОВІ АСПЕКТИ РОЗРОБКИ ІНКЛЮЗИВНОЇ ВЕБ-ПЛАТФОРМИ ДЛЯ ПЕРЕКЛАДУ ЖЕСТОВОЇ МОВИ У ТЕКСТ

Хорунжий Д. Ю.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Куланов В.О.

Актуальність. Сучасні інклюзивні цифрові технології дедалі частіше працюють із персональними, а подекуди й біометричними даними користувачів. З огляду на стрімке зростання кількості кібератак, порушень конфіденційності та витоків інформації, питання забезпечення безпеки таких систем набуває критичного значення [1]. Особливої уваги потребують веб-платформи, що опрацьовують відео та зображення людей, адже це створює додаткові ризики несанкціонованого доступу, ідентифікації особи чи зловживання отриманими даними. У цьому контексті розробка інклюзивної системи для автоматичного перекладу жестової мови в текст постає не лише як технічне чи соціальне завдання, а й як виклик у сфері кібербезпеки. Адже така платформа має гарантувати захист персональних відео, безпечне зберігання профілів користувачів і дотримання принципів конфіденційності відповідно до сучасних стандартів інформаційної безпеки та вимог GDPR [2].

Мета. Метою роботи є дослідження й впровадження комплексних рішень автентифікації, авторизації та захисту даних у веб-платформі для перекладу жестової мови з урахуванням сучасних кіберзагроз і принципів безпечного проєктування.

Основні положення. У межах дослідження побудовано архітектуру веб-платформи, серверна частина якої реалізована на базі NestJS (TypeScript) із використанням REST API для забезпечення масштабованої та захищеної взаємодії з клієнтською частиною. Для керування користувацькими сесіями впроваджено модель автентифікації на основі JWT-токенів, що дозволяє контролювати доступ до персональних даних і мінімізувати ризик несанкціонованого використання облікових записів. Розглянуто альтернативні підходи до побудови автентифікації, зокрема cookie-based механізми, plain JWT і інтеграцію OAuth 2.0 / OpenID Connect відповідно до стандарту RFC 6749 [3]. Усі запити між клієнтом і сервером шифруються за допомогою TLS, а обробка облікових даних супроводжується хешуванням паролів методом bcrypt. Здійснено також

заходи протидії найпоширенішим веб-загрозам, визначеним у керівництві OWASP Top 10 [1]. Для зменшення ризиків витоку відеоінформації реалізовано тимчасове зберігання файлів, автоматичне видалення після обробки та анонімізацію метаданих відповідно до принципів «privacy by design» [5]. Наукова новизна поєднує технології розпізнавання жестів та принципи безпеки, орієнтовані на захист даних користувача на всіх етапах життєвого циклу системи. Це дозволяє розглядати систему перекладу жестової мови не лише як засіб комунікації, а й як приклад побудови безпечного інклюзивного середовища. Практичне значення розроблюванної веб-платформа є прикладом інтеграції засобів машинного навчання та веб-безпеки в одному рішенні. Вона може бути використана в освітніх, медичних і державних установах, де особлива увага приділяється захисту конфіденційних відео та персональних даних. Представлені рішення щодо автентифікації, шифрування та контролю доступу можуть бути масштабовані на інші інклюзивні або соціально орієнтовані веб-сервіси.

Висновки. Інклюзивні цифрові платформи, що працюють із даними користувачів, мають розроблятися з урахуванням принципів безпеки на всіх етапах життєвого циклу. Запропонована архітектура демонструє можливість створення інклюзивного середовища без компромісів у сфері кіберзахисту, забезпечуючи баланс між функціональністю, доступністю та конфіденційністю користувачів.

Список літератури

1. Top 10 Web Application Security Risks – 2021. OWASP. URL – https://owasp.org/Top10 (дата звернення: 09.11.2025)
2. European Union. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679, 2016
3. Hardt, D. The OAuth 2.0 Authorization Framework (RFC 6749). Internet Engineering Task Force (IETF), 2012
4. NestJS Documentation. Security Best Practices: Authentication, CORS, CSRF, and HTTPS. URL: https://docs.nestjs.com/security (дата звернення: 09.11.2025)
5. Cavoukian, A. Privacy by Design: The 7 Foundational Principles. Information & Privacy Commissioner of Ontario, 2011

Відомості про авторів

Хорунжий Денис Юрійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.khorunzhyi@student.csn.khai.edu
Куланов Віталій Олександрович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, к.т.н., v.kulanov@khai.edu

Секція 2

ДОСЛІДЖЕННЯ НАДІЙНОСТІ БЕЗЕТАЛОННИХ МЕТРИК ЯКОСТІ ПІСЛЯ ОБРОБКИ DRUNET

Черепанов І. О.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Єремеєв О. І.

Актуальність. Зображення, отримані за допомогою радіолокатора із синтезованою апертурою (РСА), мають ключове значення для систем дистанційного зондування, що використовуються у критично важливих галузях, де від достовірності обробки даних залежить функціональна безпека інформаційних систем. Такі системи здатні забезпечити спостереження за поверхнею вдень і вночі за будь-яких погодних умов, однак РСА-зображення характеризуються наявністю спекл-шуму, який ускладнює їхню інтерпретацію та автоматичний аналіз [1]. При аналізі методів придушенняя спеклу та оптимізації їх параметрів під час моделювання використовуються тестові зображенні та метрики якості з еталоном, але для реальних РСА-даних істинні зображення відсутні, що робить необхідним застосування під час аналізу та оптимізації метрик якості без еталону. Для багатьох метрик якості з еталоном, наприклад MDSI, PSIM, VSI, FSIMc, PSNRHA, GMSD та їх нейромережевих комбінацій [2], доведено їх високу кореляцію із візуальною якістю, оціненої експертами. Але для метрик без еталону така кореляція є суттєво гіршою і їх властивості проаналізовані меншою мірою. Тому для застосування, що розглядається, потрібні метрики якості без еталону, які б мали високу кореляцію з найкращими (відомими) метриками якості з еталоном.

Метою цієї роботи є визначення безеталонних метрик якості, результати роботи яких будуть подібні до результатів метрик з еталоном, що застосовувалися для зображень, оброблених нейромережею DRUNet [3] для придушення спеклу. Для аналізу було обрано реалізації кількох метрик, зокрема PIQE, NIQE та BRISQUE, що доступні в Матлабі.

Основні положення. Для кількісного аналізу ступеню подібності між метриками з еталоном та без еталону використані коефіцієнти рангової (SROCC – Spearman Rank Order Correlation Coefficient) та лінійної (PCC – Pearson Correlation Coefficient) кореляції. Дослідження показало, що серед розглянутих метрик без еталону найвищу узгодженість із метрикою

візуальної якості з еталоном PSNR-HVS-M демонструє метрика без еталону NIQE, для якої PCC становить -0.87, а SROCC становить -0.96 (знак коефіцієнтів кореляції тут не має значення). Це свідчить про сильний обернений зв'язок: зі зростанням значення PSNR-HVS-M (тобто покращенням якості) показник NIQE зменшується, що відповідає її інтерпретації. На відміну від NIQE, метрики PIQE та BRISQUE показали слабку або помірну від'ємну кореляцію з PSNR-HVS-M (значення SROCC приблизно дорівнюють −0.4 для проаналізованих тестових зображень, які моделюють багатопоглядові РСА-зображення системи Сентінель-1). Така поведінка метрик PIQE та BRISQUE може бути зумовлена різницею у принципах їх розрахунку або їх орієнтованістю на оптичні зображення і типи завад і викривлень, що суттєво відрізняються від спекл-шуму.

Висновки. Таким чином, метрика NIQE характеризується досить високою адекватністю для зображень із спекл-шумом та результатів їх фільтрації і може бути використана як ефективна метрика якості без еталону для оцінювання результатів фільтрації та оптимізації параметрів фільтрів. Втім, доцільно також продовжити пошук або розробку метрик візуальної якості зображень без еталону для РСА-зображень, зокрема для випадків стиснення таких зображень із втратами та використання інших методів придушення спекл-шуму.

Список літератури

1. S. Abramov, O. Rubel, V. Lukin, A. Shelestov, M. Lavreniuk, "Speckle reducing for Sentinel-1 SAR data," Proceedings of the International Geoscience and Remote Sensing Symposium (IGARSS), Fort Worth, TX, USA, December 4, 2017, pp. 2353-2356. DOI: https://doi.org/10.1109/IGARSS.2017.8127463

2. Ieremeiev, O.; Lukin, V.; Okarma, K.; Egiazarian, K. Full-Reference Quality Metric Based on Neural Network to Assess the Visual Quality of Remote Sensing Images. Remote Sens. 2020, 12, 2349. DOI: https://doi.org/10.3390/rs12152349

3. K. Zhang, Y. Li, W. Zuo, L. Zhang, L. Van Gool, and R. Timofte, "Plug-and-Play Image Restoration with Deep Denoiser Prior," arXiv, 2022. DOI: https://doi.org/10.48550/arXiv.2008.13751

Відомості про авторів

Черепанов Ілля Олегович, аспірант кафедри інформаційно-комунікаційних технологій ім. О. О. Зеленського, НАУ «ХАІ», c.illia@student.khai.edu

Єремеєв Олег Ігорович, доцент кафедри інформаційно-комунікаційних технологій ім. О. О. Зеленського, НАУ «ХАІ», к.т.н., o.ieremeiev@khai.edu

Section 2

MACHINE LEARNING ANALYSIS ADVANCING SECURITY PLANNING

Yulian Hristov
JTSAC, Institute of ICT, Bulgarian Academy of Sciences, Sofia, Bulgaria
Scientific adviser: Zlatogor Minchev

Relevance. The use of Artificial Intelligence and Machine Learning-based models in the social field is a process that is mainly regulated by the business logic of companies for attracting a larger circle of users to digital platforms and thus – generating economic benefits. In the field of security planning, such approaches as digital humanities, now also have their place, primarily at the operational and tactical level - mainly for training purposes and analyzing data from tactical exercises or war game simulations [1]. However, there is still a lack of a scientific methodology that encompasses technological advances and security science in a way that supports the strategic level & the planning process. It is about introducing technologies based on AI and machine learning to keep the strategic decision-making process in a condition that is adequate to the rapidly changing security environment.

Principal provisions. Accelerating the process of analyzing large text copruses is essential for gaining an advantage in the field of national and international security. Automated tracking of the evolution of certain scenarios in the strategic documents of individual countries allows for focused and precise analysis of certain aspects of national security – military-defense, economic, financial, energy, etc. The gap in this process is slowly beginning to be bridged [2] and the scientific community must be engaged in the processes of automated information extraction, so that this process is based on precise academic statements to avoid poor-quality, subjective and distorted analysis.

The purpose. Further on we propose a system model with an approach that describes the possible technological solution for analysis, based on system modelling & natural language processing (NLP), implementing machine reading of large arrays of structured information (like: national security strategies and concepts, and their accompanying plans and roadmaps for implementation, as well as reports on the implementation of the strategies). An approach from social science was used, which proposes the isolation of specific entities such as **actor** and action [3]. This enables automatic analytical extraction of explicit and "hidden" scenarios in national conceptual documents, tracking their temporal development, presence or absence amongst the documents, the "weights" of the

scenarios and their importance. The final result of such a mechanism contains a set of scenarios with the possibility of predicting their development, but this does not end the strategic planning process.

Conclusions. Such a mechanism would serve as a human activity-supporting smart tool for expert assessment implemented in a system model that is further used for holistic strategic decision-making and planning policies development at the highest state level. The actual objective is to diminish the risks of producing hallucinations due to unproper data interpretations and obtaining a holistic model assessment of the strategic documents, both quite important for the security planning, especially for the future.

List of references

1. Hunter, C., Bowen, B. E. (2024). We'll never have a model of an AI major-general: Artificial Intelligence, command decisions, and kitsch visions of war. Journal of Strategic Studies, 47(1), 116-146. DOI: https://doi.org/10.1080/01402390.2023.2241648

2. The White House, Winning the race. America's Action Plan, July 2025. URL – https://whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf (date of accesse: 11.11.2025)

3. John W. Mohr, Robin Wagner-Pacifici, Ronald L. Breiger, Petko Bogdanov. Graphing the grammar of motives in National Security Strategies: Cultural interpretation, automated text analysis and the drama of global politics, Poetics, Volume 41, Issue 6, 2013, P. 670-700, ISSN 0304-422X. DOI: https://doi.org/10.1016/j.poetic.2013.08.003

Information about the authors

Yulian Hristov, assistant professor at JTSAC, Institute of ICT, Bulgarian Academy of Sciences, yulian.hristov@iict.bas.bg, yulianvhristov@gmail.com

Zlatogor Minchev, head of IT for Security Department, Institute of ICT, Bulgarian Academy of Sciences, zlatogor@bas.bg

ТЕЗИ ДОПОВІДЕЙ

Секція 3. Правове забезпечення кібербезпеки

ABSTRACTS OF REPORTS

Section 3. Cybersecurity law and regulation

Section 3

INTERNATIONAL LAW AND DATA EXCHANGE ON PLASTIC POLLUTION IN THE OCEANS: LEGAL AND CYBERSECURITY SUPPORT FOR AEROSPACE MONITORING

Sofia Bashkat
Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, Dnipro, Ukraine
Scientific adviser: Yurii Kiforuk

Relevance. The problem of global pollution of oceans and seas with plastic waste is one of the most serious environmental threats of our time. According to estimates by international organizations, more than 170 trillion floating plastic particles have already accumulated in the world's oceans [1]. An effective response to the problem is only possible with accurate, rapid, and continuous monitoring, which is currently provided by modern aerospace technologies – Sentinel satellites, Landsat, and other platforms. However, satellite monitoring systems depend on cross-border information exchange, which is regulated by international law. Security standards are no less important, as the number of cyberattacks on Earth remote sensing infrastructure is growing, which can lead to the distortion of environmental data or blocking access to it [2]. In this context, the combination of international legal mechanisms, cybersecurity, and aerospace monitoring is critically important to ensure the transparency and reliability of marine ecosystem assessments.

Purpose. The purpose of the study is to analyze the international legal mechanisms and cybersecurity requirements for the cross-border exchange of satellite data on plastic pollution of the oceans, as well as to determine the role of legal regulation in the functioning of aerospace monitoring systems.

Principal provisions. The key norms regulating the exchange of information on marine pollution are contained in the UN Convention on the Law of the Sea (UNCLOS), MARPOL 73/78 and the Aarhus Convention. They oblige states to conduct monitoring of the marine environment and ensure access to environmentally significant information of international importance [3]. In modern practice, the following are used: intergovernmental agreements on environmental observations; memoranda between space agencies and scientific organizations; open geoinformation system standards (GEOSS, Copernicus). They define the rules for the transmission, storage, processing and dissemination of Earth remote sensing data. There is a growing number of attacks on ground data processing centers and on machine learning algorithms used to identify areas

of plastic pollution [1,2]. Legal regulation in the field of cybersecurity includes ITU recommendations on the security of satellite channels, the principles of international law set out in the Tallinn Manual, and the requirements of the EU NIS2 Directive regarding the cyber-resilience of environmental data infrastructure. Satellite systems make it possible to identify plastic accumulations with an accuracy of tens of meters, distinguishing their spectral signatures [4]. These data can be used in international environmental investigations, in monitoring compliance with MARPOL requirements, and in global monitoring geoportals (Ocean Cleanup, ESA EO Browser). Thus, satellite observations form a reliable evidentiary basis, but the effectiveness of their use depends on legal norms of access, cybersecurity and international regulation.

Conclusions. International legal mechanisms and cybersecurity standards play a key role in ensuring the reliability and availability of satellite data on plastic pollution of the oceans. The conditions of transnational waste movement require close coordination between states and global organizations, as well as improvement of information protection infrastructure. Aerospace monitoring is the basis of the modern system for assessing the state of marine areas, but its effective application is possible only with clear legal norms, reliable cybersecurity technologies and open international exchange of environmental data.

List of references

1. Supporting the Science that Saves the Ocean. ArcUser. 2023
2. How to End Ocean Plastic Pollution. Environmental Investigation Agency
3. United Nations Convention on the Law of the Sea (UNCLOS). 1982
4. Sentinel-2 Satellite Imagery and Characteristics. EOS Data Analytics
5. Kyforuk Yu.M., Petrosyan P.A., Kravchenko K.S., Puchenina M.R., Kondrachuk S.S., Andreev S.M. Creation of aerospace monitoring of pollution of oceans and seas by plastic emissions. // Dnipro Orbit – 2025: materials of the XX scientific readings (October 22–24, 2025). National Center for Aerospace Education of Youth named after O.M. Makarov, SE “Design Bureau Yuzhnoye” named after M.K. Yangel, National Museum of Cosmonautics named after S.P. Korolev, Dnipro National University named after O. Honchar. – Dnipro, 2025. – P. 213–214

Information about the authors

Bashkat Sofia, student of the Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, sofiabaskat@gmail.com
Yurii Kyforuk, computer science teacher from Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, kiforuk.yury@gmail.com

Section 3

MECHANISMS OF FINANCING AND LEGAL SUPPORT OF NATIONAL MONITORING PROGRAMS (GRANTS, STATE TENDERS WITH REQUIREMENTS FOR CYBERSECURITY)

Ksenia Boboshko
Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, Dnipro, Ukraine
Scientific adviser: Yurii Kyforuk

Relevance. In today's digital transformation, national monitoring programs (environment, infrastructure, space) collect large amounts of data that need to be protected. Cybersecurity has become a key condition for the effective financing of such projects, because any data leakage or distortion can have strategic consequences for the state. Integrating the principle of security-by-design into financial and legal mechanisms is a necessary step to build a secure digital state. At the same time, the growing complexity of digital ecosystems requires governments to ensure not only technological but also organizational resilience. Modern monitoring systems interact with various stakeholders – from private contractors to international partners – which increases the number of potential vulnerabilities [1]. Therefore, establishing unified cybersecurity standards, mandatory for all participants of national monitoring programs, becomes essential for maintaining trust, ensuring uninterrupted data exchange, and supporting long-term project sustainability.

Purpose. Ensure a combination of financial, technical and legal instruments for the sustainable functioning of national monitoring systems with a guaranteed level of cyber protection. To form an approach in which cybersecurity is a mandatory criterion for funding, managing and controlling programs. Such an approach makes it possible to align strategic planning with modern security requirements, ensuring that every stage of program development – from budgeting to data processing – meets unified protection standards. This strengthens the resilience of national monitoring systems and supports their stable operation in a high-risk digital environment.

Principal provisions. The main provisions are based on the Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine». The cybersecurity of national monitoring programs should be ensured through a systematic approach, risk management and security audits. In financing and public procurement, the principle of «security-by-design» should be implemented, that is, data protection requirements should be taken into account

at all stages of project implementation [2]. This guarantees the reliability of the information infrastructure and increases international confidence in Ukrainian programs. An important component of these provisions is the coordination between state institutions responsible for cybersecurity and the agencies implementing monitoring programs. Such interaction ensures that technical requirements, legal norms and financial instruments function cohesively, allowing projects to remain both technologically advanced and securely protected throughout their entire lifecycle [3].

Conclusions. The main result of the study is to determine the approach to financing and legal support of national monitoring programs taking into account cybersecurity. It has been proven that the effectiveness of such programs is possible only if the principle of security-by-design is implemented at all stages. Cyber security should be a mandatory requirement for funding, auditing, and certification of performers, ensuring data reliability and increasing trust in government programs.In addition, the integration of cybersecurity into financial and legal mechanisms contributes to the long-term sustainability of national monitoring systems. It allows the state to minimize risks, optimize resource allocation, and create a transparent environment in which technological development is supported by clear regulatory safeguards.

List of references

1. ENISA. Cybersecurity Requirements in Public Procurement and Funding Programs. European Union Agency for Cybersecurity, 2024.
2. ISO/IEC 27001:2022 – Information Security Management Systems – Requirements. International Organization for Standardization.
3. Kyforuk Y.M., Petrosyan P.A., Kravchenko K.S., Puchenina M.R., Kondrachuk S.S., Andreev S.M. Creation of aerospace monitoring of pollution of oceans and seas by plastic outlets // Dnieper orbit – 2025: materials of the XX scientific readings (October 22-24, 2025) / Nats. Center for Aerospace Education of Youth. O.M. Makarov, SE "Design Bureau "Yuzhnoye" them. M.K. Yangel" Nats. Museum of Cosmonautics. S.P. Koroleva, Dniprovskyi Nats. Univ. O. Honchara.– Dnipro, 2025.– P. 213-214.

Information about the authors

Ksenia Boboshko, student from Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, kseniabobosko148@gmail.com
Yurii Kyforuk, computer science teacher from Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, kiforuk.yury@gmail.com

Section 3

INFORMATION WARFARE: DISINFORMATION AROUND WASTE MONITORING AND THE ROLE OF CYBERSECURITY

Valeriia Bozhko
Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, Dnipro, Ukraine
Scientific adviser: Yurii Kyforuk

Relevance. Monitoring the pollution of marine surfaces with plastic waste is one of the key environmental problems of modern times. According to recent scientific research, trillions of plastic particles – both macro- and microplastics – accumulate in the World Ocean, forming stable pollution zones [1]. The developed aerospace monitoring system for ocean pollution by plastic waste provides the collection and analysis of satellite images from Sentinel-1, Sentinel-2, and Sentinel-3, enabling the detection and mapping of waste accumulation areas [2]. However, the rapid spread of digital technologies has led to the emergence of new threats: falsification of satellite images, manipulation of remote sensing data, cyber interference with geographic information systems and geoportals. Such actions represent elements of modern information warfare aimed at discrediting environmental research, undermining trust in scientific methods for assessing the state of the environment, and creating information chaos that may influence international environmental policy.

Purpose. The purpose of the study is to identify key disinformation threats in the field of satellite monitoring of plastic waste and to justify the legal and technical cybersecurity measures necessary to ensure the reliability of environmental data used in the Aerospace Monitoring System for Ocean Pollution.

Principal Provisions. Fake satellite images and manipulation of spectral data. The emergence of accessible image-editing tools and AI technologies (GANs, diffusion models) enables the falsification of data that can imitate either the absence or presence of pollution. Manipulations with Sentinel spectral channels can alter NDVI, NIR reflectance, and other indicators used for plastic detection [2]. The geoportal created to display monitoring results via Google My Maps and other services becomes a potential target for: substitution of imported KMZ files; changing image classification parameters; blocking access to Sentinel Hub data. Such actions may lead to disinformation of the public and international environmental institutions [3]. To ensure the legal status of environmental information, it is necessary to implement: verification of ESA satellite image metadata; digital signatures and secure transmission channels;

satellite forensics algorithms such as PRNU, Noiseprint, and ELA. A reliable procedure also includes comparing optical Sentinel-2 data with radar Sentinel-1 data to detect inconsistencies. In international practice, the reliability of environmental data is regulated by the Aarhus Convention, Copernicus Data policies, and ISO standards for geodata quality. Within the framework of environmental monitoring, this ensures: transparency of data collection and processing methods; the possibility of independent auditing; legal liability for intentional modification or substitution of satellite data. Environmental projects should implement: open datasets of images and metadata; explanations of classification algorithms and map-building methods; PR strategies for rapid response to fake information. This reduces information risks and strengthens public trust in the results of aerospace monitoring [4].

Conclusions. The field of aerospace monitoring of ocean pollution is becoming one of the most vulnerable areas in modern information warfare. Falsification of satellite images, manipulation of spectral analysis data, and cyberattacks on geoportals can significantly reduce the reliability of environmental information and influence decision-making at the international level. To increase the resilience of the monitoring system, it is necessary to implement legal cybersecurity mechanisms, transparent data source verification procedures, algorithm audits, and active information policies. This will ensure the reliability and evidential value of data on ocean pollution with plastic waste and will contribute to effective environmental security.

List of references

1. Eriksen M. et al. A growing plastic smog PLOS ONE, 2023
2. Oleksandra B. A global approach to preventing plastic from entering the ocean. ArcGIS Journal, 2023
3. Kaandorp M. Global mass of buoyant marine plastics. Nature Geoscience, 2023
4. Kyforuk Yu.M., Petrosian P.A., Kravchenko K.S., Puchenina M.R., Kondrachuk S.S., Andreev S.M. Creation of Aerospace Monitoring of Pollution of Oceans and Seas by Plastic Waste // Dnipro Orbit – 2025: Proceedings of the 20th Scientific Readings (October 22-24, 2025) / O.M. Makarov National Center for Aerospace Education of Youth, State Enterprise “Design Bureau ‘Pivdenne’ Named After M.K. Yangel,” S.P. Korolov National Museum of Cosmonautics, O. Honchar Dnipro National University. – Dnipro, 2025. – pp. 213-214

Information about the authors

Bozhko Valeriia, student from Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, bozhko@ual.ukr.education
Yurii Kyforuk, computer science teacher from Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, kiforuk.yury@gmail.com

Секція 3

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У ПРАВОВОМУ МЕХАНІЗМІ ПУБЛІЧНОГО УПРАВЛІННЯ

Джунь С.С.
Сумський обласний інститут післядипломної педагогічної освіти, м. Суми, Україна
Науковий керівник: Луценко С .М.

Актуальність. У сучасних умовах цифрової трансформації держави питання кібербезпеки набуває стратегічного значення. Публічне управління дедалі більше спирається на інформаційно-комунікаційні технології, що забезпечують швидкість, прозорість і ефективність управлінських процесів [1]. Водночас зростає й кількість кіберзагроз, які можуть порушити стабільне функціонування органів влади, поставити під загрозу національну безпеку, права та інтереси громадян. Забезпечення кібербезпеки стає ключовим елементом правового механізму публічного управління, оскільки потребує чіткої нормативно-правової регламентації, координації діяльності державних інституцій та впровадження сучасних технологічних рішень [2].

Мета роботи проаналізувати роль кібербезпеки у правовому забезпеченні публічного управління.

Основні положення. У сучасних умовах цифрової трансформації держави питання кібербезпеки набуває стратегічного значення. Водночас зростає й кількість кіберзагроз, які можуть порушити стабільне функціонування органів влади, поставити під загрозу національну безпеку, права та інтереси громадян. Забезпечення кібербезпеки стає ключовим елементом правового механізму публічного управління, оскільки потребує чіткої нормативно-правової регламентації, координації діяльності державних інституцій та впровадження сучасних технологічних рішень [3]. Кібератаки, витоки даних, деструктивні впливи на критичну інфраструктуру та інформаційні системи становлять серйозну загрозу для стабільного функціонування органів державної влади. Наслідки таких інцидентів можуть охоплювати не лише порушення роботи державних сервісів, а й завдання шкоди національній безпеці, порушення прав громадян, підрив довіри суспільства до державних інститутів [4]. Законодавча база має забезпечувати узгодженість дій різних державних органів, органів місцевого самоврядування, суб'єктів критичної інфраструктури та приватного сектору [5]. Серед ключових завдань правового регулювання – визначення процедур запобігання, виявлення та

реагування на кіберінциденти, встановлення вимог до інформаційних систем, формування стандартів управління ризиками. Окрім нормативного забезпечення, важливою складовою кібербезпеки є координація міжвідомчої взаємодії та впровадження сучасних технічних рішень. Йдеться про розвиток систем моніторингу, раннього виявлення загроз, побудову захищених комунікаційних каналів, впровадження криптографічних механізмів захисту даних. Технічні засоби кіберзахисту повинні доповнюватися управлінськими та організаційними заходами, які забезпечують системність та безперервність роботи з підтримки кіберстійкості державного сектору.

Висновки. Узагальнюючи викладене, можна стверджувати, що забезпечення кібербезпеки є однією з ключових передумов ефективного функціонування сучасної системи публічного управління. Цифрова трансформація не лише відкриває нові можливості для розвитку державних сервісів, а й формує додаткові ризики, пов'язані з уразливістю інформаційних систем та критичної інфраструктури. У цьому контексті кіберзагрози стають серйозним чинником, який впливає на стабільність управлінських процесів, захист прав громадян та рівень довіри суспільства до держави.

Список літератури

1. Закон України "Про електронні комунікації" від 16 грудня 2020 року № 1089-IX.URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення 01.04.2025)
2. Біленчук П.Д., Шевченко В.В. Електронне врядування: *навчальний посібник.* К.: Академія, 2015. 240 с.
3. Пацурківський П.С. Публічне управління і адміністрування: теоретико-правові засади. Чернівці: Чернівецький національний університет, 2017. 356 с.
4. Кравченко О.М. Цифровізація та правове регулювання публічних відносин: сучасні тенденції // *Держава і право.* 2022. №58.
5. Кириченко О.А. Електронне врядування в Україні: проблеми та перспективи розвитку // *Державне управління: теорія та практика.* 2021. № 1.

Відомості про авторів

Джунь Семен Сергійович, студент кафедри педагогіки, КЗ СОІППО, zakladzzso@gmail.com

Луценко Світлана Миколаївна, декан факультету підвищення кваліфікації та перепідготовки, КЗ СОІППО, к.н.з держ.упр, доцент, svitlana.lutsenko@soippo.edu.ua

Секція 3

ГЕЙМІФІКАЦІЯ ЯК ІНСТРУМЕНТ ФОРМУВАННЯ МОТИВАЦІЇ ДО ВИБОРУ СПЕЦІАЛЬНОСТЕЙ У СФЕРІ КІБЕРБЕЗПЕКИ СЕРЕД МОЛОДІ

Дзюба Д. Ю.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Харченко В. С.

Актуальність. Стрімкий розвиток кіберпростору сучасного суспільства призвів до зростання потреби у фахівцях у галузі кібербезпеки. Водночас багато абітурієнтів обирають IT-спеціальності неусвідомлено, без справжнього інтересу - переважно через моду або престиж. Частина школярів, які мають потенціал до IT чи кібербезпеки, не помічають цих напрямів через нестачу сучасних профорієнтаційних інструментів, здатних емоційно зацікавити та залучити. Одним із дієвих способів підвищення зацікавленості є гейміфікація – використання ігрових механік у неігровому контексті [1]. Вона робить навчання емоційно залученим, підсилює мотивацію й допомагає сформувати позитивне ставлення до IT [2].

Метою даної роботи є дослідження методів профорієнтаційної роботи та їх покращення через впровадження гейміфікації, підсиленої штучним інтелектом, для формування стійкої внутрішньої мотивації до навчання у сфері IT та кібербезпеки.

Основні положення. Аналіз існуючих рішень виконано за напрямами:

– традиційні методи. Дні відкритих дверей, друковані матеріали інформативні, але не викликають емоційної залученості [1];

– онлайн-платформи. Такі сервіси як, CodeCombat, Cisco Networking Academy використовують ігрові елементи, однак вони зосередженні на навчанні та бракує агітації [3];

– штучний інтелект. Системи на зразок Duolingo AI Tutor аналізують поведінку користувача й адаптують складність [4]. Подібні механізми можна застосовувати для профорієнтаційних ігор;

– емоційна взаємодія. Згідно з теорією Affective Computing R. Picard, системи, що розпізнають емоції, підсилюють ефективність навчання та викликають емпатію [5].

Зроблено висновки, що гейміфікація та штучний інтелект активно використовуються у навчанні. Водночас наявні профорієнтаційні інструменти не використовують потенціал гейміфікації та штучного

інтелекту. Запропоновано впровадження гейміфікації, підсиленої штучним інтелектом, як засобу мотивації вибору ІТ-спеціальностей. Система використовує бібліотеку OpenCV для розпізнавання облич, а TensorFlow Lite – для класифікації емоцій за попередньо натренованою моделлю. Аналіз поведінки користувача та персоналізацію сценарію реалізовано через мовну модель Ollama, що формує контекстні реакції гри та діалоги з користувачем.

Висновок. Гейміфікація може стати сучасним та ефективним інструментом профорієнтаційної роботи. Запропонований підхід має допомогти в формуванні внутрішньої мотивації у молоді до вибору спеціальностей у сфері інформаційних технологій та кібербезпеки. В одночас, гейміфікація не лише підвищує зацікавленість у молоді, а й сприяє усвідомленому вибору професійного напряму.

Список літератури

1. Li M., Ma S. Examining the effectiveness of gamification as a tool promoting teaching and learning in educational settings. Frontiers in Psychology. 2023. Vol. 14. Article 1253549. DOI: https://doi.org/10.3389/fpsyg.2023.1253549

2. Demmese F., Yuan X., Dicheva D. Evaluating the Effectiveness of Gamification on Students' Performance in a Cybersecurity Course. J. of The Colloquium for Information Systems Security Education. 2020. Vol. 8(1). P. 6–12. URL – https://cisse.info/journal/index.php/cisse/article/view/129 (дата звернення: 13.10.2025)

3. Lampropoulos G., Sidiropoulos A. Impact of Gamification on Students' Learning Outcomes and Academic Performance: A Longitudinal Study. Education Sciences. 2024. Vol. 14(4). Article 367. DOI: https://doi.org/10.3390/educsci14040367

4. Picard R. W. The Evolution of Affective Computing. Nature Machine Intelligence. 2023. P. 204–210.

5. UC Berkeley Center for Long-Term Cybersecurity. Gamification in Cybersecurity Education. SC Media Report. 2023.

Відомості про авторів

Дзюба Дмитро Юрійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.y.dziuba@student.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 3

ПРАВОВІ АСПЕКТИ ВИКОРИСТАННЯ БЛОКЧЕЙН/РОЗПОДІЛЕНИХ РЕЄСТРІВ ДЛЯ ЗБЕРЕЖЕННЯ ДОКАЗОВИХ ДАНИХ

Кондрачук С. С.
Дніпровський науковий українсько-американський ліцей Дніпровської міської ради, м. Дніпро, Україна
Науковий керівник: Кифорук Ю. М.

Актуальність. Активний розвиток цифрової економіки зумовлює широке впровадження технологій блокчейн та розподілених реєстрів у правову, фінансову, управлінську та криміналістичну практику. Однією з ключових сфер, де децентралізовані системи створюють принципово нові можливості, є збереження доказових даних, що потребують гарантій незмінності, цілісності та підтверджуваності. Блокчейн забезпечує фіксацію подій у хронологічно впорядкованих блоках, захищених криптографічними механізмами, що унеможливлює несанкціоновану модифікацію інформації після її запису. Це дозволяє розглядати такі записи як потенційно надійні електронні докази. Водночас неврегульованість їхнього правового статусу в Україні, суперечності з нормами захисту персональних даних та вимогами GDPR створюють значні юридичні виклики.

Метою роботи є аналіз правових аспектів використання блокчейну для збереження доказових даних, оцінка відповідності технології вимогам національного та міжнародного законодавства, а також визначення шляхів гармонізації нормативної бази України з європейськими стандартами.

Основні положення. У низці країн (США, Китай, Сінгапур, Японія) блокчейн-записи офіційно визнаються допустимими доказами. Необхідним є адаптування національного законодавства таким чином, щоб криптографічно підтверджена незмінність записів визнавалася достатньою підставою для встановлення їх автентичності без застосування централізованих підписів. Блокчейн може забезпечувати: фіксацію договорів та транзакцій; підтвердження авторського права та ланцюга володіння; – створення цифрових міток часу (timestamping); збереження криміналістичних даних та логів подій. Особливе значення має timestamping, який підтверджує факт існування документа в конкретний момент часу за допомогою хешу, що забезпечує високий рівень достовірності цифрових доказів. Основним бар'єром до юридичного впровадження блокчейну в Європі є конфлікт між незмінністю записів та

правом громадян на видалення персональних даних. GDPR гарантує можливість повного стирання даних, у той час як блокчейн за своєю природою не дозволяє зміну вже внесених блоків. Серед можливих рішень: зберігання у блокчейні лише хешів, а не самих персональних даних; використання off-chain систем із можливістю редагування; застосування шифрування, де видалення ключа дорівнює практичному «забуттю»; Self-Sovereign Identity (SSI), де користувач контролює власні дані. На правовому рівні необхідно забезпечити відповідність реалізації таких підходів принципам GDPR.

Висновки. Технології блокчейн і розподілених реєстрів відкривають суттєві можливості для розвитку електронного судочинства, забезпечуючи прозорість, незмінність та підтверджуваність доказових даних. Водночас їх повноцінне впровадження потребує вирішення низки правових аспектів, зокрема питань автентифікації інформації, захисту приватності, узгодження з GDPR та адаптації процесуального законодавства. Україна має потенціал для впровадження інновацій у сфері цифрової юстиції, однак це потребує розробки комплексної національної стратегії нормативного регулювання блокчейн-технологій.

Список літератури

1. European Union Blockchain Observatory and Forum. Blockchain and the GDPR. European Commission, 2023
2. Finck M. Blockchain and the General Data Protection Regulation. EPRS, 2019
3. Raskin M., Nanda S. Law and Technology in the Age of Blockchain. Harvard Journal of Law & Technology, 2022
4. Кифорук Ю.М, Кондрачук С.С..Створення аерокосмічного моніторингу забруднення океанів та морів виходами пластика // Дніпровська орбіта – 2025: матеріали XX наукових читань (22-24 жовтня 2025 р.) / Нац. центр аерокосмічної освіти молоді ім. О.М. Макарова, ДП "Конструкторське бюро "Південне" ім. М.К. Янгеля" Нац. музей космонавтики ім. С.П. Корольова, Дніпровський нац. ун-т ім. О. Гончара.– Дніпро, 2025.– С. 213-214

Відомості про авторів

Кондрачук Сніжана Станіславівна, учениця Дніпровського наукового українсько-американського ліцею Дніпровської міської ради, kondrachuks@ual.ukr.education

Кифорук Юрій Миколайович, вчитель інформатики Дніпровського наукового українсько-американського ліцею Дніпровської міської ради, kiforuk.yury@gmail.com

Секція 3

АНАЛІЗ ПАТЕНТОЗДАТНИХ РІШЕНЬ ТА МЕТОДІВ ВИБОРУ ФАКТОРІВ АВТЕНТИФІКАЦІЇ В БАГАТОФАКТОРНИХ СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ

Кручина Є. В.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Харченко В. С.

Актуальність. При розробленні багатофакторної системи контролю доступу (БСКД) особливо важливим є обґрунтування підходу до вибору множини факторів автентифікації. Зазвичай, при огляді джерел дослідники обмежуються аналізом наукових статей, доповідей, звітів, не надаючи уваги рішенням, які захищено патентами. Їх аналіз дозволяє більш ретельно оглянути стан галузі, виявити винахідницькі інженерні рішення та визначити можливості для покращення характеристик БСКД.

Метою дослідження є аналіз основних класифікаційних ознак і критичний патентних рішень щодо вибору методів автентифікації в БСКД. Для досягнення даної мети необхідно:

- визначити ключові слова, які описують галузь, обрати джерела інформації, виконати патентний пошук – сформувати множину патентів на БСКД для подальшого аналізу;
- визначити ознаки відповідних методів і засобів та класифікувати їх;
- здійснити порівняльній аналіз переваг та недоліків та окреслити вікно можливостей для розроблення інноваційного рішення для БСКД на підставі власної винахідницької ідеї.

Результати. Проведено огляд патентних матеріалів та їх порівняння за способом вибору методів автентифікації. Для аналізу було відібрано низку патентів США. Зокрема, визначено, наступні підходи до вибору методів автентифікації:

– поведінкові та аналітичні методи (US11936649B2 [3], US10630693B1 [1]), що базуються на аналізі звичок, транзакцій, та поведінки користувача. Такі системи забезпечують високий рівень персоналізації, однак мають проблеми з ресурсомісткістю, а також з конфіденційністю зібраних даних;

– контекстно-орієнтовані методи (US12363106B2 [4], US8656458B2, US9118656B2 [5]) використовують зовнішні фактори – геолокацію, дані з суміжних СКД або контекстну інформацію запиту. Їх перевагою є

непомітність для користувача, проте недоліком – обмежена точність і залежність від надійності зовнішніх джерел даних;

– методи з адаптивним вибором факторів (US9912657B2 [2]) базуються на розрахунку показника довіри, виходячи з динамічних параметрів (обчислювальна складність, середовище доступу), і демонструють високий потенціал безпеки, але мають обмеження з швидкодії й складності.

Висновки. Методи автентифікації в БСКД мають бути не тільки багатофакторними, але й адаптивними, для забезпечення вимог середовища та оточення. Проте, як показав аналіз, існуючі рішення не є збалансованими. Вони змушують обирати між безпекою та складністю, а також можуть мати проблеми з приватністю.

Описано методику огляду і надано критичний аналіз патентів на способи вибору методів автентифікації. Результати буде використано для створення і патентування гібридної, безпечної, адаптованої та зручної БСКД.

Список літератури

1. Adaptive authentication: пат. US10630693B1, США: H04L63/102; заявл. 06.04.2017 ; опубл. 21.04.2020
2. Adaptive multi-factor authentication system : пат. US9912657B2 Сполучені Штати Америки (США) : H04L63/083. № US14/968,676 ; заявл. 14.12.2015 ; опубл. 06.03.2018
3. Multi-factor authentication: пат. US11936649B2, США: H04L63/0861; заявл. 27.10.2021; опубл. 19.03.2024
4. Risk-based factor selection: пат. US12363106B2, США: H04L63/0853; заявл. 19.01.2023; опубл. 15.07.2025
5. Systems and methods for MFA: пат. US9118656B2, США: H04L63/0815; заявл. 25.01.2007; опубл. 25.08.2015

Відомості про авторів

Кручина Євгеній Валерійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.v.kruchyna@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 3

КІБЕРБУЛІНГ І БЕЗПЕЧНЕ СПІЛКУВАННЯ В ІНТЕРНЕТІ СЕРЕД МОЛОДІ

Орешко Д. В.
Харківський національний університет імені В. Н. Каразіна, м. Харків, Україна
Науковий керівник: Стяглик Н. І.

Актуальність. З поширенням соціальних мереж цифровий простір став основним середовищем спілкування молоді, але разом із новими можливостями зросла й кількість негативних проявів, зокрема кібербулінгу.

У контексті цифровізації кібербулінг перетворюється на серйозну соціальну загрозу, пов'язану з психологічною безпекою молоді та формуванням цифрової культури. Тому дослідження причин, форм прояву кібербулінгу та шляхів його попередження є важливим завданням для освітніх установ, батьків і державних структур.

Мета роботи полягає у вивченні ключових аспектів кібербулінгу та дослідженні практичних підходів до його подолання.

Основні положення. Кібербулінг має свої специфічні характеристики, які відрізняють його від традиційного булінгу. Основою цього явища є можливість швидкого поширення інформації, анонімність користувачів, відсутність чітких механізмів контролю та доволі низький рівень цифрової грамотності молоді.

Кібербулінг має низку характерних особливостей. По-перше, це публічність і швидкість поширення: образливий контент миттєво охоплює широку аудиторію. По-друге, анонімність агресора створює відчуття безкарності й провокує більш жорстоку поведінку. Постійність впливу – онлайн-агресія може тривати цілодобово та не має територіальних меж. Як наслідок – психологічний тиск на жертву (тривога, стрес, депресивні стани, ізоляція). А цифровий слід забезпечує тривале існування навіть видалених матеріалів.

Прикладом ефективної боротьби з кібербулінгом є проєкт BeKindOnline – цифрова платформа, спрямована на формування безпечної поведінки в інтернеті серед молоді та створення умов для раннього виявлення ознак кібернасильства, забезпечення психологічної підтримки користувачів, які постраждали від кібербулінгу.

Платформа включає: освітній модуль, що містить інтерактивні курси,

відеолекції та тренажери з безпечної поведінки в інтернеті; систему раннього виявлення агресії, яка аналізує повідомлення й коментарі з використанням алгоритмів штучного інтелекту для виявлення потенційно небезпечної поведінки; модуль анонімної допомоги, де реалізована можливість звернення до психологів; аналітичну панель, що дозволяє формувати статистику випадків кібербулінгу та розробляти рекомендації для навчальних закладів.

Інноваційність цієї платформи полягає у використанні алгоритмів штучного інтелекту для аналізу поведінки користувачів у режимі реального часу, що дозволяє оперативно виявляти ознаки агресії.

Висновки. З огляду на збільшення часу перебування молоді в інтернеті, подальший розвиток подібних систем на основі автоматизації та штучного інтелекту сприятиме формуванню безпечного цифрового середовища, зниженню ризиків кібербулінгу та підвищенню рівня цифрової культури суспільства.

Отже, BeKindOnline – це інноваційне рішення, що спрямоване на боротьбу з кібербулінгом та формування безпечної онлайн-поведінки серед молоді. Розвиток подібних ініціатив дозволить створити захищений та відповідальний цифровий простір.

Список літератури

1. Нестеренко А. Адміністративно-правова протидія кібербулінгу стосовно дітей: дис. канд. юрид. наук. Львів: Львівський національний університет імені Івана Франка, 2019

2. Пилипишина І. І. Протидія кібербулінгу як забезпечення права дитини на безпеку. Науковий вісник Ужгородського національного університету. 2024.

3. Kraut M. E. Children and Cyberbullying. Child Crime Prevention & Safety Center. URL – https://childsafety.losangelescriminallawyer.pro/children-and-cyberbullying.html

Відомості про авторів

Орешко Дар'я Василівна, студентка ННІ «Каразінський банківський інститут» ХНУ імені В.Н.Каразіна, daria.oreshko18@gmail.com

Стяглик Наталя Іванівна, завідувач кафедри інформаційних технологій та математичного моделювання ННІ «Каразінський банківський інститут» ХНУ імені В.Н.Каразіна, к.п.н., доцент, natalia.stiahlyk@karazin.ua

Section 3

VALIDATION OF MEASUREMENT ACCURACY OF SENSORS IN AEROSPACE MONITORING SYSTEMS OF OCEAN AND SEA POLLUTION BY PLASTIC WASTE

Milania Puchenina
Dnipro Scientific and Ukrainian-American Lyceum of the Dnipro City Council, Dnipro, Ukraine
Scientific adviser: Yurii Kyforuk

Relevance. The problem of ocean and sea pollution by plastic waste has reached the scale of a global environmental crisis. According to scientific organizations, hundreds of trillions of plastic particles circulate in the World Ocean, and the areas of garbage patches cover hundreds of thousands of square kilometers. Multilevel aerospace monitoring systems integrating satellite data, UAVs, autonomous buoys, and ground stations are used to track this phenomenon. Their measurement accuracy determines the reliability of estimating the boundaries of plastic accumulations, particle concentrations, and surface roughness characteristics. Calibration errors and sensor drift directly affect the mapping of polluted areas, analysis of garbage patch dynamics, assessment of cleanup operations, and modeling of plastic dispersion [1]. Therefore, validation of measurement accuracy is critical for the functional safety of aerospace monitoring systems.

Purpose. The objective of this study is to determine methods and algorithms for validating the measurement accuracy of sensors in aerospace systems for monitoring ocean and sea plastic pollution, to assess the impact of measurement errors on observation results, and to develop recommendations for improving the reliability of collected data.

Main Provisions. Functional safety requires each sensor to remain accurate throughout the observation cycle [2]. Even minimal drift can shift garbage patch boundaries, alter spectral indices (NDVI, FDI, NDRI), and affect segmentation and classification algorithms. Calibration errors: incorrect reference points, unsuitable lighting or weather conditions, outdated calibration models, imperfect reference panels, incorrect compensation algorithms; can result in systematic spectral offsets in visible and NIR channels. Sensor drift: aging of photoelements, radiation effects in space, thermal cycles, optical contamination, sensitivity degradation of matrices; drift of 1–3% in NIR or SWIR channels can shift mapped boundaries by tens of kilometers and generate false positive signals [3,4]. Methods in-situ measurements (buoys, water sampling, photogrammetric markers), cross-validation between satellites observing the same region, drift compensation modeling predicting optical degradation, comparison with stable

natural surfaces (Sahara desert, Antarctic ice fields, calm lakes). Validation of UAV and buoy sensors – UAVs test tables with known reflectance coefficients, fixed control markers on land, self-test before flight. Plastic detection accuracy dependency Detection of plastic relies on spectral signatures, NIR/SWIR indices, radar surface roughness, and machine learning classification algorithms; errors in sensor measurements cause misclassification (plastic vs. algae vs. foam), false positives, underestimated concentrations, incorrect centroid location of garbage patches, and misprediction of movement patterns. Use of cryptographic signatures for files, data integrity verification (SHA-256, HMAC), change logging, role-based access control, duplication of sensors for verification.

Conclusions. Calibration errors and sensor drift can significantly distort plastic accumulation maps. Accuracy of spectral and radar sensors directly affects ecological decision-making. Validation must include reference measurements, inter-sensor cross-checks, self-diagnostics, and drift modeling. Control points and calibration frequency must be clearly defined by sensor type. Cybersecurity of calibration data is integral to functional safety. Comprehensive validation ensures precise detection of plastic patches, accurate movement prediction, and enhances cleanup operation effectiveness.

List of references

1. Lebreton, L. et al. (2018). Evidence that the Great Pacific Garbage Patch is rapidly accumulating plastic. Scientific Reports, 8:4666

2. Eriksen, M. et al. (2014). Plastic pollution in the world's oceans: more than 5 trillion plastic pieces weighing over 250,000 tons afloat at sea. PLoS ONE, 9(12): e111913

3. European Space Agency (ESA). (2022). Sentinel Online Calibration and Validation Reports

4. Kyforuk Yu.M., Petrosian P.A., Kravchenko K.S., Puchenina M.R., Kondrachuk S.S., Andreev S.M. Creation of Aerospace Monitoring of Pollution of Oceans and Seas by Plastic Waste //Dnipro Orbit - 2025: Proceedings of the 20th Scientific Readings (October 22-24, 2025) / O.M. Makarov National Center for Aerospace Education of Youth, State Enterprise "Design Bureau 'Pivdenne' Named After M.K. Yangel," S.P. Korolov National Museum of Cosmonautics, O. Honchar Dnipro National University. -Dnipro, 2025. - pp. 213-214

Information about the authors

Milania Puchenina, student from Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, milaniapucenina@gmail.com

Yurii Kyforuk, computer science teacher from Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, kiforuk.yury@gmail.com

Секція 3

ЕТИЧНО-ПРАВОВІ НОРМИ ПУБЛІКАЦІЇ ДАНИХ ПРО ЗАБРУДНЕННЯ ОКЕАНІВ І МОРІВ ПЛАСТИКОМ У КОНТЕКСТІ СИСТЕМ АЕРОКОСМІЧНОГО МОНІТОРИНГУ

Сиваш Т. Т.
Дніпровський фаховий коледж радіоелектроніки, м. Дніпро, Україна
Науковий керівник: Кифорук Ю. М.

Актуальність. Проблема пластикового забруднення океанів є однією з найбільш критичних екологічних загроз сучасності: за даними міжнародних досліджень, у світовому океані нині циркулює понад 170 трлн частинок пластику [1]. Розробка систем аерокосмічного моніторингу дозволяє оперативно виявляти зони накопичення сміття, однак публікація таких даних має складний етично-правовий характер. Розкриття інформації про реальний рівень забруднення може суттєво впливати на рибальську галузь, туризм і прибережні економічні системи, формуючи ризики репутаційних та фінансових втрат [2]. Таким чином, постає потреба у визначенні прозорих, науково обґрунтованих і соціально відповідальних механізмів оприлюднення результатів супутникових спостережень.

Метою дослідження є формування етично-правових підходів до публікації даних про пластикове забруднення океанів, отриманих засобами аерокосмічного моніторингу, з урахуванням ризиків для рибальства, туризму, місцевих громад та міжнародних екологічних зобов'язань.

Основні положення. Відповідно до міжнародних норм – зокрема, Оргуської конвенції – екологічна інформація має бути максимально відкритою, але її поширення не повинно завдавати шкоди економічній безпеці або комерційним інтересам стейкхолдерів. У випадку даних про морське забруднення необхідно враховувати положення міжнародних морських стандартів, систем екологічної сертифікації рибальства та вимог щодо доказовості даних дистанційного зондування [3]. Публікація неперевірених даних здатна спричинити значні економічні наслідки для рибальських громад. Зокрема, численні дослідження про мікропластик демонструють, що навіть обмежені викиди можуть викликати надмірну суспільну реакцію, яка не відповідає реальним екологічним ризикам [4]. Тому система моніторингу повинна включати механізм «етичного фільтрування», що передбачає перевірку достовірності даних, оцінку можливих економічних наслідків та консультації з галузевими організаціями. Дані про локальні зони забруднення можуть впливати на

рибальські квоти, сертифікацію продукції та доступ до зовнішніх ринків. У системах дистанційного зондування (Sentinel-1/2) виявлені артефакти, які при неправильному тлумаченні можуть створювати хибну уяву про екологічну ситуацію [2]. Репутація чистоти узбережжя є ключовим фактором туристичної привабливості. Поширення карт забруднення без урахування сезонних явищ (штормові викиди, тимчасові сміттєві плями) може завдати шкоди туристичному бізнесу. Необхідно проводити оцінку наслідків оприлюднення даних (impact assessment) для туристичної галузі регіону. Система моніторингу повинна включати комунікацію між науковцями, державними структурами, рибальськими організаціями, екологічними службами та представниками туристичної індустрії.

Висновки. Публікація супутникових даних про пластикове забруднення повинна здійснюватися в умовах суворого дотримання етичних і правових норм. Важливим є баланс між відкритістю екологічної інформації та захистом інтересів економічно вразливих секторів — рибальства та туризму. Створення інтегрованої системи аерокосмічного моніторингу з етичним фільтром, правовою верифікацією і залученням стейкхолдерів дозволяє забезпечити достовірність даних і зменшити ризики їх некоректного використання.

Список літератури

1. Eriksen M. et al. A growing plastic smog: over 170 trillion particles in the oceans. PLOS ONE, 2023.
2. Sentinel-2 Satellite Imagery Overview. EOS Data Analytics.
3. Lehmköster J. World Ocean Review 4. 2015.
4. Nunes B.Z. et al. Microplastic contamination in marine protected areas. Science of the Total Environment, 2022.
5. Кифорук Ю.М Створення аерокосмічного моніторингу забруднення океанів та морів виходами пластика // Дніпровська орбіта – 2025: матеріали XX наукових читань (22-24 жовтня 2025 р.) / Нац. центр аерокосмічної освіти молоді ім. О.М. Макарова, ДП “Конструкторське бюро “Південне” ім. М.К. Янгеля” Нац. музей космонавтики ім. С.П. Корольова, Дніпровський нац. ун-т ім. О. Гончара.– Дніпро, 2025.– С. 213-214.

Відомості про автора

Сиваш Тимофій Тарасович, учень-член гуртка «МЕХАТРОНІКА_ДФКР» Дніпровського фахового коледжу радіоелектроніки, timofey.syvash@gmail.com
Кифорук Юрій Миколайович, керівник гуртка «МЕХАТРОНІКА_ДФКР», Дніпровського фахового коледжу радіоелектроніки, kiforuk.yury@gmail.com

Section 3

ACCOUNTABILITY FOR CYBERSECURITY INCIDENTS: NOTIFICATION, INVESTIGATION, AND REPORTING

Mariya Sobolieva
Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, Dnipro, Ukraine
Scientific adviser: Yurii Kyforuk

Relevance. The rapid digitalization of public and private sectors has caused a significant increase in cyber incidents. Cyberattacks today form part of hybrid threats capable of disrupting information systems, finances, and critical operations. Weak response mechanisms and violations of notification procedures amplify the consequences of incidents and increase national vulnerability. Therefore, clear legislative requirements for classification, reporting, and investigation of cyber incidents are crucial for effective cybersecurity [1].

Purpose. This study aims to summarize the legal obligations related to cybersecurity incident notification and describe the required structure and content of incident reports; analyze national regulations in comparison with EU and NIST standards.

Principal provisions. Cyber incidents are divided into Low-severity (local) disruptions; Medium-severity compromise of internal systems; High-severity attacks affecting large networks or critical services; Critical incidents threatening national security. Examples include: unauthorized access to databases malware penetration or ransomware encryption; web defacement and phishing campaigns; DDoS attacks blocking public services; attacks on medical, financial, or energy systems; personal data leaks; compromise of military or government systems. Notification Procedure Organizations must notify designated authorities within a defined timeframe. Failure to notify authorities may be treated as: negligence; concealment of a crime; breach of national cyber defense obligations [2]. Digital Forensic investigation includes: securing systems to prevent further damage, collection and preservation of evidence, maintaining chain of custody records, Log and memory analysis, Malware reverse engineering (if needed), Identification of attack vector, Documentation of every step. Digital evidence may include system logs, network packets, credentials used during the attack, screenshots and disk images, mobile device data; cloud platform logs. Public Disclosure, in cases involving: personal data; harm to public services; impact on critical infrastructure; massive financial losses. Organizations are obliged to publish a public statement describing what occurred, what data was affected, what users should do, how risk is mitigated, what future protections are planned.

This aligns with democratic transparency standards and reduces panic, disinformation, and reputational damage Types of Liability for Non-Compliance Administrative Liability. Fines applied for missing the notification deadline, submitting incomplete information, refusing to cooperate with authorities, Civil inability Organizations may receive lawsuits and must compensate: material losses, emotional harm (in case of personal data leaks), business interruption damages. Criminal liability applies in cases of intentional concealment of cyber incidents, sabotage of critical infrastructure, large-scale economic damage repeated negligence leading to systemic harm Criminal charges may apply to CEO, CISO, or IT staff. International Context EU GDPR strictly enforces reporting standards: USA Cyber Incident Reporting Act (CIRCIA) demands 72-hour disclosure; NATO Cyber Defense Policy treats cybersecurity incidents as collective threats;Japan and South Korea penalize companies for hiding breaches; Australia requires mandatory notification within 30 days; Israel integrates intelligence agencies into cyber reporting structures; Ukraine is gradually harmonizing with these global practices.

Conclusions. Efficient incident response and transparent reporting are key to ensuring cyber resilience. Compliance with legal and procedural requirements reduces operational and reputational losses and strengthens trust in the national digital ecosystem.

List of references

1. Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine," 2017.
2. GDPR - Regulation (EU) 2016/679 of the European Parliament.
3. NIST Computer Security Incident Handling Guide - NIST SP 800-61 Rev.2.
4. Kyforuk Yu.M., Petrosyan P.A., Kravchenko K.S., Puchenina M.R., Kondrachuk S.S., Andreev S.M. Creation of aerospace monitoring of pollution of oceans and seas by plastic emissions. // Dnipro Orbit – 2025: materials of the XX scientific readings (October 22–24, 2025). National Center for Aerospace Education of Youth named after O.M. Makarov, SE “Design Bureau Yuzhnoye” named after M.K. Yangel, National Museum of Cosmonautics named after S.P. Korolev, Dnipro National University named after O. Honchar. – Dnipro, 2025. – P. 213–214

Information about the authors

Mariya Sobolieva, student from Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, sobolieva@ual.ukr.education
Yurii Kyforuk, computer science teacher from Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, kiforuk.yury@gmail.com

Секція 3

МОДЕЛЬ ВЕРИФІКАЦІЇ ДОТРИМАННЯ GDPR ДЛЯ ІНТЕЛЕКТУАЛЬНОГО ОСВІТНОГО АСИСТЕНТА

Федоренко Д. Д.
Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна
Науковий керівник: Землянко Г. А.

Актуальність. Впровадження інтелектуальних ШІ-асистентів у освітнє середовище пов’язане з обробкою значних обсягів персональних даних (ПД) студентів та викладачів. Забезпечення легітимності застосування цієї технології та захист прав суб’єктів даних потребують суворої імплементації Регламенту GDPR (General Data Protection Regulation) [1]. Однак автоматизація обробки ПДн у ML-системах створює нові, нетривіальні ризики, пов'язані з дотриманням прав на інформування, видалення та обмеження обробки, що робить розробку моделей верифікації вкрай актуальним завданням [2].

Метою даної роботи є розробка формальної моделі верифікації дотримання вимог GDPR для ШІ-асистента в університетському середовищі. Модель має бути інтегрована в систему управління інформаційною безпекою (ISMS) та процеси контролю якості даних (Data Governance) для забезпечення безперервного комплаєнсу.

Основні положення. Основою роботи є формалізація ключових вимог GDPR [2], стосовно функцій асистента [3]. Це включає право на доступ, виправлення, обмеження обробки, право на забуття (видалення), право на переносимість та управління згодою (consent management). Модель зіставляє ці права з архітектурними компонентами системи, виявляючи точки, де можуть порушуватися права суб'єктів даних – від збору даних під час аутентифікації до їх використання в ML-моделях [3]. Пропонується набір автоматичних перевірок та контролів, що вбудовуються в CI/CD пайплайн (DevSecOps) та runtime-моніторинг. Для кожної вимоги визначаються детерміновані критерії валідації: наприклад, перевірка наявності в логах позначки про згоду (consent log) до початку обробки ПД, аудит термінів зберігання даних (data retention) та автоматичне застосування псевдонімізації відповідно до принципу мінімізації даних [4]. Особлива увага приділяється специфічним ризикам ML-систем. Описано алгоритми детектування порушень на рівні потоків даних, включаючи виявлення аномалій доступу до ПД та ризиків витоку даних через самі

моделі (наприклад, атаки типу «model inversion» або «membership inference») [3,4]. Аналізується необхідність псевдонімізації/анонімізації даних, що використовуються для тренування моделей, для дотримання принципу мінімізації даних. Модель також включає процедуру реагування на інциденти. Пропонуються алгоритми автоматичного переведення сервісів у безпечний режим (fail-safe) при виявленні критичного порушення GDPR, наприклад, несанкціонованого доступу до ПДн для негайного припинення обробки даних та запуску процедур звітності (breach notification).

Висновки. У роботі запропоновано формальну модель верифікації GDPR, представлену як набір специфікацій та автоматичних контролів для впровадження у життєвий цикл розробки та експлуатації ШІ-асистента. Очікувані результати включають формалізовану специфікацію перевірок, набір автоматичних тестів (compliance tests) та runtime-контролів, а також процедури реагування та звітності про порушення. Однією з неочевидних проблем є складність верифікації «права на забуття» у складних, навчених моделях, що потребує подальших досліджень у галузі «машинного розучування» (machine unlearning).

Список літератури

1. Pevnev, V., Tsuranov, M., Zemlianko, H., & Amelina, O. (2021). Conceptual model of information security. Lecture notes in networks and systems (pp. 158–168). Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-66717-7_14

2. GDPR for machine learning: data protection in AI development. GDPR Local. URL – https://gdprlocal.com/gdpr-machine-learning (дата звернення: 11.11.2025)

3. Birahim S. A. Contesting the algorithm: advancing a right to challenge AI decisions under the GDPR for algorithmic fairness. Transforming government: people, process and policy. 2025. DOI: https://doi.org/10.1108/tg-05-2025-0148

4. Modeling data protection and privacy: application and experience with GDPR / D. Torre et al. Software and systems modeling. 2021. Vol. 20, no. 6. P. 2071–2087. DOI: https://doi.org/10.1007/s10270-021-00935-5

Відомості про авторів

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

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

Section 3

REQUIREMENTS FOR ALGORITHM TRANSPARENCY AND THEIR LEGAL REGULATION IN AEROSPACE SYSTEMs FOR MONITORING OCEAN PLASTIC POLLUTION

Myroslava Sheina
Dnipro Scientific and Ukrainian-American Lyceum of the Dnipro City Council, Dnipro, Ukraine
Scientific adviser: Yurii Kyforuk

Relevance. Modern aerospace monitoring systems that use satellite data from Sentinel-1, Sentinel-2, and Sentinel-3 to detect ocean plastic pollution actively integrate machine learning algorithms and automated surface classification. At the same time, such systems become vulnerable to cyberattacks and data manipulation, which threatens the quality of environmental monitoring and international environmental decision-making [1].

A persistent challenge is maintaining a balance between the commercial secrecy of algorithm developers and the right of states and the scientific community to verify the accuracy of the obtained results. Requirements for algorithmic transparency are gradually being formalized in international standards – the EU AI Act, OECD principles, and ISO/IEC standards [2].

Purpose. The aim of the study is to identify the legal and technical factors regulating the transparency of artificial intelligence algorithms in aerospace systems for monitoring ocean pollution, as well as to develop approaches to ensuring their cyber-resilience and auditability.

Principal provisions. Algorithm transparency as a prerequisite for cybersecurity. Algorithms for spectral image segmentation, surface roughness detection, and neural-network models for classifying plastic waste must be accompanied by open accuracy metrics (precision, recall, F1), which constitute a minimal level of transparency without disclosing the source code [1]. Black-box vs white-box in the context of legal regulation. White-box approaches ensure reproducibility and legal examination, which is essential when confirming environmental damage. Black-box models are permitted in monitoring systems only if technical documentation, operation logs, and the possibility of independent result verification via validation datasets are publicly available [2].

Legal support for independent algorithm evaluation. International practice employs «controlled transparency» regimes, which include: providing technical models to accredited auditors; mandatory documentation of the model creation chain (data–model lineage); compliance with ISO/IEC 23053 and 23894

standards on AI cybersecurity [3]. Data and model protection in satellite ecosystems. Monitoring systems that use geoportals (Google MyMaps) and satellite classification tools are vulnerable to: substitution of satellite data; modification of segmentation results; model attacks (adversarial perturbations) capable of imitating plastic patches.

This necessitates the implementation of certified cybersecurity procedures and continuous security monitoring [1,4]. Legal liability for inaccurate algorithmic data. According to environmental and international information law, states that use satellite data for environmental decision-making are responsible for their accuracy. This requires legally establishing the principles of explainable AI and auditability in monitoring systems [3].

Conclusions. The effectiveness of aerospace systems for monitoring ocean plastic pollution depends not only on algorithmic accuracy but also on the legal regulation of transparency, cyber-resilience, and the possibility of independent evaluation. Ensuring a balance between the protection of commercial information and the right to verify scientific results is a key condition for trust in algorithmic solutions and for international environmental cooperation.

List of references

1. Kyforuk Yu.M. Development of aerospace monitoring of ocean and sea pollution by plastic discharges // Dnipro Orbit – 2025: Proceedings of the 20th Scientific Readings (22–24 October 2025) / National Center for Aerospace Education of Youth named after O.M. Makarov, Yuzhnoye Design Office named after M.K. Yangel, S.P. Korolyov National Museum of Cosmonautics, Oles Honchar Dnipro National University. Dnipro, 2025. Pp. 213–214
2. OECD. OECD Principles on Artificial Intelligence. 2019
3. ISO/IEC 23053:2022. Framework for Artificial Intelligence (AI) Systems Using Machine Learning
4. European Commission. Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (EU AI Act), 2021

Information about the authors

Myroslava Sheina, student from Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, sheinam@ual.ukr.education
Yurii Kyforuk, computer science teacher from Dnipro Scientific Ukrainian-American Lyceum of the Dnipro City Council, kiforuk.yury@gmail.com

АЛФАВІТНИЙ ВКАЗІВНИК / ALPHABETICAL POINTER

АЛФАВІТНИЙ ВКАЗІВНИК / ALPHABETICAL POINTER

АЛФАВІТНИЙ ВКАЗІВНИК / ALPHABETICAL POINTER

ЗМІСТ

CONTENTS

СТУДЕНТСЬКА КОНФЕРЕНЦІЯ ІНФОРМАЦІЙНА, ФУНКЦІЙНА і КІБЕРБЕЗПЕКА СКІФіК

Відповідальний за випуск Г. А. Землянко

Відповідальність за достовірність поданих матеріалів, наведених фактів, цитат, коректність посилань, а також за відсутність інших порушень академічної доброчесності несуть їхні автори

STUDENT CONFERENCE "INFORMATION, FUNCTIONAL AND CYBERSECURITY" SCIFiC

Responsible for Publication: Heorhii Zemlianko

The authors are responsible for the accuracy of the submitted materials, the correctness of the presented facts, citations, and references, as well as for the absence of any other violations of academic integrity

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 60x84/16. Ум. друк. арк. 11.86. Тир. 100 прим. Зам. 846.

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