КАФЕДРА ТВЕРДОТІЛЬНОЇ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УЖГОРОДСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ

Закарпатське відділення УКРАЇНСЬКОГО ФІЗИЧНОГО ТОВАРИСТВА

АКАДЕМІЯ ТЕХНОЛОГІЧНИХ НАУК УКРАЇНИ

27 листопада 2025

УЖГОРОД

VIII НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

"ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ЖИТТІ СТУДЕНТІВ ТА МОЛОДИХ НАУКОВЦІВ ЗАКАРПАТТЯ"

27 листопада 2025 року

ТЕЗИ ДОПОВІДЕЙ

УЖГОРОД - 2025

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Морозов А. О. – Почесний Голова, д.тех.н., професор, Заслужений діяч науки і техніки України, академік НАН України, академік Міжнародної Академії інформатики, Президент Академії технологічних наук України;

Смоланка В. І. – Співголова, д. мед. н., професор, ректор УжНУ, Заслужений лікар України, президент Української асоціації нейрохірургів, член тренувального комітету Європейської асоціації нейрохірургічних товариств;

Кучер Я. – Співголова, заступник голови Закарпатської ОВА з питань цифрового розвитку;

Різак В. М. – заступник голови, д. фіз-мат. н., професор, завідувач кафедри ТЕІБ, Заслужений діяч науки і техніки України, член Американського фізичного товариства і Голова ЗВ УФТ, академік та керівник Закарпатського осередку АТН України;

Корченко О. Г. – перший проректор Державного університет інформаційно-комунікаційних технологій, член-кореспондент НАН України, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, Заслужений діяч науки і техніки України, Президент ГО "Асоціація спеціалістів кібербезпеки" ;

Маркевич П. В. – Начальник Управління Державної служби спеціального зв'язку та захисту інформації України в Закарпатській області;

Танчинець М. М. – заступник начальника відділу протидії кіберзлочинам в Закарпатській області Департаменту кіберполіції Національної поліції України;

Повхан І. Ф. – к. т. н., декан факультету інформаційних технологій УжНУ;

Пагіря М. М. – д. фіз.-мат. н., професор кафедри ТЕІБ, член-кореспонде́нт Академії технологічних наук України;

Корченко А. О. – д. тех. н., професор кафедри ТЕІБ ;

Різак М. В. – д.юр. н., професор кафедри технічних систем кіберзахисту Навчально-наукового інституту кібербезпеки та захисту інформації, член-кореспонде́нт Академії технологічних наук України;

Мулеса П. П. – д.п.н., завідувач кафедри кібернетики і прикладної математики УжНУ;

Біланич В. С. – к. фіз-мат. н., завідувач кафедри прикладної фізики та квантової електроніки УжНУ, академік Академії технологічних наук України;

Горват П. П. – к. фіз-мат. н., завідувач кафедри комп'ютерних систем та мереж УжНУ;

Попович Н. І. – к. фіз-мат. н., доцент УжНУ;

Матьовка Т. В. – к.ек.н., доцент УжНУ;

Мисло Ю. М. – к. ф.-м. н., доцент УжНУ;

Лісовий У. – студент УжНУ;

Джанда А. – студентка УжНУ.

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС ОБРОБКИ АКУСТИЧНИХ СИГНАЛІВ ДЛЯ ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЇ БПЛА В РЕАЛЬНОМУ ЧАСІ

Євдокімов Михайло Анатолійович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури І1 року навчання, спеціальність F5 «Кібербезпека»

У результаті виконання роботи встановлено, що в сучасних умовах зростає потреба у створенні ефективних систем виявлення та ідентифікації безпілотних літальних апаратів(БПЛА) ударного типу, зокрема «Шахед», які становлять значну загрозу для об’єктів критичної інфраструктури та безпеки держави. Обмеження традиційних радіолокаційних і оптичних засобів виявлення зумовлюють актуальність застосування пасивних акустичних методів моніторингу, здатних функціонувати в умовах завад, складного рельєфу та радіомовчання противника.

Проаналізовано фізичні джерела акустичних сигналів БПЛА та досліджено основні методи цифрової обробки акустичних сигналів, зокрема спектральний, тональний, автокореляційний і кепстральний аналіз. Обґрунтовано доцільність використання комбінованого спектрально-кепстрального підходу для виділення інформативних ознак акустичної сигнатури літальних апаратів, що забезпечує підвищену стійкість до шуму та змін умов поширення звуку. В результаті теоретичного проектування сформовано архітектурну модель програмно-апаратного комплексу пасивного акустичного моніторингу, яка включає підсистему збору акустичних даних, модуль попередньої фільтрації, алгоритми виділення ознак та блок ідентифікації. Проведено моделювання обробки акустичних сигналів, що

імітують роботу двигуна та пропелерної групи БПЛА типу «Шахед», і виконано оцінювання ефективності виявлення в умовах наявності фонового шуму.

Отримані результати розглядаються як можливість застосування акустичних методів для раннього виявлення та первинної ідентифікації ударних БПЛА і можуть бути використані як науково-методична основа для подальшої практичної реалізації систем акустичного моніторингу в автоматизованих комплексах забезпечення безпеки.

ВПЛИВ АРХІТЕКТУРИ СИСТЕМИ НА РІВЕНЬ БЕЗПЕКИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ: ЦЕНТРАЛІЗОВАНІ VS ДЕЦЕНТРАЛІЗОВАНІ РІШЕННЯ

Матвіїв Юрій Юрійович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
аспірант фізичного факультету

Сучасні системи електронного голосування (E-voting), окрім забезпечення безпеки, стикаються з унікальною вимогою — суперечністю між прозорістю процесу (transparency) та таємницею волевиявлення (приватністю) (privacy). Ключовим фактором, що визначає стійкість системи до атак та маніпуляцій, а також рівень довіри виборців, є її архітектура. Існують класичні централізовані моделі (client-server), які, наприклад, успішно функціонують в Естонії, та нові децентралізовані підходи на базі технології розподіленого реєстру (DLT (Distributed Ledger Technology)/Blockchain).

Централізовані архітектури

Історично перші системи e-voting будувалися на класичній веб-архітектурі. Найяскравішим прикладом є естонська система i-Voting [1].

Принцип роботи: у такій моделі існує центральний сервер (або кластер серверів), який адмініструється державною виборчою комісією. Голос виборця шифрується на клієнтському пристрої відкритим ключем системи, передається через захищений канал (TLS) і зберігається в центральній базі даних. Для перевірки права голосу використовується інфраструктура відкритих ключів (PKI) та цифровий підпис виборця.[2]

Переваги централізації:

- Швидкість та масштабованість: Централізовані БД (SQL/NoSQL) здатні обробляти мільйони транзакцій за секунду, що критично важливо в пікові моменти голосування.

- простота управління та впровадження: У разі виявлення критичної вразливості адміністратор може миттєво зупинити систему, оновити ПЗ («патч») та відновити роботу.
- сумісність із традиційними реєстрами виборців та державними інформаційними системами;
- юридична відповідальність: є чітко визначений суб'єкт (адміністратор сервера), який несе відповідальність за збереження даних.

Головним недоліком є проблема Single Point of Failure (SPOF) - єдиної точки відмови.[3] Компрометація центрального сервера або доступ до нього зловмисника може дозволити:

- змінити результати голосування;
- видалити або модифікувати бюлетені;
- здійснити масове викривлення даних без можливості виявлення;
- виконати DDoS-атаку, що паралізує виборчий процес.

Наприклад, системний адміністратор з правами *root* теоретично має можливість непомітно модифікувати базу даних або журнали подій (logs). Довіра до такої системи дорівнює довірі до персоналу, що її обслуговує.

Проблема «Чорної скриньки»: для спостерігачів процес підрахунку голосів є непрозорим. Вони бачать лише вхідні дані (зашифровані бюлетені) та вихідний результат, але не можуть гарантувати, що програмний код на сервері виконав саме ті дії, які декларуються. Це створює ризики маніпуляцій.[2]

Децентралізовані рішення

Використання блокчейну пропонується як засіб усунення потреби в «довіреній третій стороні». Головна ідея полягає у розподіленому зберіганні та обробці даних, коли кожен голос фіксується у ланцюжку блоків, копія якого доступна кільком незалежним вузлам. Це усуває проблему центральної точки відмови та підвищує стійкість до спроб модифікації даних.

Переваги:

- блокчейн гарантує незмінність даних (immutability). Кожен голос записується в блок, який криптографічно пов'язаний з попереднім.

- Захист від модифікації**:** щоб змінити вже записаний голос, зловмиснику потрібно отримати контроль над понад 51% обчислювальної потужності мережі (у випадку Proof-of-Work) або валидаторів (Proof-of-Stake), що робить атаку економічно невигідною або технічно неможливою для більшості акторів.
- розподіл довіри між багатьма вузлами, що усуває залежність від одного адміністратора;
- підрахунок голосів може виконуватися автоматично через смарт-контракти, код яких є відкритим і перевіреним аудиторами.

Критичні проблеми безпеки децентралізації - попри популярність, блокчейн створює нові вектори загроз, описані в звітах MIT [4]:

- Конфлікт приватності: блокчейн за своєю природою є прозорим реєстром. Якщо адресу гаманця виборця можна пов'язати з його особою, таємниця голосування порушується назавжди. Рішенням є використання складних криптографічних примітивів:
  - Ring Signatures (Кільцеві підписи): приховують відправника серед групи користувачів.
  - Zero-Knowledge Proofs (доказ з нульовим розголошенням): дозволяють довести право на голос і факт голосування, не розкриваючи самого вибору. Однак це значно ускладнює систему і підвищує вимоги до клієнтських пристроїв;
  - гомоморфне шифрування: дозволяє виконувати певні математичні дії із зашифрованим текстом й отримувати зашифрований результат, який відповідає результату аналогічної операції, що проводиться з відкритим текстом;
- масштабованості**,** оскільки обробка транзакцій може бути повільнішою, ніж у централізованих системах [5];
- потенційної залежності від конкретного консенсусного механізму, який може бути вразливим до атак типу 51% або специфічних маніпуляцій у мережі;

- неможливість відкату: Якщо зловмисник викраде приватний ключ виборця і проголосує, в блокчейні неможливо «видалити» цю транзакцію.

Вразливість клієнтської сторони: спільна проблема архітектур

Важливо зазначити, що ані централізована, ані децентралізована архітектура не вирішують проблему безпеки кінцевого пристрою (Endpoint Security). Якщо комп'ютер або смартфон виборця інфіковано шкідливим ПЗ, вірус може підмінити вибір користувача до моменту шифрування та відправки.

- У централізованій системі сервер отримає легітимний, але підроблений пакет.
- У блокчейн-системі смарт-контракт запише підроблений голос навічно. Це підтверджує тезу про те, що перенесення голосування на блокчейн не робить його автоматично безпечним, якщо вхідні дані скомпрометовані ("Garbage In, Garbage Out").

Синтез рішень: Наскрізна верифікованість (E2E-V) та гібридні моделі

Сучасний науковий консенсус схиляється до гібридних архітектур, які впроваджують властивість End-to-End Verifiability (E2E-V) [6].

Концепція E2E-V полягає у тому, що система повинна надавати математичні докази коректності на трьох етапах, незалежно від типу бази даних:

1. Cast-as-intended: Виборець може перевірити (наприклад, через QR-код або інший пристрій), що його зашифрований голос чітко відповідає його вибору.
2. Recorded-as-cast: Виборець може перевірити наявність свого зашифрованого голосу в публічному списку.
3. Tallied-as-recorded: Будь-який зовнішній аудитор може перевірити правильність математичного підрахунку всіх голосів без їх розшифрування. Це досягається за допомогою гомоморфного шифрування (додавання шифротекстів дає суму голосів) або Mix-nets (перемішування голосів для розриву зв'язку з виборцем).

Роль архітектури в гібридній моделі: у найперспективніших моделях пропонується використовувати:

- Централізований сервер для автентифікації (через державні ID) та видачі сліпих токенів (Blind Signatures).
- Публічний дозвільний блокчейн (Permissioned Blockchain) виключно як «Дошку оголошень» (Public Bulletin Board). Тут зберігаються лише зашифровані хеші голосів. Це не дозволяє адміністратору непомітно видалити голос (бо хеш є в публічному реєстрі), але знімає навантаження складної логіки з блокчейну [7].

Висновки

1. Просте перенесення електронного голосування на блокчейн не вирішує фундаментальних проблем безпеки, а часто ускладнює їх через неможливість виправлення помилок та конфлікт з таємницею голосування.
2. Централізовані системи залишаються вразливими до внутрішніх атак та мають низький рівень публічної довіри через непрозорість процесів.
3. Оптимальним шляхом розвитку є впровадження протоколів наскрізної верифікованості (E2E-V), тобто організація гібридної системи, де критично важливі процеси (наприклад, автентифікація) залишаються централізованими та керуються державними органами, а зберігання і перевірка бюлетенів (у зашифрованому вигляді) відбуваються у децентралізованому середовищі для аудиту результатів, забезпечуючи математично доведену чесність виборів.

1. Офіційний портал Valimised.ee. URL: https://www.valimised.ee/en/internet-voting/more-about-i-voting/introduction-i-voting (дата звернення: 25.11.2025)
2. Heiberg, S., Willemson, J. "Verifiable Internet Voting in Estonia". IEEE 6th International Conference on Cyber Conflict.
3. Ohize, H.O., Onumanyi, A.J., Umar, B.U. et al. Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges. Cluster Comput 28, 132 (2025).
4. Specter, M. A., Koppel, J., & Weitzner, D. J. "Going from Bad to Worse: From Internet Voting to Blockchain Voting". Journal of Cybersecurity.

5. Пащенко І. М., Яланецький В. А. “Централізовані та децентралізовані системи електронного голосування”. URL: https://ela.kpi.ua/server/api/core/bitstreams/e8041cd3-8f52-4e51-b258-89aa49a65051/content (дата звернення: 25.11.2025)

6. Benaloh, J., Rivest R. et al. "End-to-End Verifiability". (2014).

7. N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," in IEEE Software, vol. 35, no. 4, pp. 95-99, July/August 2018.

АПАРАТНИЙ СПІВПРОЦЕСОР ЦОС ДЛЯ ПРИСКОРЕНОГО ВЕЙВЛЕТ ПЕРЕТВОРЕННЯ

Махров Валентин Володимирович

ДВНЗ "Ужгородський національний університет"
88000, Ужгород, вул. Університетська, 14
магістр 2-го курсу, спеціальність 123 "Комп'ютерна інженерія"

Використання відкритих стандартів архітектур обчислювальних пристроїв є важливим етапом у розробці комп'ютерних систем та спеціалізованих пристроїв. Серед таких стандартів виділяються *SPARC*, *x*86-*x64*, *ARM* та *RISC-V*, які забезпечують високий рівень сумісності та широкі можливості інтеграції.

RISC-V використовує обмежений набір команд, що сприяє зниженню складності проєктування та виконання інструкцій, що призводить до вищої продуктивності та меншого споживання енергії. Однією з ключових переваг *RISC-V* є відкритість, що дозволяє розробникам вільно використовувати та модифікувати архітектуру відповідно до своїх потреб, тим самим створюючи простір для проведення різноманітних інженерних досліджень, а також для ефективної конкуренції як із комерційними розробниками, так і з іншими фахівцями у технічній галузі [1].

Алгоритми цифрової обробки сигналів стрімко еволюціонують через зростаючу складність додатків у сфері телекомунікації, аудіо та відео обробки, розпізнавання зображень. Оскільки алгоритми стають складнішими, вони вимагають значної обчислювальної потужності. Ця потреба підштовхує до розробки більш продуктивних процесорів, архітектур та оптимізованих програмних рішень, щоб наблизити продуктивність процесорів до вимог. Залежно від вимог, обчислення алгоритмів ЦОС можуть виконуватися окремим спеціалізованим вузлом, процесором або апаратним співпроцесором, вбудованим у структуру основного процесора. Використання останнього

підходу значно зменшує вимоги до основного процесора та сприяє покращенню загальної ефективності обчислень [2-7].

Вейвлет перетворення є підходом обробки сигналів, що використовується для декомпозиції та синтезу нестаціонарних сигналів з високою точністю. Перетворення є альтернативним інструментом традиційним методам представлення час-частота, таким як дискретне перетворення Фур'є та дискретне косинусне перетворення. Завдяки можливості представлення з кількома роздільними можливостями, вейвлет перетворення використовується: для аналізу перехідних процесів; комп'ютерному баченні; стисненні зображень та інших аудіовізуальних застосуваннях [2].

Під час виконання алгоритму безпосередньо процесором необхідно постійно записувати/читати в/з комірки пам’яті. Час доступу до пам'яті в декілька разів перевищує час тактового сигналу процесора. Відсутність повноцінного співпроцесора для виконання алгоритмів в універсальних процесорах та процесорах ЦОС є важливою проблемою. Також, системи з одноядерними процесорами працюють під керуванням операційних систем реального часу, які здійснюють перемикання між задачами через певні проміжки часу. Тому, коли в системі одночасно виконується багато задач, серед яких є задача цифрової обробки сигналів, обчислювальні ресурси процесора розподіляються між усіма задачами порівну. У результаті це призводить до зменшення пропускної здатності системи під час обробки сигналів. Тому, є актуально розробка структури співпроцесора ЦОС на основі ядра *RISC-V* архітектури, що виконує вейвлет перетворення [5-7].

Результатом проєктування є конвеєрний векторний співпроцесор, що дає можливість паралельної обробки даних розрядністю до 32-х біт із можливістю одночасного опрацювання чотирьох 32-бітних операндів. Векторне розширення доповнено однією векторною інструкцією, що призначена для прискорення обчислень вейвлет перетворення. Векторний співпроцесор впроваджено у структуру конвеєрного процесора *RISC-V* архітектури, як окремий функціональний модуль.

Модель запропонованого співпроцесора ЦОС розроблена для мікросхеми програмованої логіки *Xilinx SPARTAN* 6, що має достатній набір програмованих логічних елементів (*LUT*), елементів пам'яті (*RAMB16BWER*), тригерів, модулів ЦОС (*DSP48A1*) та інших вбудованих компонентів.

Максимальна частота співпроцесора цифрової обробки складає 250 МГц. Знайдено кількість тактів, необхідну для виконання вейвлет перетворення. Для 1024 точок співпроцесору необхідно 20224 тактів, час виконання при частоті 250 МГц – 80.89 мкс. Для 2048 точок співпроцесору необхідно 40448 тактів, час виконання при частоті 250 МГц – 161.79 мкс.

1. Patterson D. A. Computer Organization and Design. The Hardware/Software Interface: RISC–V Edition / D. A. Patterson, J. L. Hennessy. – California : Morgan Kaufmann Publishers, 2018. – 1665 p.

2. Miner N. E. An Introduction to Wavelet Theory and Analysis. Office of Scientific and Technical Information (OSTI), 1998. URL: https://doi.org/10.2172/1896

3. Improved Parallel Implementation of 1D Discrete Wavelet Transform Using CPU-GPU / E. Rodriguez-Martinez et al. Electronics. 2023. Vol. 12, no. 16. P. 3400. URL: https://doi.org/10.3390/electronics12163400

4. Bae C., Lee S., Jung Y. High-Speed Continuous Wavelet Transform Processor for Vital Signal Measurement Using Frequency-Modulated Continuous Wave Radar. Sensors. 2022. Vol. 22, no. 8. P. 3073. URL: https://doi.org/10.3390/s22083073

5. Shahbahrami A., Juurlink B., Vassiliadis S. Performance Comparison of SIMD Implementations of the Discrete Wavelet Transform. 2005 IEEE International Conference on Application-Specific Systems, Architecture Processors (ASAP'05), Samos, Greece. URL: https://doi.org/10.1109/asap.2005.51

6. Vectorization of the 2D wavelet lifting transform using SIMD extensions / D. Chaver et al. International Parallel and Distributed Processing Symposium (IPDPS 2003), Nice, France. URL: https://doi.org/10.1109/ipdps.2003.1213416

7. The FreeRTOS Reference Manual [Electronic resource]. – Access mode: https://www.freertos.org/media/2018/FreeRTOS_Reference_Manual_ V10.0.0.pdf

КОЛИ ЛОПНЕ AI-БУЛЬБАШКА?

Товтин Ярослав Ярославович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури 1 року навчання, спеціальність F5 «Кібербезпека»

Поява та стрімке зростання індустрії штучного інтелекту дедалі частіше порівнюють із формуванням технологічного «пузиря». Пузир у цьому контексті означає різке збільшення вартості та очікувань, які не підкріплені реальними економічними результатами. Ситуація нині нагадує кризу доткомів початку 2000-х, коли інвестиції вкладалися не в реальні бізнес-моделі, а в сам факт належності до трендової сфери. Так само й сьогодні компанії масово впроваджують AI-рішення, іноді лише для галочки, а інвестори вкладають кошти у будь-які проєкти з позначкою «AI».

Попри гучні заяви про революційний потенціал штучного інтелекту, реальна вигода для бізнесу часто виявляється значно нижчою за очікування. У багатьох сферах AI справді підвищує зручність роботи і зменшує рутину, але це рідко трансформується у зростання прибутку. Деякі компанії, як-от IBM, навіть після автоматизації змушені були знову наймати персонал, у тому числі для обслуговування AI-інфраструктури. Gartner повідомляє, що значна частина експериментальних POC-проєктів не показує бажаних результатів, що підсилює скепсис до впроваджень.

Важливу роль у формуванні AI-гіперінфляції відіграє Nvidia, яка стала ключовим постачальником обчислювального обладнання для AI. Компанія інвестує мільярди доларів у OpenAI, CoreWeave та інші структури, що у відповідь купують її обладнання. Так створюється замкнене коло, яке штучно підтримує попит і збільшує ринкову капіталізацію учасників. Водночас OpenAI, попри величезну оцінку, працює у збиток і змушена брати позики, що робить її фінансову модель нестійкою. За оцінками Bain, AI-компаніям потрібно буде

генерувати близько 2 трильйонів доларів до 2030 року лише для покриття інфраструктурних витрат, але цього досягти майже неможливо — прогнозується дефіцит у 800 мільярдів.

Додатковим чинником перегріву є брак електроенергії: нові дата-центри вимагають величезних ресурсів, перевантажують мережі та суперечать колишнім екологічним гаслам індустрії. Попри це, компанії продовжують експансію, намагаючись виправдати зростаючі інвестиції та підтримати інтерес інвесторів. Однак навіть невеликий тригер може спричинити обвал — приклад моделі DeepSeek, яка нібито була навчена за значно менші кошти, вже призвів до падіння акцій Nvidia.

Аналітики сходяться на думці, що у разі падіння ринку частина компаній збанкрутує або буде поглинута більшими гравцями, але сама технологія штучного інтелекту не зникне. Як і після кризи доткомів, ринок очиститься і залишить кількох найбільш ефективних та стійких гігантів. Попри заперечення Дженсена Хуанга та Сема Альтмана, навіть Білл Гейтс визнає, що ринок AI переоцінений і демонструє класичні ознаки пузыря. Зрештою все покаже час, але сьогоднішня ситуація свідчить про значний дисбаланс між реальними можливостями технології та очікуваннями інвесторів та великого бізнесу.

РОЗРОБКА UI/UX ДОДАТКУ ДЛЯ ВІДОБРАЖЕННЯ МОНІТОРИНГУ ЕКОЛОГІЧНОГО СТАНУ МІСТА

Носок Ніколетта Сергіївна

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студентка 3-го курсу, спеціальність 125 «Кібербезпека»

В даному часі екологічний моніторинг потребує не лише доступу до правдивої інформації, але й створення гнучких, адаптивних інструментів, які можуть у реальному часі збирати, обробляти й аналізувати дані, здійснюючи відстеження навколишнього середовища.

Метою дослідження стало об’єднання передових інформаційних технологій, таких як Інтернет речей (IoT) , технології розумного дому, розумного міста, а також БПЛА та їх можливостей для побудови екологічної платформи для міста Ужгород та безпосередньо дослідження складової кібербезпеки на її основі. Попри інтенсивний розвиток концепції розумного міста, увага здебільшого приділяється питанням електрифікації, оптимізації трафіку та цифровізації послуг, в той час як екологічна безпека часто залишається недостатньо опрацьована. Це вимагає впровадження новітніх рішень, спрямованих на захист довкілля. Сучасні наукові дослідження визначають певні напрями розвитку систем моніторингу довкілля. Інтеграція Інтернету речей (IoT) і великих даних (BigData), які дозволяють встановлювати мережі сенсорів, що збирають інформацію про стан атмосфери, води, ґрунту в режимі реального часу. За даними дослідження , використання IoT у моніторингу підвищує оперативність збору даних на 40% у порівнянні з традиційними методами. Водночас обробка великих обсягів даних із застосуванням хмарних технологій та штучного інтелекту (AI) дає змогу прогнозувати екологічні зміни і вчасно попереджати про небезпеку. Це також

можна використати і в українському досвіді, коли відбувається повна руйнація міст, датчики є набагато ефективніші ніж метеостанції та центри вимірювань. Мобільні технології стали важливим каналом донесення екологічної інформації, це є ще один основний напрям. За даними World Economic Forum (2022), близько 68% населення у містах розвинених країн використовує мобільні додатки для отримання даних про якість повітря . Прикладами є додатки IQAir AirVisual і BreezoMeter, які поєднують дані із супутникових джерел, наземних станцій і персональних сенсорів. Проекти типу Smart Citizen Kit (Барселона, Іспанія) дозволяють жителям міста самостійно встановлювати датчики і долучатися до створення екологічних карт (Balestrini et al., 2017), що також не можливо оминути і в контексті вітчизняного розвитку. Однією з функцій додатку є часткове поширення даних для науковців та студентів певних спеціалізацій. Конкретними світовими прикладами є ініціатива Smart Nation у Сінгапурі, де в рамках проекту було запущено мобільний додаток myENV, який надає громадянам доступ до інформації про екологічний стан довкілля. У США набув розголосу додаток AirVisual від компанії IQAir, який надає глобальні карти забруднення повітря, побудовані на основі даних із супутників та наземних сенсорів (IQAir, 2020) . Користувачі отримують індивідуальні повідомлення про ризики для здоров'я залежно від місцезнаходження. У Європі діють різноманітні ініціативи в межах програми Green Deal, що передбачають встановлення спеціальних мереж в містах. Зокрема, проект Air Quality Platform в Іспанії дозволяє в реальному часі відстежувати концентрації основних забруднюючих речовин (European Commission, 2022) .

Недоліками в такому випадку можуть бути агреговані дані з різних джерел — супутникових знімків, сенсорів, метеорологічних моделей, в той час як Green Guard використовуватиме більшість даних з власних датчиків та дрони, які можуть проводити додаткові виміри. Більшість додатків орієнтовані на загальні показники для великих зон, а не для конкретної вулиці або мікрорайону. Варто врахувати і слабку інтеграцію із науковими дослідженнями (результат – закритість даних) та, на мою думку, один з найкритичніших факторів проблеми з кібербезпекою і приватністю (додатки збирають дані про

геолокацію користувача для прогнозів, але часто не пояснюють, як ці дані захищаються або ким ще можуть бути використані).

В Україні екологічний моніторинг лише починає набирати популярності та уваги. Найвідомішим прикладом є платформа SaveEcoBot, яка об’єднує дані державних і комерційних станцій моніторингу повітря. Проте ці рішення переважно орієнтовані на візуалізацію даних і мають обмежені можливості для аналітики та наукової обробки інформації. Також варто згадати проект Luftdaten у Києві, де ентузіасти встановлюють самостійно зібрані датчики для вимірювання якості повітря (Luftdaten Kyiv, 2022) . Проте такі системи часто страждають на нестачу точності та недостатню стандартизацію даних. Серед основних проблем, які притаманні вітчизняним екологічним додаткам, можна виокремити: Відсутність єдиної централізованої системи збору екологічних даних; Відсутність спеціалізованих сервісів для різних категорій користувачів (зокрема алергіків, дітей, людей з обмеженнями). Тому передбачення недоліків для покращення нового мобільного додатку, здатне підвищити ефективність функціонування навіть у складних умовах, зокрема під час воєнного стану.

У відповідь на все вище зауважене, є рішення - це створення інноваційного мобільного додатку під назвою Green Guard. На відміну від багатьох існуючих систем, Green Guard буде опиратися переважно на дані власного збору, що підвищить точність, актуальність та незалежність інформації. Унікальність проекту полягає в деталізованих даних до рівня окремих вулиць або мікрорайонів міста Ужгород, що дозволить мешканцям оперативно отримувати інформацію саме про свій район. Використання безпілотників дозволить проводити регулярні вимірювання, уточнювати певні дані, а також стане перспективою розвитку нових літальних апаратів. Дизайн та інтерфейс додатку спеціально розроблені для максимальної зручності користувачів: легка навігація, яскраві інфографіки, інтерактивні мапи з можливістю накладення різних екологічних показників, адаптивність під різні пристрої. У контексті кібербезпеки та захисту приватності, Green Guard передбачатиме повну прозорість політики збору та використання даних. Геолокаційні дані користувачів будуть використовуватись лише з їхньої згоди

та не надаватимуться для сторонніх джерел чи використання для покращення додатку.

Архітектура цього проекту включає інтеграцію IoT-пристроїв, дронів, хмарних технологій та штучного інтелекту для прогнозування змін екології. Мобільний додаток відображає дані, дозволяючи користувачам одержувати прогнози та візуалізувати результати моніторингу, що забезпечить масштабованість системи та надасть перспективи для подальшого розвитку. І це тільки один з планів, як може бути реалізований проект. Після опису технічних аспектів варто вказати перспективи та його значення. Завдяки такій архітектурі, Green Guard стане важливим інструментом для моніторингу екологічного стану міста, надаючи жителям та органам місцевого управління точну та своєчасну інформацію для прийняття обґрунтованих рішень. Проект має великий потенціал для перенесення в інші міста, що дозволить покращити екологічний моніторинг на національному рівні та сприяти сталому розвитку урбаністичних територій.

У підсумку дослідження, проект Green Guard є інноваційним рішенням , яке може змінити екологічну безпеку в міських умовах. Завдяки використанню новітніх інформаційних технологій, розробка подібного додатку сприятиме покращенню обізнаності населення щодо стану довкілля, підвищенню особистої безпеки громадян та стимулюванню розвитку екологічної культури. Для науковців та студентів це стане важливим кроком у напрямі розвитку STEM-освіти, дослідницьких проєктів та інноваційних екологічних рішень. Для держави та громад — створення ефективних механізмів швидкого реагування на екологічні загрози.

РОЗПІЗНАВАННЯ DDOS-BOT АТАК В ТЕХНОЛОГІЯХ ІНТЕЛЕКТУАЛЬНОГО МОНІТОРИНГУ КОРПОРАТИВНОЇ МЕРЕЖІ

Сергій Голуб, Вадим Олексюк, Олексій Шебалін

Черкаський державний технологічний університет
бульвар Шевченка, 460, Черкаси, Черкаська область, 18000, Україна

Представлено підхід до розпізнавання DDoS-bot атак у технологіях інтелектуального моніторингу корпоративної мережі. Підхід розроблено із використанням багатошарового персептрона та навченого на датасеті FLNET2023. Модель показала ефективність на тестовому синтетичному наборі з 126 813 точок спостережень, з наступними показниками: точність — 99,92%, точність виявлення — 100%, повнота — 99,55%, F1-міра — 99,77%. Запропонований підхід забезпечує оперативне виявлення DDoS-bot атак.

Актуальність дослідження підтверджується тенденцією до зростання кількості кібератак у світі. Згідно звіту Cloudflare [1], у першому кварталі 2025 року зафіксовано 20,5 мільйона DDoS-bot атак, що у 4,5 раза більше, ніж за аналогічний період 2024 року. Крім того, загальна кількість атак зазначеного типу у 2024 році становить 21,3 млн. інцидентів. Подібна тенденція відслідковується у звітах A10 Networks (2025) [2] та «Nexusguard 2025 DDoS Trends Report» [3]. Жертвами кібератак стають інфраструктурні об’єкти, сайти державних органів, комерційні та фінансові організації тощо.

Метою дослідження є проектування, налагодження та випробування моделі глибокого навчання на основі багатошарового персептрона з використанням датасету FLNET2023 для автоматизованого розпізнавання DDoS-bot атак у технологіях інтелектуального моніторингу корпоративної мережі.

У результаті дослідження реалізовано модель глибокого навчання, призначену для подальшої інтеграції в архітектуру інтелектуального моніторингового агента. Запропоноване рішення забезпечує ефективне

розпізнавання DDoS-bot атак і створює підґрунтя для подальшого впровадження механізмів самонавчання й адаптивного оновлення параметрів моделі.

Інтеграція технології виявлення DDoS-bot атак здійснюється у розроблений багатошаровий моніторинговий програмний агент, який реалізує трирівневий підхід до аналізу мережевого трафіку.

Для побудови моделі розпізнавання DDoS-bot атак використано багатошаровий персептрон (MLP). Це архітектура штучної нейронної мережі, що складається з кількох шарів нейронів, з'єднаних між собою.

Попередня обробка даних включає кодування міток (Label Encoding) та масштабування ознак (Standardization).

Розроблена нейронна мережа складається з трьох прихованих шарів (128, 64, 32 нейрони) та вихідного шару з одним нейроном із сигмоїдальною активацією для оцінки ймовірності належності зразка до класу DDoS-bot атаки. Модель навчається з функцією втрат для бінарної класифікації за допомогою оптимізатора Adam із застосуванням Dropout для запобігання перенавчанню та підвищення узагальнювальної здатності.

Модель продемонструвала ефективність, підтверджену на тестовому наборі з 126 813 точок спостережень. Показник точності (Accuracy): 99.92%, тобто модель правильно класифікує майже всі вхідні зразки. Ідеальна точність (Precision): 100%, що свідчить про відсутність хибних спрацювань. Висока повнота (Recall): 99.55% свідчить про здатність моделі виявляти майже всі фактичні DDoS-bot атаки. Висока F1-міра: 99.77%, демонструє відмінний баланс між точністю та повнотою, роблячи модель дуже надійною.

Запропонована технологія розпізнавання DDoS-bot атак показала високу ефективність та може бути інтегрована в систему інтелектуального моніторингу корпоративної мережі. Подальші дослідження доцільно спрямувати на тестування запропонованого рішення із використанням реальних даних мережевого трафіку.

1. CLOUDFARE. DDoS Threat Report for 2025 Q1 [Електронний ресурс] / Cloudflare ; авт. Omer Yoachimik, Jorge Pacheco. – The Cloudflare Blog, 2025-04-27. –

Режим доступу: https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/. – Назва з екрана. – Дата звернення: [27.10.2025].

2. A10 Networks. DDoS Weapons Report 2025. – San Jose : A10 Networks, Inc., 2025. – 24 p. – Режим доступу: https://www.a10networks.com (дата звернення: 27.10.2025).

3. Nexusguard. 2025 DDoS Trends Report [Електронний ресурс]. – 2025. – 36 с. – Режим доступу: https://www.nexusguard.com (дата звернення: 27.10.2025).

4. Білоніг А., Голуб С. Методи оптимізації процесу навчання великого обсягу моделей нейронних мереж в моніторингових програмних агентах // INFORMATION, COMMUNICATION, SOCIETY (ICS-2024): Proc. Int. Conf., 23–25 May 2024, Zozuli (Lviv region, Ukraine). – Lviv, 2024. – С. 119–120.

5. Kumar P., Liu J., Tayeen A.S.M. та ін. FLNET2023: Realistic Network Intrusion Detection Dataset for Federated Learning // MILCOM 2023 - IEEE Military Communications Conference. 2023. Vol. 36, No. 5. DOI: 10.1109/MILCOM58377.2023.10356272.

АВТОМАТИЗОВАНА КРИМІНАЛІСТИЧНА ЕКСПЕРТИЗА ЕКСФІЛЬТРАЦІЇ ЦІЛЬОВИХ ДАНИХ: ЦИФРОВА КРИМІНАЛІСТИКА НОСІЇВ ДАНИХ

Шаламай Денис Сергійович, Манчур Павло Богданович

Львівський національний університет імені Івана Франка
79007, м. Львів, вул. Університетська, 1
студенти магістратури 2 року навчання, спеціальність 125 «Кібербезпека та Захист інформації»

Цифрові злочини щороку стають дедалі поширенішими як наслідок швидкого оцифрування даних та розвитку цифрових технологій в цілому. Завдяки значно більшим можливостям комунікації і доступу до користувачів всесвітньої мережі, а також анонімності та поширення даних, злочинці не лише займаються незаконною діяльністю за допомогою цифрових технологій, але й вигадують нові види злочинів. У публікації 2022 року "*Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні"* [1] українські науковці Степанюк Р. Л. та Перлін С. І. дослідили та визнали, що в Україні існує нагальна потреба у становленні окремого розділу криміналістичної техніки, присвяченого криміналістичному дослідженню цифрових доказів. Вочевидь, ця потреба лише зросла від початку повномасштабного вторгнення. Проблема поширена не лише в Україні, адже науковці у міжнародних дослідженнях, як наприклад Xiaoyu Du, Chris Hargreaves та інші у роботі "*SoK: Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation*" [2], визнають завали у справах через брак кадрів та часу на дослідження великих обсягів даних. Ексфільтрація даних, з метою викрадення даних, чи то поширення нелегальних матеріалів або шкідливого програмного забезпечення, є без сумнівів поширеним цифровим злочином. У щорічному звіті Національного центру безпеки Великої Британії (NCSC) за 2024 рік [3] згадується, що близько

81% злочинів включали певний рівень ексфільтрації. Такі показники наводять на нагальну потребу вирішення проблеми, наприклад, шляхом удосконалення етапів криміналістичної експертизи.

Для спрощення та пришвидшення криміналістичної експертизи було програмно реалізовано систему автоматизації криміналістичної експертизи ексфільтрації цільових даних. За наявності певних цільових файлів, принаймні їхніх метаданих, розроблений алгоритм здатний з'ясувати чи ці файли наявні або були наявні на пристрої, а також чи були ексфільтровані через фізичні або віртуальні інтерфейси. Програма стане у нагоді як у випадку експертизи органами правопорядку чи комерційних організацій, що практикують збір цінних файлів у певні бази даних, так і для персонального використання, адже не вимагає навичок цифрової криміналістики і значно пришвидшує процес пошуку доказів. Отримуючи цифровий зліпок файлової системи із потенційно вилученого пристрою, алгоритм власноруч визначає її тип та працює згідно її архітектури, не опираючись лише на особливості операційної чи файлової системи.

Архітектура реалізованої програми побудована на основі модулів, що відповідають за різні частини дослідження цифрового зліпку й за технічної можливості використовують багатопотоковість для пришвидшення роботи. Загальну послідовність алгоритму зображено на блок-схемі (рис.1).

Алгоритм працює із вхідними зліпком файлової системи, набором цільових файлів або набором метаданих цільових файлів, та захопленим мережевим трафіком за наявності. Отримані дані обробляються для використання оптимального підходу до експертизи, відкидаючи непотрібні частини серед файлового носія та записів телеметрії та визначаючи справжні їхні типи, не опираючись на розширення, що могло бути змінене. Подальша робота з даними розподіляється між логічними модулями, що порівнюють знайдені докази наявності та/або ексфільтрації файлів із вхідним набором, після чого формується звіт. Звіт містить результати експертизи, додаючи також розділ, що містить свідчення про потенційну ексфільтрацію цільових даних у разі нестачі доказів.

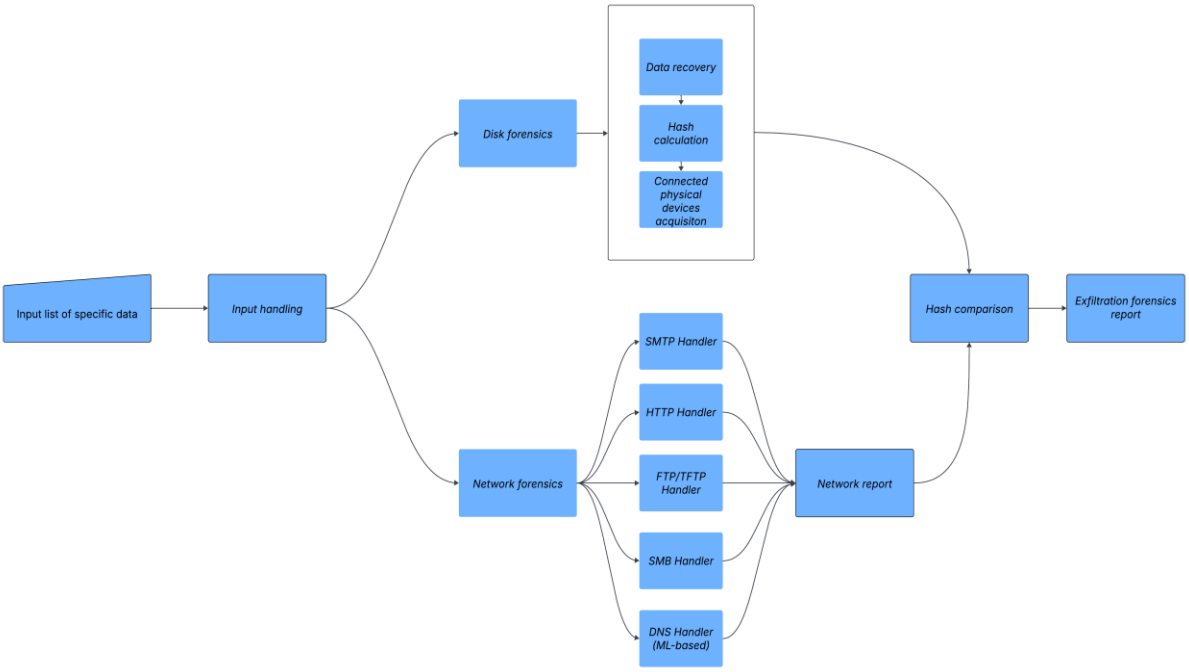

Рис.1. Блок-схема роботи алгоритму

Наступна частина присвячена **цифровій криміналістиці носіїв даних**, лише складовій цілої програми.

Модуль аналізу носіїв даних (сховища файлів, жорсткого диску) разом із відфільтрованим набором цільових даних отримує повний зліпок файлової системи для експертизи. Цей зліпок використовується для пошуку файлів-кандидатів для порівняння із цільовими файлами, опираючись на типи файлів, отримані обчислювальним алгоритмом, що не зважає на потенційно змінене злочинцем розширення чи відредаговані метадані. Блок-схему роботи алгоритму аналізу файлової системи зображено на рисунку 2.

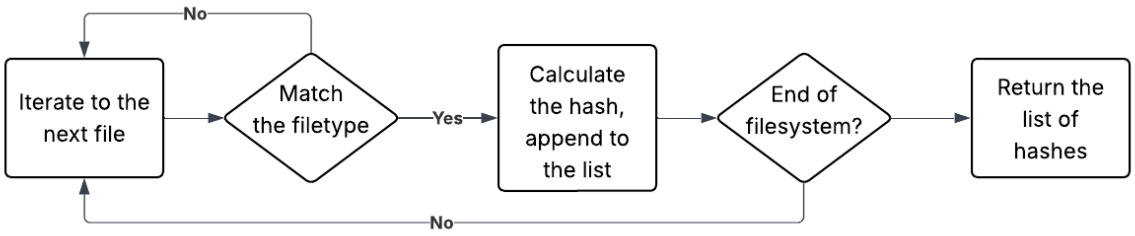

Рис. 2. Блок-схема алгоритму обходу файлової системи

Оскільки цільові файли могли бути видалені злочинцем, до обходу системи здійснюється відновлення усіх видалених файлів, також опираючись на їхній тип. В силу особливостей роботи жорстких дисків, ці файли можуть існувати на ньому після видалення, поки ці комірки пам’яті не будуть перезаписані або диск не буде відформатовано. Після відновлення файли зазнають такого ж обходу згідно наведеної блок-схеми.

Як показує схема, результатом обходу системи є обчислені хеші. За наявності лише метаданих цільових файлів, обчислюються значення криптографічних хеш-функцій MD5 та SHA256, після чого порівнюються із значеннями із вхідного набору.

Однак, за наявності самих файлів, алгоритм обирає точніший метод визначення подібності, застосовуючи так зване “нечітке хешування” (з англ. Fuzzy hashing, similarity hashing).

Функція нечіткого хешування розбиває вхідний набір даних, в цьому випадку файл, на частини, та обчислює значення хеш-функції кожної з частин. Алгоритм повторюється із розбиттям на частини різного розміру, після чого отриманий набір хешів використовується для порівняння із набором хешів файла-кандидата. Для пришвидшеня обчислення використовується багатопотоковість. Якщо кількість однакових хешів для різних частин є вищою за встановлений поріг, обидва файли вважаються подібними.

Наприклад, злочинець може додати зайву інструкцію, що не впливає на поведінку шкідливого ПЗ, до його програмного коду. В такому випадку, завдяки “лавинному ефекту” хеш-функцій значення хеша виконавчого файлу зміниться до невпізнаваності, що дає змогу злочинцю успішно обійти порівняння із оригінальним файлом системами безпеки чи експертами-криміналістами. За допомогою нечіткого хешування дрібні зміни внесені злочинцями до файлів для експлуатації цього ефекту не впливатимуть на ефективність експертизи.

Отриманий набір хеш-значень, незалежно від методу хешування що був застосований, порівнюється із відповідним вихідним набором хешів цільових файлів. Їхня рівність, чи достатня подібність, є індикатором наявності файлів у

файловій системі. Цей результат записується у відповідний розділ згенерованого звіту.

Водночас, в залежності від типу файлової системи, алгоритм отримує історію фізично підключених зовнішніх пристроїв, що могли бути використані для ексфільтрації. Якщо NTFS-система містить встановлену операційну систему Windows, історія підключених пристроїв отримується із реєстру, а у випадку інших файлових систем ця інформація отримується з журналів подій. Без наявного зовнішнього пристрою чи зліпку його файлової системи неможливо чітко визначити чи файл було ексфільтровано саме туди. Отже, у звіті результат експертизи зовнішніх пристроїв підключених до фізичних інтерфейсів записується у розділ потенційних ексфільтрацій.

Розроблений алгоритм був протестований на кількох системах, з яких було ексфільтровано 2 файли, метадані яких були змінені, а самі файли видалені. Середній часовим показник повної експертизи - 6 хвилин. Результат та затрачений час криміналістичної експертизи вручну за допомогою інструментів цифрової криміналістики покладається на людський фактор та компетенції фахівця. Програма не вимагає встановлення додаткових інструментів чи наявність навичок, що потрібні для цифрової криміналістики. Тим не менше, автоматизоване рішення не здатне повністю замінити процес криміналістичної експертизи, тому ми заохочуємо використовувати програму як інструмент оптимізації експертизи, а згенерований звіт може лише допомогти у написанні звіту для судової експертизи.

1. Степанюк Р. Л., Перлюк С. І. (2022) - “Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні” https://luhbulletin.dnuvs.ukr.education/index.php/main/article/view/72/68

2. Xiaoyu Du et al. (2020) - “SoK: Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation” [2012.01987] SoK: Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation

3. Reuters - “UK facing increased hostile activity in cyberspace, security official warns” UK facing increased hostile activity in cyberspace, security official warns | Reuters

АВТОМАТИЗОВАНА КРИМІНАЛІСТИЧНА ЕКСПЕРТИЗА ЕКСФІЛЬТРАЦІЇ ЦІЛЬОВИХ ДАНИХ: ЦИФРОВА КРИМІНАЛІСТИКА МЕРЕЖЕВОГО ТРАФІКУ

Манчур Павло Богданович, Шаламай Денис Сергійович

Львівський національний університет імені Івана Франка

79007, м. Львів, вул. Університетська, 1

студенти магістратури 2 року навчання, спеціальність 125 «Кібербезпека та захист інформації»

Цифрові злочини щороку стають дедалі поширенішими як наслідок швидкого оцифрування даних та розвитку цифрових технологій в цілому. Завдяки значно більшим можливостям комунікації і доступу до користувачів всесвітньої мережі, а також анонімності та поширення даних, злочинці не лише займаються незаконною діяльністю за допомогою цифрових технологій, але й вигадують нові види злочинів. У публікації 2022 року "*Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні"* українські науковці Степанюк Р. Л. та Перлін С. І. дослідили та визнали, що в Україні існує нагальна потреба у становленні окремого розділу криміналістичної техніки, присвяченого криміналістичному дослідженню цифрових доказів. Вочевидь, ця потреба лише зросла від початку повномасштабного вторгнення. Ба більше, проблема поширена не лише в Україні, адже науковці у міжнародних дослідженнях, як наприклад Xiaoyu Du, Chris Hargreaves та інші у роботі "*SoK: Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation*", визнають завали у справах через брак кадрів та часу на дослідження великих обсягів даних. Ексфільтрація даних, з метою викрадення даних, чи то поширення нелегальних матеріалів або шкідливого програмного забезпечення, є без сумнівів поширеним цифровим злочином. У щорічному звіті Національного центру безпеки Великої Британії (NCSC) за 2024 рік згадується, що близько 81% злочинів включали певний рівень ексфільтрації. Такі показники наводять

на нагальну потребу вирішення проблеми, наприклад, шляхом удосконалення етапів криміналістичної експертизи.

Для спрощення та пришвидшення криміналістичної експертизи було програмно реалізовано систему автоматизації криміналістичної експертизи ексфільтрації цільових даних. За наявності певних цільових файлів, принаймні їхніх метаданих, розроблений алгоритм здатний з'ясувати чи ці файли наявні або були наявні на пристрої, а також чи були ексфільтровані через фізичні або віртуальні інтерфейси. Програма стане у нагоді як у випадку експертизи органами правопорядку чи комерційних організацій, що практикують збір цінних файлів у певні бази даних, так і для персонального використання, адже не вимагає навичок цифрової криміналістики і значно пришвидшує процес пошуку доказів. Отримуючи цифровий зліпок операційної системи із потенційно вилученого пристрою, алгоритм власноруч визначає тип файлової системи та працює згідно її архітектури, не опираючись на особливості операційної чи файлової системи.

Архітектура реалізованої програми побудована на основі модулів, що відповідають за різні частини дослідження цифрового зліпку й за технічної можливості використовують багатопотоковість для пришвидшення роботи. Загальну послідовність алгоритму зображено на блок-схемі:

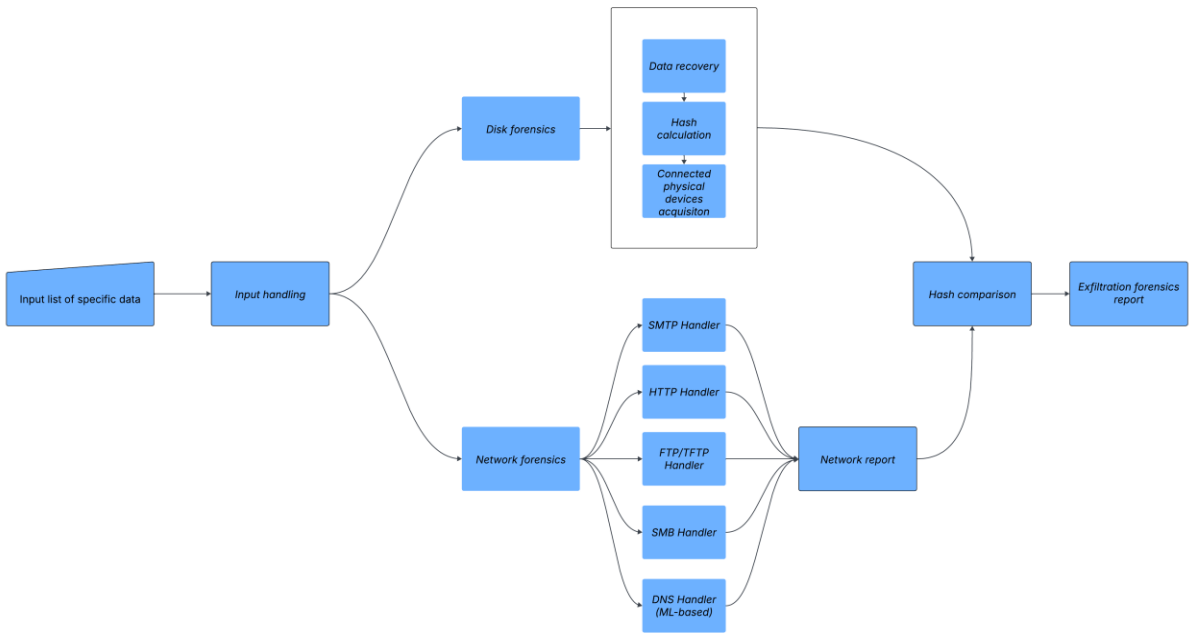

Рис.1

- Блок-схема роботи алгоритму

Алгоритм працює із вхідними зліпком операційної системи, набором цільових файлів або набором метаданих цільових файлів, та захопленим мережевим трафіком за наявності. Отримані дані обробляються для використання оптимального підходу до експертизи, відкидаючи непотрібні частини серед файлового носія та записів телеметрії. Подальша робота з даними розподіляється між логічними модулями, що порівнюють знайдені докази наявності та/або ексфільтрації файлів із вхідним набором, після чого формується звіт. Звіт містить результати експертизи, додаючи також розділ, що містить свідчення про потенційну ексфільтрацію цільових даних у разі нестачі доказів.

Наступна частина присвячена **цифровій криміналістиці мережевого трафіку**.

Розроблений модуль мережевого розслідування призначений для виявлення та реконструкції можливих спроб ексфільтрації даних через стандартні мережеві протоколи на основі захопленого пакетного трафіку. Його основна мета – виявлення шкідливих або несанкціонованих передач даних із компрометованого хоста до зовнішніх ресурсів через широко використовувані протоколи, такі як HTTP, FTP/TFTP, SMBv1/SMBv2, SMTP та DNS. Модуль працює з файлами захоплених пакетів мережевого трафіку (у форматі PCAP або PCAPNG) і забезпечує як аналіз на рівні протоколу, так і реконструкцію корисного навантаження, надаючи спеціалісту з цифрової криміналістики матеріальні докази ексфільтрованих даних та пов’язаної метаінформації.

Система має модульну та розширювану архітектуру, що складається з декількох взаємопов’язаних Python-скриптів:

1. Обробник HTTP трафіку;
2. Обробник FTP та TFTP трафіку;
3. Обробник SMBv1 та SMBv2 трафіку;
4. Обробник SMTP трафіку;
5. Обробник DNS трафіку (на базі моделі машинного навчання);

6. Центральний оркестратор, який інтегрує всі аналізатори протоколів та генерує підсумковий криміналістичний звіт.

Кожен модуль-обробник протоколу реалізує спеціалізовану логіку для виявлення команд або операцій, пов’язаних із передаванням даних (таких як POST і PUT у HTTP-запитах, STOR у FTP-запитах, WRITE або CREATE в SMBv2-запитах тощо). Такі операції зазвичай свідчать про передавання файлів по мережі із цільового хоста до віддаленого вузла, що відповідає типовим моделям ексфільтрації. У разі виявлення відповідних мережевих пакетів, модуль витягує корисне навантаження, реконструює переданий файл і фіксує відповідну контекстну інформацію, включно з IP-адресами джерела та призначення, часовими мітками, типом протоколу, типом запиту, назвою та розміром файлу тощо.

Центральний оркестратор виконує роль основної точки входу. Він завантажує файл із захопленим мережевим трафіком (PCAP або PCAPNG), фільтрує та класифікує пакети за протоколами, а також викликає відповідні модулі-обробники для аналізу, що працюють в різних потоках для оптимізації. Після завершення аналізу результати з обробників усіх протоколів об’єднуються у єдиний звіт. Таким чином забезпечується розділення відповідальностей – кожен модуль працює лише з одним типом трафіку, а оркестратор відповідає за збереження централізованого керування й узгодженого виведення.

Загальний робочий процес модуля криміналістики мережевого трафіку можна підсумувати так:

1. Завантаження PCAP-файлу – центральний оркестратор завантажує файл захопленого мережевого трафіку.
2. Фільтрація за протоколами – мережеві пакети класифікуються за типом протоколу на основі портів або мережевих шарів, створюються проміжні PCAP-файли відповідно до протоколу.
3. Виявлення цільових команд – визначаються команди, пов’язані з передаванням даних (POST, STOR, WRITE тощо).

4. Реконструкція корисного навантаження – витягуються сегменти мережевих пакетів, що належать одній сесії, збирається вміст файлу та зберігається локально (якщо можливо).
5. Логування метаданих – у структурований проміжний криміналістичний звіт записується контекстна інформація про передачу файлів.
6. Агрегація результатів – усі знайдені інциденти об’єднуються в єдиному вихідному документі для швидкого огляду можливих випадків витоку даних.

Інтегрований конвеєр аналізу файлових передач забезпечує виявлення, реконструкцію (при можливості) та документування можливих ексфільтрацій даних через мережеві протоколи HTTP, SMBv1/SMBv2, FTP/TFTP, SMTP та DNS.

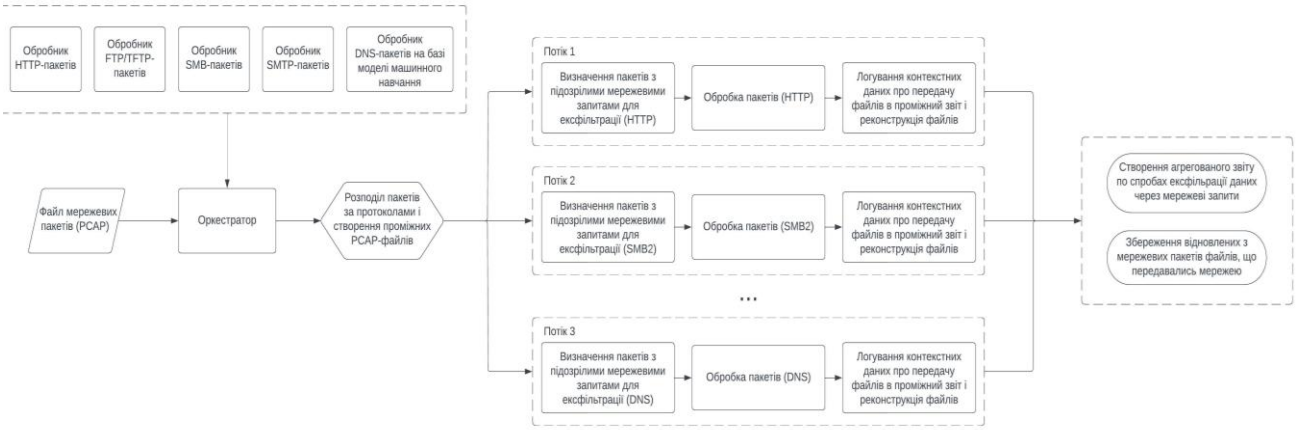

Рис.2. Блок-схема робочого процесу мережевого модуля

Його робота ґрунтується на єдиній послідовності аналітичних етапів, адаптованих до специфіки кожного протоколу. Варто зазначити, що модуль криміналістики мережевого трафіку є частиною ширшої системи криміналістичної експертизи, що включає експертизу електронних (дискових) носіїв даних, і може використовуватись лише у випадках наявності файлу із захопленим мережевим трафіком. Наприклад, це можливо при встановленні спеціального обладнання (network tap) для моніторингу трафіку певного сегменту мережі (до прикладу, на вимогу органів правосуддя), або у корпоративному середовищі.

Спершу система класифікує пакети за протоколами, використовуючи службові заголовки, порти або контрольні команди. Після визначення протоколу аналізатор перевіряє, чи містять пакети операції, пов’язані з передаванням файлів:

- Для HTTP – POST/PUT запити та multipart/form-data;
- Для SMBv2 – CREATE/WRITE запити та їхні legacy-версії для SMBv1;
- Для FTP та TFPT – STOR та WRQ запити відповідно;
- Для SMTP – DATA/BOAT запити (при передаванні листа з вкладеннями або передавання фрагментованих даних в режимі CNHUNKING) і MIME-вкладення;

У подальшому модуль зосереджується на передаваннях файлів, ініційованих з цільового хоста, оскільки саме вони найчастіше свідчать про ексфільтрацію. Об’ємні або нетипові передачі (аномальний розмір або кількість пакетів) маркуються як потенційно підозрілі. Для кожного протоколу застосовуються відповідні методи відновлення вмісту: реконструкція multipart-даних у HTTP, відтворення файлових об’єктів у SMB, збирання блоків у FTP/TFTP тощо.

Щодо виявлення ексфільтрації даних через DNS протокол, використовується модель машинного навчання, інтегрована у відповідний модуль-обробник. На даному етапі обробник збирає метадані мережевих пакетів та передає їх на обробку моделі машинного навчання для класифікації. В цьому випадку відновити файли, передані через DNS-пакети, неможливо. Проте, враховуючи, що цей модуль створений для автоматизації початкової стадії криміналістичного розслідування, це не завжди потрібно і може бути передано на мануальне дослідження.

Результати об’єднуються у стандартизований криміналістичний звіт, що включає метадані файлів, їхній розмір, хеші, IP-адреси джерела і призначення, типи запитів, а також позначки про виявлені аномалії. Така уніфікована структура забезпечує можливість міжпротокольної кореляції та дозволяє швидко оцінити потенційні інциденти витоку даних.

Розроблений алгоритм був протестований на кількох системах, з яких було ексфільтровано 2 файли, метадані яких були змінені, а самі файли видалені. Середній часовим показник повної експертизи - 6 хвилин. Результат та затрачений час криміналістичної експертизи вручну за допомогою інструментів цифрової криміналістики покладається на людський фактор та компетенції фахівця. Програма не вимагає встановлення додаткових інструментів чи наявність навичок, що потрібні для цифрової криміналістики. Тим не менше, автоматизоване рішення не здатне повністю замінити процес криміналістичної експертизи, тому ми заохочуємо використовувати програму як інструмент оптимізації експертизи, а згенерований звіт може лише допомогти у написанні звіту для судової експертизи.

1. Степанюк Р. Л., Перлін С. І. “Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні”. [Електронний ресурс] https://dspace.univd.edu.ua/server/api/core/bitstreams/5f268f43-1af7-4fa7-bae0-5e2d05ac71bb/content

2. Xiaoyu Du et al. (2020) “SoK: Explooring the State of the Art and the future potential of Artificial Intelligence in Digital Forensic Investigation”. [Електронний ресурс] https://arxiv.org/pdf/2012.01987

3. Reuters - “UK facing increased hostile activity in cyberspace, security official warns”. [Електронний ресурс] https://www.reuters.com/technology/cybersecurity/uk-facing-increased-hostile-activity-cyberspace-security-official-warns-2024-12-03/

ЗАВДАННЯ ТА МЕТОДИ OPEN SOURCE INTELLIGENCE

Пузяк Денис Мирославович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури 1 року навчання, спеціальність 125 «Кібербезпека»

Розвідка на основі відкритих джерел (Open Source Intelligence, OSINT) представляє собою технологію збирання різноманітної інформації, включаючи військову, політичну, економічну та іншу, з доступних для громадськості ресурсів. OSINT використовується для збору інформації та розвідувальних даних для різних цілей, зокрема для підтримки процесів прийняття рішень у сферах, таких як національна безпека та бізнес-розвідка, виявлення потенційних ризиків та загроз, а також для моніторингу громадських настроїв та управління репутацією.

Основними компонентами OSINT є публічні реєстри, які дають доступ до офіційних документів (судові рішення, державні звіти, патенти), медіа (традиційні та цифрові), а також інтернет-ресурси. Соціальні мережі, такі як Facebook, Instagram чи Twitter, форуми та веб-сайти, стали необхідною складовою OSINT, надаючи можливість отримувати значну кількість інформації для відстеження трендів та збору даних про конкретних осіб чи організації.

Завдання OSINT охоплюють різні сфери життя. Уряди та військові використовують його для моніторингу та аналізу загроз національній безпеці. У бізнесі OSINT застосовується для конкурентної розвідки та вивчення ринкових тенденцій. Він також є важливим інструментом для журналістських розслідувань, академічних досліджень та аналізу глобальних конфліктів. При зборі даних важливо дотримуватися принципів поваги до приватного життя та законодавчих норм, які регулюють використання інформації з відкритих джерел.

Для практичного застосування OSINT існують спеціалізовані програмні інструменти. Наприклад, Maltego дозволяє шукати інформацію в профілях соціальних мереж та аналізувати зв'язки. Shodan використовується для пошуку серверів, веб-камер та інших пристроїв, підключених до Інтернету. Техніка Google Dorks дозволяє створювати спеціальні запити для виявлення прихованої інформації. Інструменти на кшталт PhoneInfoga та namecheck.com допомагають у пошуку інформації за номером телефону та "нікнеймом" відповідно.

ПЕРСОНАЛІЗОВАНЕ НАВЧАННЯ ТА ГЕНЕРАТИВНИЙ ШТУЧНИЙ ІНТЕЛЕКТ: ВІД «ГШІ ДУМАЄ ЗА МЕНЕ» ДО «ГШІ ДУМАЄ РАЗОМ ЗІ МНОЮ»

Яковець Вадим Васильович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54

аспірант кафедри твердотільної електроніки та інформаційної безпеки

Генеративний штучний інтелект (ГШІ) стрімко інтегрується в освітній процес. За даними Higher Education Policy Institute (2025), 92% студентів використовують інструменти ШІ в навчанні, що на 26% більше, ніж роком раніше [1]. В Україні дослідження МАН України, Projector Institute та Factum Group (2023-2024) показало, що 91% школярів і студентів знають про ШІ-сервіси, а 85% хоча б раз їх використовували [2]. Водночас опитування Rakuten Viber (2025) серед понад 6000 українців виявило: хоча 58% уже користуються ШІ, значна частина респондентів визнає, що не до кінця розуміє принципи роботи цих технологій [3]. Така розбіжність між поширенням і розумінням створює підґрунтя для «сліпої довіри» та ризик втрати власних когнітивних навичок.

Метою роботи є обґрунтування необхідності зміни парадигми використання ГШІ в освіті: від моделі «генератора відповідей» до моделі «інтелектуального партнера», що сприяє розвитку критичного мислення студентів.

На ризики «сліпого» використання ГШІ вказує нейрофізіологічне дослідження MIT Media Lab, які у 2025 році провели експеримент «Your Brain on ChatGPT», де студенти писали есе трьома способами: з LLM, з пошуком і повністю самостійно, а активність мозку вимірювали за допомогою ЕЕГ [4]. Результати показали, що при написанні роботи з LLM мозок демонстрував найнижчу залученість порівняно з іншими умовами, що автори розглядають як зниження когнітивного навантаження. Крім того, студенти, які звикли до LLM, при спробі писати роботу самостійно показували гіршу когнітивну активність,

ніж ті, хто весь час працював без ШІ. Це явище дослідники назвали «когнітивним боргом».

У роботах Zhai et al. (2024) та Gerlich (2025) показано, що коли студенти надто часто перекладають завдання на ШІ, у них гірше розвинені навички самостійного аналізу та зважування рішень [5, 6]. Йдеться не про разове використання, а про звичку делегувати все на ШІ. Ще одна проблема полягає в тому, що моделі здатні «галюцинувати». Дослідження Bhattacharyya та співавторів (2023) проаналізувало 115 посилань, згенерованих ChatGPT у медичних текстах: 47% виявилися повністю вигаданими, ще 46% справжніми, але з помилками, і лише 7% були коректними [7]. Студент, який не звик усе перевіряти, легко плутає швидку й переконливу відповідь ШІ із справжнім знанням.

Водночас мета-аналіз Хіа та співавторів (2025) показав інші результати. Дослідники узагальнили дані 24 досліджень про вплив генеративного ШІ на навчання студентів, спираючись на таксономію Блума, і виявили, що ГШІ позитивно впливає і на базові когнітивні навички (g = 0,93), і на навички вищого порядку, зокрема критичне мислення та креативність (g = 0,64) [8]. При цьому важливу роль відіграє дисципліна, наприклад: у технічних та природничих науках ГШІ працює краще, ніж у гуманітарних, що автори пов'язують зі структурованим характером таких предметів. Цікаво, що для розвитку складніших навичок ефективнішим виявилося саме індивідуальне використання ГШІ.

Усі наведені дані підводять до ідеї переходу від моделі «Генератор» (студент просить - ШІ пише замість нього) до моделі «Партнер» (студент мислить - ШІ ставить уточнювальні запитання, пропонує контраргументи, допомагає переробити відповідь). На практиці це виглядає як робота з ШІ у форматі «спаринг-партнера» та персоналізованого пояснювача [9, 10]. University of Bath (2025) підтверджує, що діалогічний підхід «студент — опонент» поглиблює розуміння матеріалу та змушує студентів займати активну позицію в навчанні [9].

Для молодих науковців ШІ може слугувати інструментом підсилення можливостей дослідника у роботі з даними за принципом: ШІ обробляє - людина інтерпретує [10, 11, 12]. Системи типу AI co-scientist допомагають знаходити неочевидні зв'язки у великих масивах літератури, а метод human-in-the-loop дозволяє прискорити кодування якісних даних у кілька разів, зберігаючи за дослідником контроль над остаточними висновками [12, 13].

У журналі PLOS Computational Biology (2025) запропоновано FOCUS-фреймворк з 10 правилами обережного використання ГШІ в науці, зокрема: чітке визначення цілей і меж застосування ШІ, розуміння можливостей та обмежень інструментів, передача рутинних операцій, обов'язкова перевірка результатів, збереження наукової строгості та прозорість щодо використання ШІ [14].

Висновки. Використання ГШІ в освіті демонструє, наскільки зріло ми ставимося до власного навчання. Якщо ми ставимося до нього як до «персонального виконавця», який має зробити все замість нас, мозок поступово відвикає від напруги, а залежність від підказок лише зростає. Якщо ж сприймати ШІ як партнера по мисленню, він, навпаки, може підштовхувати до глибших запитань і точніших формулювань. Ключова ідея в тому, що ШІ має працювати разом із нами, а не замість нас. Роль університету - чітко пояснити правила гри: створити зрозумілу політику використання ШІ, дати доступ до безпечних інструментів і так змінити завдання, щоб перевірявся не тільки результат, а й хід думок. Роль студента - навчитися працювати з такими інструментами критично: брати допомогу, але залишати за собою право осаточного рішення.

1. Higher Education Policy Institute. Student generative AI survey 2025 (HEPI Report 172). 2025. URL: https://www.hepi.ac.uk/reports/student-generative-ai-survey-2025/

2. Мала академія наук України, Projector Institute, Factum Group. Як штучний інтелект змінює шкільну освіту: результати дослідження. 2023. URL: https://platform.man.gov.ua/media/eb0068b6-4437-4bee-b6df-fd953caffebd

3. Rakuten Viber. Дослідження використання штучного інтелекту серед українців. 2025. n=6000. URL: https://unn.ua/news/maizhe-60percent-ukraintsiv-vzhe-korystuiutsia-shtuchnym-intelektom-opytuvannia

4. Kosmyna N. et al. Your brain on ChatGPT: Accumulation of cognitive debt when using an AI assistant for essay writing task. arXiv:2506.08872. 2025.

5. Zhai C., Wibowo S., Li L. D. The effects of over-reliance on AI dialogue systems on students' cognitive abilities. Smart Learning Environments. 2024. Vol. 11, No. 1. P. 28.

6. Gerlich M. AI tools in society: Impacts on cognitive offloading and the future of critical thinking. Societies. 2025. Vol. 15, No. 1. P. 6.

7. Bhattacharyya M., Miller V. M., Bhattacharyya D., Miller L. E. High rates of fabricated and inaccurate references in ChatGPT-generated medical content. Cureus. 2023. Vol. 15, No. 5. e39238. DOI: 10.7759/cureus.39238

8. Xia Q., Zhang P., Huang W., Chiu T. K. F. The impact of generative AI on university students' learning outcomes via Bloom's taxonomy: a meta-analysis and pattern mining approach. Asia Pacific Journal of Education. 2025. DOI: 10.1080/02188791.2025.2530503

9. Renfrew K. A collaborative sparring partner: Transforming postgraduate learning. University of Bath, Academic & Employability Skills Blog. 2025.

10. Mollick E. Co-intelligence: Living and working with AI. Penguin Press, 2024.

11. Gottweis J., Natarajan V. Accelerating scientific breakthroughs with an AI co-scientist. Google Research Blog. 2025.

12. Morgan D. L. Exploring the use of artificial intelligence for qualitative data analysis: The case of ChatGPT. International Journal of Qualitative Methods. 2023. Vol. 22. DOI: 10.1177/16094069231211248

13. Morgan D. L. Query-based analysis: A strategy for analyzing qualitative data using ChatGPT. Qualitative Health Research. 2025. DOI: 10.1177/10497323251321712

14. Helmy M. et al. Ten simple rules for optimal and careful use of generative AI in science. PLOS Computational Biology. 2025. Vol. 21, No. 10. e1013588. DOI: 10.1371/journal.pcbi.1013588

ШТУЧНИЙ ІНТЕЛЕКТ В МУЗИЦІ, ЯК НЕЙРОМЕРЕЖІ ЗАЙМАЮТЬ ТОП-ЧАРТИ?

Царенко Юрій Романович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54

студент бакалавру 1 року навчання, спеціальність F5 «Кібербезпека»

Генеративний штучний інтелект трансформувався з допоміжного інструменту на повноцінного конкурента в музичній індустрії. Актуальність теми зумовлена тим, що сучасні нейромережі здатні створювати треки студійної якості за лічені хвилини, що фактично нівелює бар'єр входу в індустрію, але водночас створює правовий хаос та проблеми з авторським правом.

Еволюція технологій генерації музики пройшла довгий шлях від ланцюгів Маркова, які не мали «пам'яті» та створювали хаотичні мелодії, до рекурентних нейромереж (RNN) та LSTM, що змогли утримувати контекст. Справжнім проривом стала поява архітектури Transformer та механізму Self-Attention, що дозволило моделям бачити глобальну структуру композиції.

На сучасному етапі State of the Art рішення (Suno AI, Udio) використовують гібридну архітектуру, поєднуючи Трансформери та Дифузійні моделі. Трансформери відповідають за зміст, лірику та структуру, генеруючи семантичні токени, тоді як дифузійні моделі забезпечують високу якість звуку та текстуру, поступово відновлюючи аудіо з шуму.

Впровадження таких інструментів, як RVC (Retrieval-based Voice Conversion), дозволяє клонувати та змінювати тембр голосу, що відкриває нові творчі можливості, але й створює загрозу діпфейків. Це призводить до юридичних конфліктів, зокрема судових позовів від лейблів (RIAA) проти AI-розробників через використання захищених творів для навчання мереж.

Головною проблемою залишається юридичний вакуум: згідно з позицією Бюро авторського права США, твори, згенеровані AI, часто потрапляють у

Public Domain, оскільки авторське право захищає лише твори, створені людиною.

У перспективі прогнозується зміна моделі споживання музики: перехід від прослуховування записаних треків до генеративних потоків, адаптованих під настрій слухача в реальному часі. Роль музиканта трансформується у роль «куратора» нейромереж, а цінність живих виступів та людського фактора значно зросте.

EDGE-АНАЛІТИКА В СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ: БЕЗПЕКА ПЕРЕДАЧІ ТА ЗАХИСТ AI-МОДЕЛЕЙ ВІД АТАК

Довгінка Богдан Михайлович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54

студент магістратури 1 року навчання, спеціальність F5 «Кібербезпека та захист інформації»

У роботі обґрунтовано зростання ролі систем відеоспостереження в сучасній цифровій інфраструктурі, а також визначено необхідність переходу від централізованих серверних рішень до моделей Edge-аналітики. Розкрито чинники, які обумовлюють підвищену увагу до безпеки обробки відеоданих на периферійних пристроях, та проаналізовано нові типи кіберзагроз, притаманні Edge-системам.

Показано, що сучасні системи відеоспостереження все частіше інтегрують обчислювальні модулі на основі штучного інтелекту, які здійснюють розпізнавання об’єктів, поведінковий аналіз та класифікацію подій безпосередньо на камері. Це дозволяє знизити навантаження на мережеву інфраструктуру, зменшити затримки та підвищити ефективність обробки даних у реальному часі.

Визначено основні загрози безпеці Edge-пристроїв, серед яких:

- перехоплення та підміна відеопотоку внаслідок нешифрованих протоколів передачі;
- атаки типу Man-in-the-Middle та компрометація RTSP/SRTP каналів;
- спроби модифікації або викрадення моделей ШІ;
- застосування adversarial attacks, які призводять до навмисно хибної роботи системи розпізнавання;
- ризики несанкціонованої зміни прошивки або впровадження бекдорів у камери.

Проаналізовано сучасні технологічні інструменти, що забезпечують безпеку Edge-аналітики, зокрема:

- шифрування відеопотоків із використанням протоколів TLS 1.3, SRTP та RTSP over TLS;
- застосування криптографічних механізмів перевірки цілісності відеокадрів;
- сегментацію камер у окремі VLAN, використання ACL, DHCP Snooping та Dynamic ARP Inspection;
- впровадження підписаних прошивок, механізмів Secure Boot та захищених середовищ виконання (TEE) для моделей ШІ;
- захист AI-моделей через обфускацію, цифровий підпис і adversarial-захищене навчання.

Забезпечення безпеки Edge-аналітики потребує комплексного підходу, який включає технічні, криптографічні й організаційні заходи. Особливу увагу приділено питанням кіберстійкості, які включають аудит прошивок, контроль оновлень, періодичне тестування системи на вразливості та побудову політик безпечного доступу до камер.

Зроблено висновок, що розвиток Edge-аналітики вимагає впровадження сучасних механізмів кіберзахисту для запобігання втручанню, збереження конфіденційності відеоданих та гарантування коректної роботи моделей штучного інтелекту. Комплексне використання зазначених технологій дозволяє створити стійкі та ефективні системи відеоспостереження, здатні працювати в умовах високих кіберризиків.

ШТУЧНИЙ ІНТЕЛЕКТ ТА АВТОРСЬКЕ ПРАВО

Йовбак Назар Юрійович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент бакалаврату 1 року навчання спеціальність F5 «Кібербезпека та захист інформації»

Штучний інтелект — це інноваційний інструмент який з плином часу і розвитком технологій все сильніше і сильніше закріплюється в нашому житті і стає буденністю, можливо, через декілька років ми не зможем уявляти своє життя без нього, проте попри його користь потрібно розуміти, що у всього є свої мінуси, найбільша ж проблема ШІ полягає в принципі його дії, останні версії різних ШІ покращують вміння створювати «нові» продукти (текст, музика, блоги, романи, поезія, картини та малюнки) використовуючи великі мовні моделі (LLMs), навчальні дані для яких переважно складаються з творів, захищених авторським правом.

Завантаження та зберігання захищених авторським правом даних для навчання моделей машинного навчання може порушувати закон про авторське право та накладати надмірну відповідальність на розробників ШІ. Проблематика інтелектуальних прав та штучного інтелекту також характеризується значною складністю та браком єдиного підходу до вирішення. Законодавча база більшості держав не пристосована до таких у світінових явищ, як авторський продукт, створений за допомогою ШІ, у світі відсутня сформована судова практика з розгляду подібних справ.

Відсутність таких важелів впливу пов’язана також з дилемою критичної залежності. Тобто, з одного боку, дослідження показують, що великі мовні моделі (LLMs) можуть зачепити мільйони робочих місць, що вплине на продуктивність створення нових продуктів. З іншого боку, посилення охорони авторського права контенту, згенерованого людиною,

може перешкоджати розвитку ШІ та знизити суспільний добробут, зменшуючи доступність до автоматизації певних процесів.

Найбільший ризик ШІ припадає на ІТ спеціалістів та творців. Відносно останніх виникають економічні ризики (навіть якщо ШІ-контент технічно не порушує авторське право, оскільки видозмінює його, тож створюється пряма конкуренція), правові ризики (чи є використання творів після їх видозміни, шляхом створення з різних продуктів одного, порушенням авторського права? бо здатність моделей запам’ятовувати твори створює ризик плагіату захищеного контенту), що, зрештою, переростає в девальвацію авторства, коли ШІ витісняє творців і їх професія перестає бути актуальною.

Проте слід відмітити, що останнім часом через надмірну увагу до таких випадів, а також численних судових позовів від великих компаній (Sony, Universal, Disney і т.д.) лідери різних країн почали шукати методи вирішення таких суперечок щодо копірайту. До прикладу, члени ЄС пропонують створити певний чотирьохетапний тест, за яким аналізується оригінальний твір. У свою чергу США почали актуалізовувати доктрину «Made for Hire» та «Fair use», щоб полегшити процеси винесення вироків у справах щодо ШІ, а також планують створити так звану «безпечну гавань» або «Safe harbor», тим самим обмеживши базу, з якої мовні моделі беруть свої дані, і все для того, щоб виключити можливість створення плагіату.

Штучний інтелект створює безпрецедентні виклики для системи авторського права, оскільки моделі навчання масово використовують захищені твори без чітких юридичних меж. Чинне законодавство як ЄС, так і США поки не дає однозначної відповіді, чи є таке використання правомірним та кому належать результати генеративного ШІ. Судові поклики творців (музикантів, художників та письменників) підкреслюють нагальність врегулювання цієї сфери. Потрібні гнучкі, але чіткі правила, що одночасно захищатимуть людську креативність і не стримуватимуть розвиток інновацій. Комплексна юридична адаптація є ключем до збалансованого співіснування людської творчості та штучного інтелекту.

ЗАХИСТ IoT РЕЧЕЙ У РОЗУМНИХ МІСТАХ

Гребеняк Дмитро Володимирович

ДВНЗ «Ужгородський національний університет»
студент 5-го курсу, спеціальність 125 «Кібербезпека»

Захист IoT у розумних містах базується на забезпеченні надійності взаємодії між сенсорами, контролерами та міськими сервісами, що функціонують у реальному часі. IoT-пристрої збирають і передають дані про транспорт, енергетичні системи, екологічний стан, відеоспостереження та інші компоненти інфраструктури. Через обмежені ресурси та спрощені комунікаційні протоколи такі пристрої є особливо вразливими до зовнішніх кіберзагроз.

Основні ризики включають перехоплення та модифікацію даних, підміну ідентичності пристроїв, несанкціоноване втручання у роботу систем керування та використання IoT-вузлів як точки входу для атак на інші сегменти міської мережі. Вразливості виникають через використання типової конфігурації, відсутність шифрування, відкриті порти та слабкі механізми автентифікації. Протоколи, такі як MQTT, CoAP, Zigbee чи LoRaWAN, часто не мають вбудованого захисту, що дозволяє організовувати атаки перехоплення й інжекції команд.

Базовим засобом захисту є застосування криптографічних методів. Використання TLS або DTLS забезпечує шифрування каналів зв’язку, асиметричні алгоритми дозволяють безпечно розподіляти ключі, а цифрові підписи гарантують цілісність отриманих даних. Для пристроїв з обмеженими обчислювальними ресурсами доцільними є легковагові криптографічні рішення, зокрема ECC або ChaCha20. Індивідуальні ключові пари кожного IoT-вузла знижують ризик компрометації всієї інфраструктури у разі порушення безпеки одного елемента.

Важливою складовою є система контролю доступу. Ідентифікація та авторизація повинні виконуватися з використанням сертифікатів або токенів, а взаємодія пристроїв має регулюватися централізованими політиками. Принцип Zero Trust передбачає перевірку кожної операції, незалежно від того, в якій частині мережі знаходиться пристрій.

Підвищення безпеки також досягається через сегментацію мережі. Критичні підсистеми — транспорт, енергетика, служби безпеки — виділяються в окремі логічні сегменти з обмеженим доступом і ретельно контрольованими шлюзами. Фільтрація пакетів та обмеження зовнішніх підключень зменшують можливість проникнення сторонніх у внутрішню інфраструктуру міста.

Моніторинг IoT-середовища дозволяє своєчасно виявляти аномальні дії пристроїв, підозрілий трафік, порушення режиму роботи сенсорів чи спроби зовнішнього втручання. Автоматизований аналіз даних забезпечує швидке реагування: блокування небезпечних вузлів, повторну автентифікацію, ізоляцію сегментів та фіксацію інцидентів.

Практичне застосування захисту охоплює різні міські сервіси. У транспортних системах криптографія захищає телеметрію світлофорів і навігаційні дані транспорту. У відеоспостереженні шифрування запобігає доступу сторонніх до потоків відео. У системах освітлення захист не допускає віддаленої зміни конфігурацій. Дані екологічних моніторингових сенсорів підписуються для виключення їх підміни.

Комплексне поєднання криптографії, контролю доступу, сегментації та постійного моніторингу є необхідною умовою для стійкої роботи розумного міста. Такий підхід забезпечує захист інформаційних потоків, стабільність критичної інфраструктури та мінімізацію ризиків кібератак у середовищі з великою кількістю IoT-пристроїв.

СУЧАСНА OSINT-РОЗВІДКА: ВІД ПОВСЯКДЕННОСТІ ДО ВІЙНИ

Решетар Дмитро Васильович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
Студент 3 курсу, спеціальність 125 «Кібербезпека»

Сучасна інформаційна екосистема характеризується величезним обсягом відкритих даних, які щодня генеруються користувачами соціальних мереж, медіа, державними порталами та технічними засобами збору інформації. На цьому ґрунтується OSINT — розвідка з відкритих джерел (Open Source Intelligence), що передбачає збирання, аналіз і використання публічно доступної інформації для отримання розвідувальних висновків.

Одним із ключових аспектів OSINT є широке коло об’єктів дослідження. До них належать профілі та активність у соціальних мережах, публічні реєстри, новинні ресурси, фотографії й відеоматеріали, геопросторові дані, супутникові знімки, форуми та архіви. Усі ці джерела формують величезний масив даних, з якого аналітик може вилучити корисну інформацію для розслідувань різного характеру — від журналістських до військових.

Методи збору інформації в OSINT охоплюють структуровані пошукові запити з використанням операторів (site:, filetype:, «*», intitle:), аналіз соціальних мереж, геопросторову розвідку (GEOINT), дослідження відкритих баз даних, веб-скрапінг, вивчення відео та аудіо, а також використання спеціалізованих інструментів. Ефективність OSINT залежить не лише від кількості знайдених даних, а й від уміння аналітика оцінити достовірність, актуальність і контекст знайденої інформації.

Процес OSINT-розслідування включає кілька базових етапів: визначення мети, збирання вхідних даних, організацію інформації, інтерпретацію знахідок і фактчекінг. На початковому етапі важливо відповісти на два ключові питання: яку інформацію ми маємо і яку інформацію необхідно отримати. Це дозволяє

сформувати чітку логіку пошуку й уникнути надмірного збору непотрібних даних.

Не менш важливою складовою OSINT є персональна безпека аналітика. Робота з відкритими джерелами вимагає дотримання цифрової гігієни: використання VPN, окремих поштових скриньок, нереальних імен, тимчасових номерів, а також обмеження передачі особистої інформації. Це дозволяє уникнути деанонімізації та зменшити ризики під час роботи з чутливими темами.

Особливе значення OSINT має у військових конфліктах. Сьогодні більшість бойових дій залишають цифрові сліди, що робить OSINT одним із ключових інструментів підтвердження фактів. Його застосовують для геолокації місць вибухів, ідентифікації військової техніки, аналізу маршрутів колон, розвінчання фейків, перевірки пропагандистських матеріалів та оцінки руйнувань за супутниковими знімками. У руках професійних аналітиків OSINT може навіть передбачати подальші переміщення військ, виявляти підготовку наступів та спростовувати інформаційно-психологічні операції противника.

Таким чином, OSINT є важливою складовою сучасної інформаційної безпеки як у мирний час, так і в період війни. Його головні переваги — доступність, швидкість оновлення даних, точність аналізу та можливість використання як державними структурами, так і волонтерами чи журналістами. Поєднуючи відкриті дані з аналітичним підходом, OSINT перетворюється на дієвий інструмент для прийняття рішень, розслідувань та інформаційної протидії.

АТАКИ НА СИСТЕМИ ЦИФРОВОЇ ІДЕНТИЧНОСТІ ПОКОЛІННЯ WEB3

Гецянин Дмитро Вікторович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури 1 року навчання, спеціальність F5 «Кібербезпека та захист інформації»

Системи цифрової ідентичності Web3 є важливою складовою децентралізованої екосистеми, оскільки дозволяють користувачам повністю контролювати власні автентифікаційні дані, зберігаючи їх у розподілених реєстрах без участі централізованих провайдерів. Проте впровадження таких технологій супроводжується виникненням нових кіберзагроз, спрямованих на компрометацію приватних ключів, підміну децентралізованих ідентифікаторів (DID), модифікацію ончейн-записів та несанкціоноване втручання в протоколи автентифікації. У Web3 користувач несе повну відповідальність за зберігання ключів, тому будь-яка помилка може призвести до втрати цифрової особи, що робить такі системи надзвичайно привабливими для зловмисників.

Однією з найпоширеніших атак є фішингові кампанії, у яких шахраї імітують інтерфейси гаманців або децентралізованих застосунків, переконуючи користувача підписати шкідливу транзакцію. Такі атаки особливо небезпечні, оскільки користувач часто не може відрізнити справжній smart contract call від підробленого. Крім того, смарт-контракти самі по собі можуть містити вразливості, які дозволяють використовувати помилки логіки для отримання доступу до цифрових атрибутів ідентичності.

Значну небезпеку також становлять атаки на механізми decentralized identifiers. Зловмисники можуть створювати підроблені DID-документи, змінювати ключі прив’язки або впливати на валідаторів мережі, що виконують роль посередників у підтвердженні ідентичності. У деяких випадках

реалізуються атаки, спрямовані на соціальну інженерію, у яких користувача обманом спонукають перегенерувати або передати свої ключі. Відсутність централізованого органу, який би міг відновити або скасувати ідентичність, перетворює такі інциденти на критичні та незворотні.

Окремо варто розглянути атаки на протоколи self-sovereign identity (SSI). Попри стійкість до централізованих зламів, вони можуть бути вразливими до атак типу Sybil, а також до маніпуляцій валідаторами, які презентують неправдиві атрибути особи. Подібні атаки загрожують не лише окремим користувачам, а й широким екосистемам, у яких цифрова ідентичність використовується для доступу до фінансових операцій, медичних даних, управління активами тощо.

Для захисту систем цифрової ідентичності Web3 необхідно впроваджувати поєднання криптографічних та організаційних механізмів. Серед них важливе місце займає застосування hardware security modules, які забезпечують зберігання ключів у захищеному середовищі, ізолюючи їх від основної операційної системи. Мультипідпис (multisig) дозволяє розподілити контроль над ідентичністю між кількома пристроями чи учасниками, знижуючи ризик повної втрати доступу. Розподілене генерування ключів (DKG) дозволяє уникнути створення ключа в одному місці, що значно ускладнює його перехоплення. Додатково використовуються протоколи перевірки цілісності DID-документів, криптографічні докази з нульовим розголошенням (ZKP), а також механізми децентралізованих репутаційних систем.

Отже, захист цифрової ідентичності у Web3 вимагає комплексного підходу, який включає вдосконалення криптографічних протоколів, підвищення обізнаності користувачів та впровадження високих стандартів безпеки на рівні смарт-контрактів і децентралізованих платформ. Подальші наукові дослідження у цьому напрямі є ключовими для побудови безпечного цифрового середовища та формування стійкої та надійної ідентифікаційної інфраструктури нового покоління.

МЕТОДИ АВТОМАТИЧНОЇ ДЕТЕКЦІЇ ТА ПРОТИДІЇ DEEPFAKE-КОНТЕНТУ ЯК ІНСТРУМЕНТУ ІНФОРМАЦІЙНОЇ ВІЙНИ

Багрінець Христина Богданівна

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54

студентка магістратури 1-го року навчання, спеціальність 125 «Кібербезпека»

Сучасна інформаційна війна характеризується масованим використанням синтетичного медіаконтенту, створеного за допомогою технологій штучного інтелекту. Інформація, що поширюється через соціальні мережі та медіаплатформи, стає об’єктом маніпуляцій, які здатні дестабілізувати суспільно-політичну ситуацію. Одним з найнебезпечніших інструментів такого впливу є технологія Deepfake.

Основними проблемами, що виникають при поширенні діпфейків, є: підрив довіри до офіційних джерел, створення компрометуючих матеріалів на військово-політичне керівництво та складність візуального розрізнення підробки пересічним користувачем.

Найбільш дієвим засобом боротьби з високоякісними діпфейками в умовах великих потоків даних є автоматизований програмний аналіз на основі алгоритмів машинного навчання.

У роботі розглядаються методи автоматичної детекції, що базуються на використанні згорткових нейронних мереж (CNN) для виявлення артефактів генерації. Особлива увага приділяється методу аналізу фізіологічних сигналів (фотоплетизмографії), який дозволяє фіксувати мікрозміни кольору шкіри, викликані кровообігом, що присутні у реальних відео, але відсутні у синтетичних.

Використання комплексного підходу до детекції зменшує ймовірність помилки другого роду (пропуску фейку), оскільки аналізуються як візуальні

невідповідності (рух губ, кліпання очей), так і спектральні характеристики аудіопотоку.

Модифікаційною складовою запропонованого підходу є поєднання технічної детекції з методами підтвердження автентичності контенту (цифрові водяні знаки та хешування). Це дозволяє не лише виявляти підробки, але й верифікувати оригінальні джерела інформації на етапі їх створення.

Відповідно до рівня загрози, методи протидії класифікуються на: пасивні (освіта та медіаграмотність) та активні (блокування контенту алгоритмами платформ та спеціалізованим ПЗ). Чим досконалішими стають генеративні змагальні мережі (GAN), що створюють фейки, тим складнішими мають бути алгоритми їх виявлення.

Дослідження та впровадження розглянутих методів вирішує проблему оперативного реагування на інформаційні атаки та може бути використано для розробки національних систем кібербезпеки.

ШТУЧНИЙ ІНТЕЛЕКТ У РУКАХ ХАКЕРА: НОВІ ЗАГРОЗИ МАЙБУТНЬОГО

Пашко Богдан Васильович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури 1 року навчання, спеціальність 125 «Кібербезпека»

Штучний інтелект стрімко інтегрується у всі сфери цифрового середовища — від побутових пристроїв до критичних інфраструктур. Одночасно зі зростанням його можливостей зростає і ризик використання цієї технології зловмисниками. AI стає інструментом, який значно підсилює потенціал хакерських атак, підвищує їхню ефективність і зменшує поріг входження для кіберзлочинців.

Одним із найнебезпечніших напрямів є використання AI у фішингових атаках. Алгоритми здатні генерувати стилістично і граматично бездоганні листи, адаптовані під конкретного адресата. Це робить фішинг і спір-фішинг набагато ефективнішим навіть проти обізнаних користувачів. Широке застосування deepfake-технологій створює новий рівень ризиків: зловмисники можуть згенерувати реалістичний голос або відеозвернення керівника компанії та маніпулювати працівниками, що вже призвело до багатомільйонних збитків у реальних кейсах.

Ще один небезпечний вектор — автоматизоване сканування вразливостей. AI здатен аналізувати тисячі систем за лічені хвилини, визначаючи найслабші точки для атаки. Хакеру більше не потрібно проводити трудомісткий ручний пошук — алгоритм повністю виконує цю роботу, генерує звіти та пропонує оптимальні цілі. Аналогічно, моделі комп’ютерного зору ефективно долають CAPTCHA, відкриваючи шлях масовим бот-атакам і несанкціонованим діям.

Сучасні мовні моделі можуть створювати шкідливий код різного рівня складності, включаючи скрипти для крадіжки даних, експлойти чи програми

прихованого доступу. Навіть попри обмеження платформ, зловмисники легко обходять фільтри шляхом модифікації запитів. Таким чином, можливість створення шкідливого ПЗ стає доступною навіть користувачам без високого технічного рівня.

AI-боти набувають поширення у соціальній інженерії: вони імітують справжню людську поведінку, збирають персональні дані, надсилають фішингові посилання та здатні працювати з великою кількістю жертв одночасно. Подібні технології вже впроваджуються у даркнет-сервіси, де «фішинг як сервіс» стає буденністю.

Особливо небезпечним трендом є автономні AI-атаки — системи, що самостійно виявляють вразливості, створюють експлойти, здійснюють проникнення, викрадають інформацію та приховують сліди без участі людини.

Зростання загроз вимагає впровадження сучасних захисних рішень. На рівні користувачів це — двофакторна автентифікація, уважність до електронних листів, критичне мислення та використання менеджерів паролів. Для компаній — впровадження AI-захисту (поведінкового аналізу, фаєрволів нового покоління, антифішингових шлюзів), регулярні тренінги персоналу та моделювання атак.

Штучний інтелект є нейтральним інструментом, який може служити як на благо, так і на шкоду. Подальший розвиток технологій робить вкрай важливим підвищення обізнаності та адаптацію систем кіберзахисту до нових реалій.

ІНСТРУМЕНТ ДЛЯ ІНТЕГРОВАНОГО ВИЯВЛЕННЯ ТА ОЦІНКИ ВРАЗЛИВОСТЕЙ ВЕБ-ДОДАТКА OWASP Juice Shop (OWASP ZAP + Nmap + CVSS)

Зуб Василь Васильович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

Автоматизовані інструменти для виявлення вразливостей у веб-додатках відіграють ключову роль у забезпеченні кібербезпеки сучасних інформаційних систем. Значна частина сервісів сьогодні працює онлайн, а веб-додатки стають основною точкою взаємодії між користувачами, бізнесом і державними установами. Через високу складність архітектур і наявність численних інтеграцій ризики виникнення вразливостей постійно зростають. Вразливості веб-рівня та мережевої інфраструктури можуть бути використані для крадіжки даних, обходу контролю доступу чи повного захоплення серверів. Тому виникає потреба у системних інструментах, здатних поєднувати різні підходи до аналізу безпеки, автоматизувати процеси сканування та забезпечувати стандартизовану оцінку ризиків.

Розроблений інструмент інтегрує функціонал OWASP ZAP, Nmap та CVSS, поєднуючи аналіз веб-додатка, сканування мережевої інфраструктури та формальне оцінювання критичності знайдених вразливостей. OWASP ZAP виконує аналіз логіки веб-застосунку, виявляючи такі типові загрози, як SQL-ін’єкції, XSS, некоректні заголовки чи конфігураційні помилки. Nmap, у свою чергу, досліджує поверхню атаки з боку мережі, визначає відкриті порти, працюючі сервіси та версії програмного забезпечення, а також дозволяє виявити слабкі місця у транспортному рівні. Комбінація цих двох інструментів створює більш комплексну картину, оскільки кожен з них аналізує свою частину

середовища, а разом вони дають змогу точніше оцінити реальний контекст і взаємозв’язки вразливостей.

Особливістю інтегрованого підходу є здатність не лише виявляти вразливості, але й структурувати їх через систему CVSS, яка надає стандартизований числовий бал критичності. Це дозволяє уникнути суб’єктивності та забезпечує можливість швидко визначати, які проблеми потребують негайного втручання. Враховується складність експлуатації, необхідні привілеї, умови атаки, а також вплив на конфіденційність, цілісність і доступність даних. Автоматичне формування CVSS-векторів забезпечує відтворюваність оцінки та спрощує прийняття рішень у сфері кібербезпеки, що є критично важливим як для аналітиків, так і для менеджменту.

Застосування такого інструмента особливо важливе в навчальному середовищі, де студенти та молоді фахівці можуть відпрацьовувати навички тестування на прикладі вразливого веб-додатка OWASP Juice Shop. Автоматизація процесів дозволяє сфокусуватися на аналізі та правильній інтерпретації результатів, а не на технічних деталях запуску численних сканерів. Крім того, інструмент сприяє формуванню системного мислення: користувачі бачать, як веб-рівень та інфраструктурний рівень взаємодіють між собою й як одна вразливість може впливати на інші компоненти системи.

Перспективи подальшого розвитку таких інструментів охоплюють глибшу інтеграцію в DevSecOps-процеси, автоматичне тестування у CI/CD-конвеєрах, розширення підтримки додаткових сканерів і застосування методів машинного навчання для виявлення аномалій та кореляції даних. Зважаючи на постійний розвиток кіберзагроз, поєднання веб-сканування, мережевого аналізу та формальної оцінки ризику стає необхідністю для будь-яких сучасних організацій. Інструмент, розроблений у рамках цього проєкту, є прикладом того, як через інтеграцію відкритих технологій можна створити потужне й доступне рішення для комплексного аналізу вразливостей.

STEM-ПРОГРАМА ГУРТКОВОЇ ДІЯЛЬНОСТІ З ВИКОРИСТАННЯМ 3D-ДРУКУ У ЗАКЛАДАХ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ

Ковач Дмитро Іванович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54

студент магістратури 2 року навчання, спеціальність «Середня освіта. Фізика»

Розроблена STEM-програма гуртка з 3Д-друку для закладів загальноосвітньої середньої школи. Під час розробки були досліджені основні форми реалізації STEM-освіти, сучасні технології задіяні в освіті, а також вплив гуртkової діяльності на формування навчальних компетентностей.

Також було проведено аналіз основних видів апаратного та програмного забезпечення, необхідного для роботи гуртка, зокрема, 3Д-принтери Elegoo Neptune 4 та Anycubic Photon Mono 4K - для апаратного забезпечення, та Microsoft 3D Buider, Lychee slicer та FreeCAD – для програмного забезпечення. Після розробки програми гуртка були проведені практичні заняття. Серед виконаних проєктів учасників гуртка можна виділити створення популярної декоративної фігурки, корпус для електронного пристрою та виготовлення органайзеру для шкільного приладдя.

ІНТЕЛЕКТУАЛЬНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ ДО ЖИТЛА

Маргітич Станіслав Михайлович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури 1 року навчання, спеціальність F2 «Кібербезпека»

Повномасштабна війна та економічна міграція призвели до того, що значна частина громадян України тривалий час перебуває за кордоном, залишаючи квартири та будинки без постійного нагляду. За таких умов різко зростає ризик крадіжок, несанкціонованого проникнення та умисного пошкодження майна. Типові пультові охоронні системи є дорогими і потребують абонентської плати, а масові IP-камери орієнтовані на закриті хмарні сервіси виробника і не завжди дозволяють гнучко керувати даними чи інтегруватися з іншими сервісами. Тому актуальною є розробка відносно недорогої, відкритої та розширюваної інтелектуальної системи контролю доступу до житла.

Запропонована система поєднує прихований бездротовий датчик стану вхідних дверей, центральний мікропроцесорний модуль, приховану відеокамеру, звуковий модуль відлякування та Telegram-бота для сповіщень. Факт відкриття дверей фіксується герконовим датчиком, розміщеним у дверній коробці, а магніт утоплений у торець дверного полотна. Такий підхід не прив’язує контроль лише до механізму замка й дозволяє виявити не тільки нормальне відчинення дверей ключем, а й силове виламування, коли полотно відходить від коробки. Дані з геркона обробляються малогабаритним мікроконтролерним модулем з підтримкою бездротового зв’язку (LoRa або Wi-Fi), який передає події до центрального вузла системи.

Центральний вузол реалізовано на базі сучасного мікроконтролера сімейства ESP з підтримкою Wi-Fi, що забезпечує підключення системи до локальної мережі та Інтернету. Тут формується журнал подій

відкриття/закриття дверей, виконується аналіз аномальної активності (відкриття у нетиповий час, велика тривалість відчинених дверей, часті спроби доступу тощо) та здійснюється взаємодія з Telegram-ботом. У разі відсутності Інтернет-з'єднання події тимчасово буферизуються у локальній пам'яті й передаються власнику після відновлення зв'язку, що підвищує надійність сповіщень.

Окремим компонентом системи передбачається мобільний додаток, розроблений на базі платформенного фреймворка Flutter. Додаток забезпечує адаптивне налаштування параметрів безпеки під індивідуальні потреби користувача: вибір режимів охорони, рівнів чутливості датчиків, сценаріїв сповіщення, часових інтервалів «нормальної» активності, керування звуковим модулем та доступом до архіву подій і відеозаписів. Використання Flutter дає змогу реалізувати єдиний програмний код для ОС Android та iOS, що спрощує супровід і розширення функціоналу системи та робить її доступною для більшої кількості користувачів.

У режимі тривоги система автоматично активує приховану камеру для фото- та відеофіксації зловмисника, а також модуль звукового відлякування. Через динамік відтворюється попередньо записане голосове повідомлення про те, що особу зафіксовано на відео, дані передано власнику та правоохоронним органам. Такий підхід створює додатковий психологічний бар'єр для зловмисника: усвідомлення факту викриття та неминучості ідентифікації часто змушує відмовитися від подальших протиправних дій навіть до втручання поліції. Окрім цього, система може накопичувати статистику доступу й автоматично визначати періоди «звичайної» та «підвищеної» небезпеки для конкретного об'єкта.

Використання доступних компонентів – герконових датчиків у стандартних корпусах, масових мікроконтролерних модулів ESP, бездротових радіомодулів LoRa, недорогих IP-камер та кросплатформенного мобільного додатку на Flutter – дає змогу знизити вартість розробки порівняно з комерційними охоронними комплексами, які включають дорогі пульти, централізований моніторинг і закриті програмні рішення. Відкритість програмної частини дозволяє адаптувати інтелектуальну систему контролю

доступу до особливостей конкретного житла, інтегрувати її з іншими елементами «розумного дому» та надалі розширювати функціональність. Така система може стати практичним та економічно доцільним інструментом захисту житла українців, які вимушено перебувають за кордоном, сприяючи зменшенню побутової злочинності й підвищенню відчуття безпеки власників.

СИСТЕМА ПРОТИДІЇ КІБЕРЗАГРОЗАМ ТА ІНФОРМАЦІЙНИМ АТАКАМ У МЕСЕНДЖЕРІ Telegram В УМОВАХ ВІЙНИ В УКРАЇНІ

Джанда Анастасія Святославівна

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54

студент магістратури 2 року навчання, спеціальність F2 «Кібербезпека»

Метою роботи є комплексне дослідження кіберзагроз та інформаційних атак у середовищі месенджера Telegram в умовах російсько-української війни та розроблення концептуальної моделі системи протидії загрозам з формуванням практичних рекомендацій щодо забезпечення безпечного використання платформи.

Для досягнення мети застосовано описово-аналітичний та системний підходи, контент-аналіз Telegram-каналів і ботів та методи експертних оцінок у вигляді інтерв'ю з експертами у сферах державного управління, кібербезпеки та стратегічних комунікацій і опитування студентів фізичного факультету спеціальності F5 Кібербезпека та захист інформації.

У роботі сформовано каталог основних загроз, ідентифіковано ключові наративи та патерни інформаційних атак. Розроблено концептуальну модель системи протидії, що відображає взаємозв'язок між джерелами загроз, видами загроз, етапом реагування, заходами протидії та очікуваними результатами їх реалізації, а також сформовано практичні рекомендації, спрямовані на підвищення рівня кіберстійкості та безпеки інформаційного середовища фізичного факультету ДВНЗ «Ужгородський національний університет».

СТВОРЕННЯ ТА ВПРОВАДЖЕННЯ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ВИЯВЛЕННЯ ФІШИНГОВИХ ПОВІДОМЛЕНЬ, ЗГЕНЕРОВАНИХ ШТУЧНИМ ІНТЕЛЕКТОМ

Скоблей Сергій Сергійович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури 2 року навчання, спеціальність F2 «Кібербезпека»

Було розроблено інтелектуальну систему виявлення фішингових повідомлень згенерованих за допомогою штучного інтелекту. Створена система інтегрує семантичний аналіз , оцінку посилань , поясний штучний інтелект та механізми стійкості до атак в єдину архітектуру.

Результати впровадження та оцінки демонструють, що запропонована система досягає високої точності виявлення з низьким рівнем хибнопозитивних результатів, залишаючись при цьому стійкою до методів маніпуляцій з боку зловмисників.

ВИЗНАЧЕННЯ СПЕКТРАЛЬНОЇ ЗАЛЕЖНОСТІ ПРОПУСКАННЯ ГРАДІЄНТНИХ ПЛІВОК СИСТЕМИ Ge-S МЕТОДАМИ АПРОКСИМАЦІЇ ТА ЇХ КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ

Пічкарь Ігор Едуардович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури II року навчання, спеціальність 104 «Фізика та астрономія »

Дипломна робота присвячена дослідженню оптичних властивостей градієнтних модифікованих структур на основі халькогенідних систем Ge–S із застосуванням методів комп'ютерного моделювання та апроксимації експериментальних даних. Проведено комплексне дослідження оптичних властивостей градієнтних модифікованих структур систем Ge–S з використанням методів апроксимації та комп'ютерного моделювання в середовищі Lazarus. Реалізовано математичні моделі та розроблено програми розрахунку лінійної, експоненційної, степеневої і поліноміальної апроксимації з використанням методу найменших квадратів в середовищах Lazarus.

Досліджено формування градієнтних модифікованих структур систем Ge–S з використанням методів двопараметричної експоненціальної апроксимації та термічного випаровування у вакуумі та їх оптичні властивості. Отримані результати показали задовільну узгодженість комп'ютерної моделі та експериментальних даних. Представлені підходи можуть бути використані для оптимізації параметрів тонкоплівкових матеріалів, прогнозування їх оптичної поведінки та подальшого застосування у фотонних та оптоелектронних пристроях.

РОЗВИТОК ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ КІБЕРБЕЗПЕКИ

Сухан Руслан Сергійович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури 1 року навчання, спеціальність 125 «Кібербезпека»

Штучний інтелект (Artificial Intelligence, AI) відіграє дедалі важливішу роль у сфері кібербезпеки, забезпечуючи автоматизацію, підвищення точності аналізу та швидкість реагування на загрози. Використання AI у кіберзахисті охоплює широкий спектр задач — від моніторингу мережевої активності й виявлення аномалій до прогнозування потенційних атак та автоматичного усунення вразливостей. Завдяки машинному навчанню та аналізу великих обсягів даних штучний інтелект допомагає ефективніше ідентифікувати шкідливу поведінку, яку важко виявити традиційними методами.

Основними джерелами даних для систем AI у кібербезпеці є журнали подій (logs), трафік мережі, телеметрія пристроїв, дані з систем виявлення вторгнень (IDS/IPS) та інформація з відкритих джерел. Важливу роль відіграє інтеграція AI з технологіями SIEM та SOAR, що дозволяє автоматизувати обробку інцидентів, проводити кореляцію подій та пришвидшувати реагування на атаки. Такі системи здатні самостійно визначати ризик, аналізувати поведінкові патерни користувачів (UBA/UEBA) та виявляти приховані загрози, ґрунтуючись на статистичних моделях і поведінковій аналітиці.

Завдання штучного інтелекту в кібербезпеці охоплюють широкий спектр напрямів. Уряди та великі корпорації використовують AI для виявлення складних атак, зокрема APT-кампаній, та забезпечення захисту критичної інфраструктури. У бізнесі AI застосовується для оцінки вразливостей, фільтрації шкідливого трафіку, антивірусного аналізу та захисту хмарних середовищ. Він також є ключовим інструментом у фішинг-детекції, аналізі шкідливих вкладень, автоматичному визначенні ботнет-активності та прогнозуванні майбутніх

тенденцій у сфері кіберзагроз. Водночас важливо дотримуватися етичних норм: незважаючи на розвиток AI, необхідно забезпечувати конфіденційність даних, прозорість алгоритмів та уникати надмірного втручання у приватне життя користувачів.

Для впровадження штучного інтелекту у сфері кібербезпеки існує широкий набір інструментів і технологій. Наприклад, Darktrace використовує машинне навчання для створення поведінкових моделей мережі та автоматичного реагування на загрози. CrowdStrike Falcon застосовує AI для аналізу кінцевих пристроїв та виявлення шкідливих дій у реальному часі. IBM QRadar Advisor with Watson використовує можливості NLP для автоматизованого аналізу інцидентів. Інструменти VirusTotal, Cortex XDR, Microsoft Defender 365 AI, а також моделі глибинного навчання допомагають виявляти шкідливі файли, аналізувати аномалії та прогнозувати небезпечні патерни у кіберпросторі.

СОЦІАЛЬНІ МЕРЕЖІ ЯК СЕРЕДОВИЩЕ ФОРМУВАННЯ НАУКОВИХ СПІЛЬНОТ МОЛОДІ

Бородай Юрій Юрійович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури 1 року навчання, спеціальність 125 «Кібербезпека»

Соціальні мережі перестали бути винятково простором для розваг і сьогодні активно використовуються студентами та молодими науковцями для обміну знаннями, пошуку наукової інформації та встановлення професійних контактів. Платформи на кшталт Facebook, Instagram, LinkedIn, Telegram і навіть TikTok формують нову культуру доступної та швидкої наукової комунікації. Молодь отримує можливість оперативно ділитися результатами власних досліджень, отримувати фідбек від ширшої аудиторії, стежити за роботою провідних учених та наукових установ. Це сприяє формуванню відкритого інформаційного середовища, у якому зростає мотивація до досліджень і саморозвитку.

У соціальних мережах активно розвиваються тематичні наукові спільноти: групи, канали, чати та пабліки, присвячені окремим галузям науки — від IT і біології до гуманітаристики. Молоді науковці можуть долучатися до міжнародних дослідницьких груп, брати участь у вебінарах, отримувати доступ до наукових ресурсів, порад і менторства. Формуються мікроспільноти, де учасники обговорюють актуальні проблеми, діляться досвідом, публікують наукові статті, завдання, методики та власні напрацювання. Це не лише розширює коло професійних контактів, а й створює умови для колаборативних досліджень та міждисциплінарної взаємодії.

Перевагами є швидкий доступ до нової інформації, можливість отримати безкоштовні освітні матеріали, знайти партнерів для досліджень, обговорювати

проблемні питання та популяризувати власну наукову діяльність. Водночас існують істотні ризики: поширення недостовірної інформації, вплив псевдонауки, формування інформаційних «бульбашок», залежність від алгоритмів рекомендацій, а також ризики цифрової безпеки. Через це особливо важливою стає цифрова грамотність: уміння фільтрувати джерела, критично мислити та перевіряти наукову інформацію перед поширенням.

Соціальні мережі відкривають студентам можливість створювати власний науково-популярний контент: відеолекції, наукові огляди, інфографіку, короткі пояснення складних явищ. Така активність сприяє не лише поширенню науки серед однолітків, а й розвитку навичок презентації, комунікації, структурного мислення. Молоді науковці дедалі частіше вибудовують персональні наукові бренди, які допомагають знаходити можливості для участі в проєктах, грантах, стажуваннях та конкурсах. Соціальні мережі стають потужним каналом формування громадського інтересу до науки.

У перспективі соціальні мережі дедалі глибше інтегруватимуться в освітнє та наукове середовище. Очікується зростання ролі штучного інтелекту в персоналізації наукового контенту, рекомендації джерел і модерації спільнот. Студенти зможуть проводити віртуальні наукові конференції, створювати цифрові лабораторії, брати участь у міжуніверситетських дослідженнях незалежно від географії. Молодь уже сьогодні формує культуру відкритої науки, а соціальні мережі виступають платформою, яка об’єднує ініціативних дослідників, підтримує міждисциплінарність та розширює можливості наукової творчості.

НАПІВПРОВІДНИКОВІ ГАЗОВІ СЕНСОРИ ДЛЯ СИСТЕМ МЕДИЧНОЇ ДІАГНОСТИКИ

Шимон Євген Мирославович

ДВНЗ «Ужгородський національний університет» 88000, Ужгород, вул. Волошина, 54
студент магістратури 2 року навчання,
спеціальність 105 «Прикладна фізика та наноматеріали»

Сучасні інформаційні технології дедалі активніше інтегруються у сферу охорони здоров'я, формуючи новий напрям - цифрову та персоналізовану медицину. Одним із перспективних прикладів такої інтеграції є системи медичної діагностики, що поєднують сенсорні пристрої, мікроелектроніку та програмну обробку даних. Особливий інтерес викликають неінвазивні методи діагностики, зокрема аналіз видихуваного повітря людини. У ньому містяться леткі органічні сполуки, які можуть виступати біомаркерами стану організму. Одним із таких біомаркерів є ацетон, концентрація якого корелює з порушеннями вуглеводного обміну та використовується для моніторингу цукрового діабету. Основою багатьох сучасних газоаналітичних систем є напівпровідникові газові сенсори на базі оксидів металів. Вони перетворюють хімічну інформацію (наявність газу) у електричний сигнал, який легко інтегрується з електронними та цифровими системами. Найбільш поширеним матеріалом є діоксид олова (SnO_2) - напівпровідник n-типу, електричний опір якого змінюється при взаємодії з молекулами газу. Сенсор фактично виступає аналоговим перетворювачем "газ → електричний сигнал", що є зручним для подальшої цифрової обробки.

У повітрі на поверхні SnO_2 адсорбується кисень, який захоплює електрони і формує приповерхневий шар просторового заряду. Це призводить до зростання опору сенсора. При появі ацетону відбувається його окислення, електрони повертаються у напівпровідник, а опір зменшується. Для підвищення ефективності таких сенсорів активно використовуються нанотехнології,

зокрема: наноструктурування поверхні; модифікація благородними металами; контроль морфології на нанометровому рівні.

У представлених дослідженнях поверхню SnO_2 модифіковано ультратонкими острівцевими плівками золота та платини товщиною близько 1,5–2 нм. Такі плівки не є суцільними, а формують нанорозмірні каталізаторні острівки, що суттєво підсилюють сенсорний відгук.

З точки зору інформаційних технологій, газовий сенсор є лише першою ланкою системи. Повноцінна діагностична платформа включає: газовий сенсор (SnO_2 / Au, SnO_2 / Pt); мікронагрівач для стабілізації температури; аналогову вимірювальну схему (дільник напруги); мікроконтролер; програмну обробку сигналів; передачу даних (у нас - USB); інтерфейс користувача (ПК).

Таким чином, концентрація ацетону у видиху може бути представлена як цифровий параметр, що: зберігається у базі даних; аналізується в динаміці; використовується для побудови персональних профілів здоров'я.

Результати досліджень показали, що використання острівцевих плівок Au підвищує чутливість сенсора приблизно у 1,25 раза, а Pt - до 1,55 раза порівняно з немодифікованим SnO_2. Сенсори стабільно працюють у діапазоні концентрацій 1–10 ppm ацетону, що відповідає реальним умовам медичної діагностики. Вони зберігають працездатність за високої вологості, характерної для людського дихання, що є критичним для практичних застосувань. Отримані результати мають безпосереднє прикладне значення для створення **портативних неінвазивних аналізаторів ацетону**; персональних моніторів стану пацієнтів із діабетом; елементів сенсорних матриць типу «електронний ніс». Поєднання наноструктурованого SnO_2 з острівцевими плівками Pt/Au дозволяє досягти **низьких меж виявлення (≈1 ppm)**, швидкого відгуку та прийнятної стабільності сигналу — ключових вимог для клінічних і домашніх діагностичних систем.

Отже, напівпровідникові газові сенсори є ефективним інтерфейсом між фізичними процесами та інформаційними системами. Модифікація SnO_2 нанорозмірними плівками Au та Pt суттєво покращує чутливість до біомаркерів.

Поєднання сенсорів з мікроконтролерами та програмною обробкою створює основу для сучасних цифрових медичних систем.

СТВОРЕННЯ ТА ВПРОВАДЖЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ДЛЯ ВИЯВЛЕННЯ ДЕЗІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ ЗА ДОПОМОГОЮ OSINT

Анткевич Вікторія Вікторівна

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студентка 2 курсу магістратури, спеціальність F5 «Кібербезпека»

Зі зростанням популярності мережі Інтернет невпинно підвищується його роль у повсякденному житті людини. Онлайн-платформи, зокрема соціальні мережі, поступово стають домінантним джерелом новин та інформації для сотень мільйонів людей. Простота створення й розповсюдження новин через Інтернет, а також фізична неможливість перевірити величезні обсяги інформації, що циркулює у всесвітній мережі, різко збільшила поширення дезінформації та фейкових новин.

Оманлива інформація може формувати переконання, ставлення та поведінку, що часто призводить до помилкових висновків і дій. Наслідки цього можуть варіюватися від незначних непорозумінь до значного суспільного розбрату. У гіршому випадку неправдива інформація може викликати страх, спровокувати насильство або вплинути на політичні та соціальні рішення з далекосяжними наслідками.

Дезінформацію можна визначити наступним чином – це спотворена, свідомо неправдива, провокаційно-тенденційна інформація, з питань що становлять суспільний інтерес, що створюється, подається та/ або поширюється як правдива з метою введення в оману громадськості, політичних опонентів, конкурентів тощо та/або спричинення серйозної суспільної шкоди

Так дезінформація є поняттям, що лежить на стику двох сфер: неправди (обману) та зловмисних намірів, і характеризується змістом, який є:

• хибним, тобто таким, що не відповідає дійсності;

• маніпулятивним, оскільки має на меті прихований вплив на психіку людей з метою їх спонукання до дій в інтересах суб'єкта впливу;

• сфабрикованим — придуманим навмисно, щоб ввести в оману споживача інформації;

• безпідставним, тому що посилається на видумані або анонімні джерела для приховування походження інформації та перешкоджання перевірці її справжності.

Штучний інтелект (ШІ) відіграє ключову роль у цьому процесі. Виділимо деякі способи, які за допомогою штучного інтелекту виявляють дезінформацію:

• Аналіз тексту та контексту: Штучний інтелект може аналізувати текстові дані, виявляючи незвичайні висловлювання, суперечливі факти або недостовірні джерела. Він також враховує контекст, щоб визначити, чи відповідає інформація загальноприйнятим фактам.

• Моніторинг соціальних мереж: Штучний інтелект аналізує мільйони повідомлень у соціальних мережах, виявляючи підозрілі теми, теги або посилання. Він також визначає популярність дезінформаційних матеріалів.

• Виявлення deepfake: Штучний інтелект розпізнає фейкові відео, аудіо або зображення. Він аналізує різницю між оригінальними та зміненими даними.

• Масштабізація аналізу: Штучний інтелект може обробляти великі обсяги даних, що дозволяє виявляти дезінформацію в реальному часі.

OSINT (Open Source Intelligence) — це методологія збору й аналізу відкритої інформації, що стала невід'ємним інструментом сучасних аналітичних систем.

Її головна перевага — доступ до великої кількості джерел без порушення правових норм.

Це збір, аналіз та інтерпретація відкритої інформації з вільних джерел, доступних для будь-якого користувача. Це може включати в себе дані з

відкритих джерел в Інтернеті, такі як соціальні мережі, публічні бази даних, новинні статті, та інші відкриті ресурси.

Розвідка з відкритих джерел - це практика збору інформації з опублікованих або інших загальнодоступних джерел.

Технологія OSINT має широкий спектр застосувань у сфері розвідки та забезпечення безпеки. У розвідувальних операціях, вона використовується для збору великої кількості відкритої інформації про осіб, організації, або навіть держави. Аналіз соціальних мереж, форумів та інших відкритих платформ надає розвідникам можливість відстежувати зміни в громадському настрої, виявляти потенційні загрози та проводити аналіз публічних думок.

Розроблена концепція поєднує AI-моделі для обробки текстів і OSINT-методики перевірки джерел, що робить систему комплексним аналітичним інструментом.

Обрана мікросервісна архітектура гарантує гнучкість, масштабованість і стійкість до навантажень.

Надалі можливе розширення системи для роботи з відео, соціальними мережами та багатомовними джерелами. Майбутні перспективи у цій сфері виглядають дуже масштабно, з удосконаленням алгоритмів, розвитком штучного інтелекту та машинного навчання, що робить OSINT розвідку більш точною, швидкою та ефективною. Таким чином, використання технології OSINT для аналізу соціальних мереж має значний потенціал у різних сферах, включаючи безпеку, розвідку, бізнес-аналітику та громадську діяльність. Постійний розвиток цієї технології та її поєднання з іншими інноваційними підходами відкриває нові можливості для досягнень у майбутньому.

СИСТЕМА ВИЯВЛЕННЯ АНОМАЛІЙ МЕРЕЖЕВОГО ТРАФІКУ ПІД ЧАС DDoS-АТАК НА ОСНОВІ ЕНТРОПІЙНОГО МЕТОДУ

Яцик Олександр Іванович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент 2 курсу магістратури, спеціальність F5 «Кібербезпека»

У результаті виконання магістерської роботи було встановлено що потреба в легкоінтегрованій системі захисту може допомогти захистити малі та середні інтернет сервіси від DDoS атаки типу HTTP-flood. Це допоможе зменшити збитки для малого та середнього бізнесу, а також збільшить стабільність їх систем.

Було проаналізовано основні методи захисту баз даних. Та вибрано метод який відповідає на системні характеристики і середню інтенсивність інтернет трафіку сайтів малого бізнесу 1000-10000 одночасних запитів запитів. В результаті розробки, одержано систему яка ефективно захищає бази даних без додаткового навантаження на виробничу потужність серверів.

ICS / SCADA SECURITY: ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІД ЧАС ВІЙНИ

Гебрян Юрій Юрійович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54

студент магістратури 1 року навчання, спеціальність 125 «Кібербезпека»

Системи керування технологічними процесами (ICS) та диспетчерські системи SCADA становлять основу функціонування критичної інфраструктури: енергетики, водопостачання, транспорту, хімічної промисловості, логістики та об’єктів оборонного значення. У сучасних умовах війни їхня кібербезпека стає пріоритетним національним завданням, адже навіть короткочасне порушення роботи таких систем здатне спричинити серйозні економічні збитки, масштабні перебої у функціонуванні держави та створити загрозу для життя людей.

Кібератаки на ICS/SCADA сьогодні є невід’ємною частиною гібридних операцій. Зловмисники застосовують як інструменти загального призначення, так і спеціалізоване шкідливе ПЗ, розроблене для ураження промислових мереж і контролерів. Вони використовують фішинг, атакують віддалені доступи, компрометують постачальників, сканують промислові протоколи та намагаються змінити параметри технологічних процесів. Особливо небезпечні атаки, що спрямовані на фізичне руйнування обладнання або створення аварійних ситуацій — такі інциденти можуть мати катастрофічні наслідки.

Складність захисту полягає в тому, що багато промислових систем проєктувалися задовго до появи сучасних кіберзагроз. Вони використовують застарілі протоколи без шифрування, мають обмежені можливості оновлення та часто не призначені для роботи в умовах мережевої небезпеки. Крім того, підприємства нерідко нехтують сегментацією мереж, що створює можливість для проникнення з IT-сегмента в OT-середовище.

Ефективний захист ICS/SCADA вимагає багаторівневого підходу. Сегментація та ізоляція критичних компонентів є першими кроками, які значно обмежують можливості зловмисника. Далі необхідно впроваджувати спеціалізовані системи моніторингу OT-трафіку, що здатні виявляти аномалії у роботі технологічних протоколів. Важливо проводити регулярні аудити безпеки, тестування на проникнення та симуляції атак для оцінки реальної стійкості об’єктів.

Не менш значущим є людський фактор: персонал має бути навчений правилам кібергігієни, правильним діям під час інцидентів та принципам безпечної роботи з технологічними мережами.

У воєнний час кіберзахист критичної інфраструктури — це основа стійкості держави. Тільки поєднання технологій, підготовки кадрів і координації між державою та приватним сектором дозволить мінімізувати наслідки атак і забезпечити безперервність роботи життєво важливих систем.

СТВОРЕННЯ АВТОМАТИЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ВИЯВЛЕННЯ ЗМІНИ ТРАФІКУ ТА РІЗНИХ ВИДІВ АТАК ТИПУ MAN-IN-THE-MIDDLE (MITM)

Марко Євгеній Володимирович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

Представлена доповідь робота присвячена дослідженню атак типу Man-in-the-Middle у локальних комп’ютерних мережах та розробці програмного засобу для їх виявлення і протидії. У роботі проаналізовано основні види MITM-атак, особливу увагу приділено ARP-spoofing як одному з найпоширеніших способів реалізації таких атак у локальних мережах.

У процесі виконання роботи розроблено програмний модуль на мові Python, який здійснює моніторинг ARP-трафіку в режимі реального часу, виявляє підміну IP–MAC відповідностей та автоматично блокує джерела атак на мережевому обладнанні MikroTik. Створене програмне рішення поєднує функції системи виявлення та запобігання вторгненням (IDS/IPS) і може бути використане для підвищення рівня захищеності локальних і корпоративних мереж.

BEHAVIORAL BOT SHIELD: МУЛЬТИПАРАМЕТРИЧНИЙ РИЗИК-СКОРИНГ HTTP-ЗАПИТІВ НА ОСНОВІ ПОВЕДІНКОВИХ МЕТРИК ДЛЯ ЗАХИСТУ ВЕБ-ДОДАТКІВ

Бурак Віталій Васильович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

У доповіді представлено результати роботи, під час якої розглянуто проблему протидії автоматизованим бот-атакам у веб-додатках, що використовують HTTP-інтерфейси та зазнають зловживань на рівні запитів (сканування, credential stuffing, підбір ресурсів, масова реєстрація).

Метою роботи є розроблення системи Behavioral Bot Shield для виявлення підозрілої активності та прийняття рішення про обмеження або блокування запитів у режимі реального часу.

Запропоновано мультипараметричний ризик-скоринг, що поєднує поведінкові метрики (частота та “сплески” запитів, повторюваність шаблонів, характеристики клієнта, сигнали сесійної стабільності) із гібридним підходом до оцінювання: порогові правила та вагова агрегована модель з можливістю подальшого калібрування.

Наукова новизна полягає у комплексному застосуванні набору поведінкових параметрів до скорингу HTTP-запитів з урахуванням контексту взаємодії. Практичним результатом є працездатний прототип, що забезпечує моніторинг, логування та автоматичне блокування підозрілих запитів у реальному часі.

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ ВЗАЄМОДІЇ УРАЦИЛУ З АТОМАРНО ЧИСТОЮ ПОВЕРХНЕЮ (110) РУТИЛУ TiO_2: ВІД ТЕОРІЇ ДО ЕКСПЕРИМЕНТУ

Неймет Богдан Юрійович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
аспірант кафедри твердотільної електроніки та інформаційної безпеки

Дослідження механізмів взаємодії біомолекул з неорганічними поверхнями є критично важливим для розробки біосенсорів, медичних імплантів та матеріалів для біоелектроніки. У цій роботі представлено комплексне комп'ютерне моделювання взаємодії урацилу (однієї з основних складових нуклеїнових кислот) з атомарно чистою поверхнею (110) рутилу TiO_2 за допомогою методів теорії функціоналу густини (DFT) та молекулярної динаміки (MD).

Ми провели детальний аналіз фізико-хімічних властивостей урацилу та структури поверхні рутилу TiO_2(110). Урацил, як складова частина РНК, виявляє складну електронну структуру з наявністю водневих зв'язків та полярних груп, які визначають його реакційну здатність. Поверхня TiO_2(110) являє собою гідроксильовану структуру з активними центрами (Ti^{4+} та O^{2-}), що забезпечує можливість адсорбції органічних молекул.

Квантово-хімічні розрахунки проведені з використанням функціоналу PBE з врахуванням дисперсійних взаємодій (DFT-D3). Базисний набір та параметри обрізання енергії були оптимізовані для отримання збіжних результатів. Молекулярно-динамічне моделювання проводилось при різних температурах для дослідження динаміки адсорбційного процесу.

- Ідентифіковано кілька енергетично вигідних конфігурацій адсорбції урацилу на поверхні TiO_2(110). Розраховані енергії адсорбції для різних активних центрів поверхні. Детально досліджено природу хімічного зв'язку між

урацилом та поверхнею (переважно кумулятивні координаційні зв'язки з атомами титану), визначено енергетичні бар'єри дифузії молекули по поверхні. Прогнозовані спектральні характеристики для експериментального підтвердження (SERS, XPS, SRPES)

При адсорбції спостерігаються помітні деформації молекули урацилу та часткова реконструкція поверхні TiO_2. Аналіз розподілу електронної густини показує перерозподіл заряду між молекулою та поверхнею, що вказує на істотний гібридизацію електронних орбіталей.

Отримані результати забезпечують теоретичне обґрунтування для розробки біосенсорів на основі TiO_2, здатних детектувати нуклеїнові кислоти та їх компоненти. Знання про механізми адсорбції критично важливе для оптимізації поверхні та підвищення чутливості приладів.

Результати теоретичних розрахунків будуть експериментально верифіковані методами:

- SERS (поверхнево підсилена рамановська спектроскопія) – для дослідження молекулярних коливань
- XPS (рентгенівська фотоелектронна спектроскопія) – для аналізу хімічних зв'язків
- SRPES (синхротронна фотоелектронна спектроскопія) – для детального картування електронної структури.

Проведене комп'ютерне моделювання дає комплексне розуміння механізмів взаємодії урацилу з поверхнею рутилу TiO_2. Результати демонструють значний потенціал матеріалів на основі TiO_2 для біосенсорних застосувань та відкривають нові можливості для раціонального дизайну наноструктурованих матеріалів для біоелектроніки та медичних пристроїв.

Робота відповідає напрямку конференції з фундаментальних та прикладних досліджень в галузі інформаційно-комунікаційних технологій та матеріалознавства, а також демонструє застосування сучасних обчислювальних методів у науковому дослідженні.

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ПРОТИ АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В УМОВАХ ВОЄННОГО СТАНУ

Васильчук Владислав Олегович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

У доповіді представлено результати роботи з дослідження проблеми забезпечення інформаційної безпеки підприємств від атак соціальної інженерії в умовах воєнного стану. Актуальність теми зумовлена зростанням кількості соціально-інженерних атак, що в умовах збройного конфлікту набувають ознак гібридної загрози та спрямовані не лише на отримання конфіденційної інформації, а й на дестабілізацію роботи підприємств, вплив на поведінку персоналу та підрив довіри до державних і корпоративних інституцій.

У роботі проаналізовано сутність, класифікацію та сучасні методи соціальної інженерії, а також особливості їх застосування в умовах війни. Розглянуто соціальну інженерію як інструмент інформаційно-психологічного впливу в межах гібридних операцій, проаналізовано реальні приклади атак, що мали місце під час російсько-української війни, та визначено їхній вплив на інформаційну безпеку підприємств і суспільну стійкість.

У межах емпіричного дослідження проведено оцінку рівня обізнаності працівників підприємства щодо загроз соціальної інженерії, їх здатності розпізнавати маніпулятивні повідомлення та дотримуватися правил кібергігієни. На основі отриманих результатів виявлено ключові вразливості людського фактору в системі інформаційної безпеки підприємства.

За результатами дослідження розроблено освітньо-практичну програму підвищення обізнаності персоналу, спрямовану на формування навичок протидії соціально-інженерним атакам, розвитку критичного мислення та підвищення

психологічної стійкості в умовах воєнного стану. Практичне значення роботи полягає у можливості використання отриманих результатів у діяльності підприємств, органів кіберзахисту та освітніх установ з метою посилення інформаційної безпеки.

СИСТЕМА ДИСТАНЦІЙНОГО МОНІТОРИНГУ ДЛЯ КОНТРОЛЮ ПОГОДНИХ УМОВ У ВИСОКОГІР'ЯХ

Григаш Максим Михайлович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54

студент магістратури 2 року навчання, спеціальність 172 «Телекомунікації та радіотехніка»

Розглянуто принципи побудови систем віддаленого моніторингу на основі технології LoRa, для контролю віддалених об'єктів з передачею інформації по ефіру, які надають можливість організовувати збір та передачу даних про стан об'єктів, зокрема для контролю погодних умов у високогір'ях. Системи дистанційного збору даних належать до класу автоматизованих інформаційно-вимірювальних систем, які забезпечують збір, передавання, збереження та аналіз інформації з віддалених об'єктів у режимі реального часу або з певною періодичністю. Основна мета таких систем полягає у підвищенні ефективності моніторингу, керування процесами та прийняття рішень на основі достовірних даних, отриманих з різних джерел

Розвиток мікроелектроніки, бездротових технологій і мережевих протоколів сприяв переходу від локальних вимірювальних систем до масштабованих систем дистанційного збору даних, які здатні функціонувати на великих територіях і обслуговувати сотні або тисячі сенсорних вузлів. Такі системи широко застосовуються в енергетиці, екології, сільському господарстві, транспорті, а також у побутових і муніципальних застосуваннях. Типова структура системи дистанційного збору даних включає кілька взаємопов'язаних компонент: первинні перетворювачі, що здійснюють вимірювання фізичних величин та перетворюють їх у електричні сигнали; контролер – пристрій, який приймає сигнали від датчиків, проводить їх попередню обробку та формує пакети даних для передавання; канал зв'язку – середовище, через яке передається інформація до центру збору даних. Проведено оцінку ефективності

системи дистанційного моніторингу на базі технології LoRa та модуля ESP32, вивчення особливостей технології LoRa, розробку архітектури системи моніторингу, тестування її функціональності та оцінку ефективності в для контролю погодних умов у високогір’ях.

ВИКОРИСТАННЯ СИСТЕМИ КОМП'ЮТЕРНОГО ЗОРУ У ВИРОБНИЦТВІ ЕЛЕКТРОНІКИ

Гулич Володимир Володимирович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54

студент магістратури 2 року навчання, спеціальність 172 «Телекомунікації та радіотехніка»

Проведено порівняльний аналіз методів реалізації систем контролю якості друкованих плат та розроблено автоматизований пристрій для їх інспекції. Системи машинного зору (Machine Vision, MV) є одним із ключових технологічних інструментів сучасного виробництва. Вони забезпечують: **Неконтактний та високошвидкісний контроль; Збір даних у реальному часі; Автоматизоване прийняття рішень.**

MV-системи функціонують як інтелектуальні датчики, які здійснюють безперервний моніторинг, підтримуючи високу ефективність та гнучкість виробництва. Їхня робота базується на інтеграції високошвидкісних відео камер, профілометричних алгоритмів та потужних процесорів.

Такі системи виступають основними постачальниками даних для MES- та ERP-рішень, що дозволяє реалізувати замкнуті цикли контролю й проактивно оптимізувати виробничі процеси.

У сфері контролю електронної продукції, зокрема контролю якості друкованих плат на основі систем машинного зору застосовуються три основні технології:

- **SPI** — контроль якості друку паяльної пасти на друковані плати;
- **AOI** — автоматичний оптичний контроль;
- **AXI** — автоматичний рентгенівський контроль, виявлення прихованих дефектів, зокрема у BGA-компонентах.

Ефективне виробництво потребує гібридного підходу: швидкий AOI поєднується з вибірковим AXI для критичних вузлів.

Ключовим напрямом розвитку є інтеграція штучного інтелекту та машинного навчання, зокрема технології глибокого навчання підвищують точність виявлення дефектів, зменшують кількість хибних спрацьовувань і роблять системи більш стійкими у високошвидкісному виробничому середовищі.

РОЗРОБКА КРОСПЛАТФОРМНОГО ЗАХИЩЕНОГО МЕНЕДЖЕРА ПАРОЛІВ ЗА ДОПОМОГОЮ ФРЕЙМВОРКУ QT ТА АЛГОРИТМУ PBKDF2

Дужар Олександр Вікторович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

У представленій доповіді роботі проведено аналіз та розроблено кросплатформний застосунок для безпечного управління паролями з використанням алгоритмів PBKDF2 та AES-256-CBC. Основна увага спрямована на імплементацію надійного механізму захисту облікових даних та організацію локального сховища з шифруванням.

Проведено проєктування архітектури системи та реалізовано захист системи за допомогою майстер-пароля з використанням алгоритму PBKDF2 з 600000 ітерацій та алгоритму AES-256-CBC для шифрування бази даних. Продемонстрована доцільність застосування фреймворку Qt для кросплатформної розробки та бібліотеки SQLCipher для захищеного збереження облікових записів.

Розроблені функціональні компоненти для генерування стійких паролів, організації даних у папки, експорту та імпорту облікових даних у форматах CSV та JSON, безпечне очищення пам’яті та механізм автоматичного блокування при неактивності. Здійснено тестування ефективності розробленого менеджера паролів і проведено аналіз безпеки системи.

ІНТЕГРАЦІЯ ЦИФРОВОГО ПІДПИСУ З ТЕХНОЛОГІЯМИ БЛОКЧЕЙН У СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Паламарчук Олександр Сергійович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54

студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

У результаті виконання роботи встановлено, що потреба у застосуванні блокчейн-технологій у системах електронного документообігу постійно зростає у зв’язку з критичними недоліками централізованих рішень.

Традиційні системи ЕДО мають ризики єдиної точки відмови (12% організацій щорічно втрачають дані), можливість несанкціонованої модифікації документів та відсутність прозорого аудит-сліду.

Проаналізовано десять існуючих блокчейн-систем документообігу (Stampery, Blockcerts, Factom, IBM Blockchain та інші) та виявлено сім критичних обмежень: відсутність підтримки українського кваліфікованого електронного підпису (ДСТУ 4145-2002), компроміс між продуктивністю та децентралізацією, високі витрати на блокчейн-транзакції (від $5 до $50 у мережі Ethereum), обмежену функціональність смарт-контрактів. Досліджено чотири криптографічні алгоритми цифрового підпису (RSA-2048, ECDSA-256, EdDSA-256, ДСТУ 4145-256) та обґрунтовано вибір ECDSA для блокчейн-підписів через оптимальний баланс безпеки (128 біт) та компактності (64 байти).

Розроблено гібридну архітектуру зберігання даних, де метадані документів зберігаються у PostgreSQL для швидкого пошуку (1-10 мс), бінарні файли розміщуються в IPFS для економічності ($0.02/GB/міс), а криптографічні хеші та цифрові підписи записуються у блокчейн Polygon для забезпечення незмінності. Така модель дозволяє обробляти 99% запитів без звернення до блокчейну, забезпечуючи економію 99.96% коштів порівняно з повністю on-

chain рішенням (для 1000 документів на день економія становить $91.2 млн →$37.8 тис. на рік).

У результаті розробки програмного забезпечення створено функціональну систему електронного документообігу, що включає три смарт-контракти на Solidity (DocumentRegistry, SignatureValidator, AccessControl загальним обсягом 500 рядків коду), backend API на Node.js + TypeScript з сімома спеціалізованими сервісами, frontend застосунок на React 18 з інтеграцією Web3 через RainbowKit та Wagmi. Реалізовано адаптер для українського КЕП з автоматичною OCSP-перевіркою статусу сертифікатів у реальному часі.

Навантажувальне тестування (Apache JMeter, 100 одночасних користувачів, 50 документів/хвилину) показало продуктивність системи з p95 latency 200 мс, error rate 0.1%, що підтверджує масштабованість архітектури до 10,000 користувачів. Система розгорнута на тестовій мережі Polygon Mumbai з вартістю транзакції $0.001 (у 1000 разів дешевше за Ethereum mainnet).

Проведено порівняльний аналіз з чотирма конкурентними рішеннями, що продемонстрував переваги розробленої системи за критеріями економічності, продуктивності (7000 транзакцій/секунду), підтримки українського законодавства та відкритості вихідного коду.

РОЗРОБКА СИСТЕМИ ВИЯВЛЕННЯ ДІПФЕЙКІВ У МЕДІАКОНТЕНТІ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ

Равлюк Сергій Олександрович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54

студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

У сучасному світі технології штучного інтелекту досягли такого рівня розвитку, що стало можливим створювати високоякісні підроблені зображення та відео, які важко відрізнити від справжніх. Ці технології, відомі як діпфейки (deepfakes), створюють серйозні загрози для інформаційної безпеки, особистих даних, репутації людей та суспільної довіри. Діпфейки можуть використовуватися для поширення дезінформації, шахрайства, шантажу та інших злочинних дій.

Традиційні методи детекції діпфейків, що базуються на одній моделі глибокого навчання, мають обмеження: вони можуть давати хибні спрацьовування на зображеннях поганої якості, не враховують різні типи артефактів генерації та не забезпечують пояснюваність результатів. Мета дослідження полягала в розробці системи багатокритеріального аналізу зображень для детекції діпфейків, яка інтегрує кілька незалежних методів детекції та забезпечує високу точність та пояснюваність результатів.

Наукова новизна роботи полягає в розробці комплексного підходу до детекції діпфейків, що поєднує кілька незалежних методів аналізу (глобальні моделі детекції, частотний аналіз, геометричний аналіз) з урахуванням якості вхідного зображення та забезпеченням пояснюваності результатів. Практична значущість полягає в створенні готового до використання desktop-додатку, який може бути використаний для перевірки зображень на наявність діпфейків у різних сферах: журналістиці, правоохоронних органах, соціальних мережах тощо.

БАГАТОРІВНЕВИЙ ЗАХИСТ МОБІЛЬНОГО ОФЛАЙН-ФІНАНСОВОГО ЗАСТОСУНКУ

Боценюк Любомир Русланович

ДВНЗ «Ужгородський національний університет»
88000, Ужгород, вул. Волошина, 54
аспірант фізичного факультету

Сьогодні смартфон фактично став персональним сховищем конфіденційної інформації: від фото й листування до банківських застосунків та приватних фінансових нотаток. Саме тому захист даних на телефоні є не менш важливим, ніж захист у мережі. Реальні ризики часто виникають у повсякденних ситуаціях: підглядання через плече, випадковий скріншот, запис екрана, відкритий застосунок у “recent apps” або короткий доступ до пристрою без власника. Навіть якщо застосунок працює офлайн і не передає дані на сервер, загроза витоку не зникає — вона просто зміщується на локальне зберігання та поведінку інтерфейсу.

У межах проєкту створено мобільний офлайн-фінансовий застосунок для обліку та керування коштами. Він дозволяє створювати кілька гаманців, задавати назву, валюту та суму, додавати курс обміну й одразу бачити перерахунок у гривню. Застосунок підраховує загальний баланс по всіх гаманцях, підтримує редагування й видалення записів, зміну порядку гаманців, а також має режим приватності: суми можна швидко замаскувати або показати керовано — окремо по кожному гаманцю чи одразу для всіх.

Захист реалізований за принципом багаторівневості (defense-in-depth), коли безпека не зводиться до одного механізму, а розподіляється на кілька незалежних шарів.

Перший рівень — автентифікація доступу: вхід через PIN-код і, за потреби, біометрію (Face ID/Touch ID) з коректною обробкою сценаріїв, коли користувач просто скасовує біометричну перевірку.

Другий рівень — захист від підбору коду: ліміт невдалих спроб і прогресивне блокування (1 секунда → 2 → 5 → 10 → 30…), що робить brute-force практично неефективним, при цьому користувач бачить прозорий таймер блокування.

Третій рівень — контроль сесії: автоматичне блокування при неактивності та при поверненні застосунку з фону, щоб фінансова інформація не залишилася відкритою без нагляду.

Четвертий рівень — захист від витоку через інтерфейс: заборона скріншотів/запису екрана та захист прев'ю в перемикачі застосунків там, де це підтримується платформою.

Окремо важливий базовий принцип — безпечне зберігання: чутливі дані та ключі доступу зберігаються в захищеному сховищі пристрою в зашифрованому форматі, щоб навіть у разі доступу до файлів вони не читалися у відкритому вигляді.

Додатковим напрямом у межах проєкту став модуль Face ID, який розширює класичну ідею "пустити / не пустити". У більшості застосунків біометрія — це бінарна перевірка: користувач пройшов автентифікацію і отримав доступ. У моєму випадку підхід інший: Face ID виступає інструментом ідентифікації, тобто дозволяє не просто підтвердити факт входу, а визначити, хто саме зайшов у систему. Це дає можливість прив'язувати сесію до конкретної особи, а також застосовувати розмежування доступу залежно від ролі. Концепція працює так: під час реєстрації для користувача створюється локальний профіль з ідентифікатором та роллю, а під час входу здійснюється біометричне розпізнавання, яке визначає відповідність до одного з зареєстрованих профілів. Після успішної ідентифікації система може надавати різні рівні доступу до функцій і даних. Таким чином, біометрія перетворюється на основу керування правами, а не лише на зручний "замок" для входу.

Логічним продовженням розвитку застосунку є поглиблення цього механізму: розширення системи ролей і політик доступу, додавання сценаріїв "підвищеного підтвердження" для критичних дій (повторна ідентифікація), а також гнучке налаштування правил приватності під конкретного користувача.

Перспективними є й режими спільного використання одного пристрою кількома людьми, ведення безпечного локального журналу подій (без фінансових деталей, але з фіксацією фактів входу/виходу) та посилення захисту локального зберігання і резервних копій, щоб навіть у разі компрометації середовища дані залишаються недоступними без ключів і підтвердження особи.

У підсумку багаторівневий підхід дозволяє зробити офлайн-фінансовий застосунок не лише зручним, а й стійким до типових реальних загроз. Він поєднує механізми операційної системи, продуману логіку доступу та приватність у UI, формуючи просте правило: навіть якщо один бар’єр не спрацює, інші шари все одно зменшать ризик витоку та несанкціонованого доступу.

DFT-РОЗРАХУНКИ ЕЛЕКТРОННОЇ СТРУКТУРИ КРИСТАЛІВ $Li_2B_4O_7$ У КЛАСТЕРНОМУ НАБЛИЖЕННІ

Янтолик Юрій Михайлович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54

студент магістратури 2 року навчання, спеціальність 176 «Мікро-та наносистемна техніка»

У роботі розглянуто структурні особливості та ключові фізичні характеристики кристалів тетраборату літію, а також наведено аналіз основних підходів до першопринципних розрахунків.

Виконано ab initio моделювання рівноважної геометричної структури, параметрів електронної будови та коливальних спектрів для кластерних моделей кристала $Li_2B_4O_7$. Розрахунки проводилися за допомогою обмеженого за спіном методу Хартрі-Фока (RHF) із застосуванням базисного набору 6-31G*.

В результаті роботи було підтверджено стабільність досліджуваних кластерів та збереження ними топології кристалічної решітки. На базі розроблених моделей обчислено повну та парціальну густину електронних станів сполуки.

Здійснено порівняння отриманих теоретичних даних інфрачервоних спектрів та спектрів комбінаційного розсіювання світла для $Li_2B_4O_7$ із наявними експериментальними показниками.

РОЗРОБКА СИСТЕМИ БЕЗПЕЧНОГО ОБМІНУ ПОВІДОМЛЕННЯМИ З ВИКОРИСТАННЯМ НАСКРІЗНОГО ШИФРУВАННЯ

Нагірний Ростислав Олегович

ДВНЗ «Ужгородський національний університет»

88000, Ужгород, вул. Волошина, 54

студент магістратури 2 року навчання, спеціальність 125 «Кібербезпека»

У сучасному цифровому суспільстві проблема захищеного спілкування стала одним із ключових пріоритетів у сфері інформаційних технологій. Зі зростанням кількості кіберзагроз, спроб злому та несанкціонованого доступу до персональних даних суттєво зростає потреба в надійних механізмах конфіденційного обміну інформацією між користувачами.

У роботі проведено аналіз теоретичних і практичних підходів до забезпечення безпеки комунікаційних систем із особливим акцентом на технології наскрізного шифрування (End-to-End Encryption, E2EE). Досліджено принципи функціонування алгоритмів шифрування (AES, RSA) і методів безпечного обміну ключами, а також їх імплементацію в клієнт-серверній архітектурі на основі ASP.NET Core, React і PostgreSQL.

Метою роботи є проєктування та реалізація системи захищеної комунікації між користувачами, яка забезпечує конфіденційність, цілісність даних та захист від несанкціонованого доступу.

У межах цієї загальної мети автор вирішує такі завдання:

1. описати теоретичні та методологічні засади захищених комунікаційних систем;

2. проаналізувати основні типи алгоритмів шифрування та механізмів автентифікації;

3. реалізувати прототип системи безпечного обміну повідомленнями з використанням сучасних програмних технологій;

4. оцінити рівень безпеки, ефективності та потенційні загрози для розробленого рішення.

Об’єктом дослідження є системи захищеної комунікації, що забезпечують конфіденційний обмін повідомленнями між користувачами. Предметом дослідження є архітектура, алгоритми та особливості реалізації системи обміну повідомленнями з наскрізним шифруванням.

м