НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

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

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

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

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

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

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

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

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

UDC 004.056

Editor-in-chief:

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

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

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

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

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

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

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

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

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

інформаційної безпеки істотно підвищують здатність користувачів розпізнавати загрози та коректно реагувати на інциденти.

Окрему увагу в роботі приділено етичним і правовим аспектам проведення навчальних фішингових симуляцій. Показано, що подібні дослідження є допустимими виключно за умов інформованої згоди учасників, мінімізації потенційної шкоди, прозорості методики та обов'язкового видалення чутливих даних після завершення аналізу.

Практична значущість отриманих результатів полягає в можливості їх застосування під час розроблення програм підвищення обізнаності з кібербезпеки, створення внутрішніх регламентів реагування на фішингові інциденти та впровадження обов'язкових механізмів багатофакторного захисту в освітніх і корпоративних інформаційних системах.

Список використаної літератури:

1. Putra F. P. E. et al. Analysis of phishing attack trends, impacts and prevention methods: literature study. Brilliance: Research of Artificial Intelligence. 2024. Vol. 4, No. 1. P. 413-421.
2. Alghenaim M. F. et al. Phishing attack types and mitigation: A survey. The International Conference on Data Science and Emerging Technologies. Singapore : Springer Nature Singapore, 2022. P. 131-153.

Ключові слова: фішинг, фішингова атака, поведінкові вразливості, людський фактор, соціальна інженерія, навчальна фішингова симуляція, кібергігієна, аналіз реакції користувачів, кібербезпека.
Keywords: phishing, phishing attack, behavioral vulnerabilities, human factor, social engineering, educational phishing simulation, cyber hygiene, user reaction analysis, cybersecurity.

СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАХИСТУ ЛОГІВ

Бойко Віктор

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

Вуль Анастасія

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

Сучасні інформаційно-комунікаційні системи (ІКС) генерують величезні обсяги логів – журналів подій, що є основним джерелом інформації для моніторингу, виявлення інцидентів безпеки та розслідування кібератак [1]. Саме на основі логів фахівці з кібербезпеки визначають, коли і як відбулося

вторгнення, встановлюють причини інцидентів та відновлюють хронологію подій. Проте традиційні системи зберігання логів виявляються вразливими до фальсифікацій, несанкціонованих змін та видалення даних [2]. Зловмисник, отримавши доступ до серверів, може не лише здійснити атаку, а й приховати свої сліди шляхом модифікації логів. Це унеможливлює об'єктивне розслідування події та значно знижує довіру до систем кіберзахисту, навіть у доброчесних адміністраторів виникає проблема довіри до даних логів, адже вони зберігаються централізовано і не мають захисту від внутрішнього втручання.

Проблема автентичності та цілісності логів стає критичною у контексті сучасних кібератак, особливо для великих корпорацій, державних установ і провайдерів послуг. Одним із найперспективніших напрямів вирішення цієї проблеми є застосування технології блокчейн для децентралізованого зберігання логів [3]. Використання блокчейну дозволяє створити незмінну хронологічну послідовність записів, де кожен блок є криптографічно захищеним і пов'язаний із попереднім. Це унеможливлює підробку чи знищення записів навіть у разі компрометації окремих вузлів системи [4].

Тому постає питання: як зробити логи незмінними, достовірними та перевірюваними? Відповіддю може бути використання технології блокчейн, яка дозволяє створювати децентралізовану, прозору й захищену систему зберігання логів.

Мета даного дослідження – розробити концепцію системи виявлення вторгнень, у якій усі журнали подій (логи) записуються до блокчейну, що забезпечує їхню цілісність, автентичність і неможливість фальсифікації.

Система зберігання логів на базі блокчейну необхідна:

- організаціям із підвищеними вимогами до кіберзахисту, де важливо мати достовірні докази у випадку інцидентів (банки, держустанови, енергетичні компанії);
- хмарним провайдерам та дата-центрам, які обробляють великі обсяги журналів із різних серверів і клієнтів;
- командам безпеки (SOC), що проводять моніторинг, аудит і реагування на інциденти;
- системам штучного інтелекту для кіберзахисту, яким потрібні достовірні навчальні дані з реальних логів.

Для всіх цих випадків ключовою вимогою є довіра до логів: якщо дані можуть бути підроблені, уся система аналітики втрачає сенс.

Система виявлення вторгнень із блокчейн-захистом логів поєднує класичні механізми збору подій із децентралізованим зберіганням.

Основні етапи роботи виглядають так:

1. Збір логів. Модулі-агенти встановлюються на вузлах мережі (сервери, маршрутизатори, робочі станції). Вони відстежують події авторизації, мережевий трафік, помилки системи, запити до баз даних тощо.

2. Формування запису. Кожен лог перетворюється на структурований об'єкт, що містить часову мітку, джерело події, тип активності, цифровий підпис агента.

3. Хешування та запис у блокчейн. Система обчислює SHA-512 хеш від змісту запису та додає його у блок разом із попереднім хешем. Завдяки цьому будь-яка спроба змінити лог змінить увесь ланцюг блоків.

4. Розповсюдження між вузлами. Копія блокчейну зберігається на кількох вузлах системи. Навіть якщо один сервер буде зламаний, дані можна перевірити через інші копії.

5. Виявлення вторгнень. Аналітичний модуль аналізує нові логи (зокрема з використанням машинного навчання або сигнатур), фіксує підозрілі дії й створює відповідний блок у ланцюгу.

6. Верифікація логів. Адміністратор може будь-коли перевірити справжність записів, порівнявши хеші з блокчейну з локальними журналами.

Переваги підходу: Незмінність(жоден запис логу не може бути видалений або змінений без сліду), Децентралізація(логи не зберігаються на одному сервері — це унеможливлює знищення доказів атаки), прозорість(усі учасники системи мають однакову копію блокчейну, що гарантує єдиний стан журналів), доказовість(у разі розслідування кібератак логи з блокчейну можуть виступати надійними цифровими доказами), автоматизація(смарт-контракти можуть автоматично створювати сповіщення чи блокувати IP-адреси при повторних інцидентах).

Таким чином, система забезпечує не лише виявлення загроз, а й захист самих даних, на основі яких робиться аналіз.

У процесі дослідження було проведено аналіз сучасних систем управління логами (ELK Stack, Splunk, Graylog) та рішень із використанням блокчейн-технологій у сфері інформаційної безпеки [6]. Виявлено, що хоча вони забезпечують потужну аналітику, але не гарантують незмінність записів.

Для усунення цього недоліку було розроблено прототип гібридної системи, що об'єднує збір логів із блокчейн-зберіганням.

До складу прототипу входять:

- Агент збору логів на Python, який зчитує системні журнали подій і перетворює їх на транзакції.

- Модуль хешування для створення криптографічних відбитків (SHA-512).

- Приватний блокчейн на основі технології Hyperledger Fabric, який зберігає усі записи.
- Веб-інтерфейс для перегляду журналів, перевірки їх автентичності та моніторингу атак.

Тестування показало, що навіть при спробі вручну змінити лог на сервері, хеш перевірки не збігається з записом у блокчейні, і система фіксує факт підробки. Це доводить ефективність методу для гарантованої цілісності логів у корпоративних мережах.

У ході роботи ми довели, що використання технології блокчейн для зберігання логів у системах виявлення вторгнень дозволяє вирішити одразу кілька критичних проблем:

- забезпечити цілісність журналів подій;
- гарантувати достовірність даних навіть при зламі сервера;
- створити повну історію змін і часову хронологію подій.

Ми реалізували прототип, який успішно фіксує події безпеки, записує їх у блокчейн і дозволяє перевіряти справжність логів у будь-який момент. Система продемонструвала стабільність, масштабованість і повну відсутність можливостей для маніпуляцій із записами.

Ми змогли об’єднати аналітику безпеки з криптографічним захистом журналів, створивши інноваційний підхід до моніторингу інцидентів. Цей підхід не лише підвищує рівень довіри до систем виявлення вторгнень, а й формує нову культуру прозорого зберігання цифрових доказів.

Подальші кроки в розвитку проєкту передбачають:

- розширення системи для обробки великої кількості логів у реальному часі;
- застосування штучного інтелекту для аналізу шаблонів атак у блокчейні;
- інтеграцію з існуючими IDS, такими як Snort або Suricata;
- реалізацію розподіленої аналітики, коли різні організації можуть спільно перевіряти достовірність логів, не розкриваючи конфіденційних даних.

Таким чином, створена система є важливим кроком у розвитку прозорих, надійних і стійких до фальсифікації систем безпеки, у центрі яких стоїть захищений журнал подій — лог, гарантований технологією блокчейн.

Список використанних джерел:

1. Zyskind G., Nathan O., Pentland A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops, 2015. URL: https://ieeexplore.ieee.org/document/7163223
2. Conti M., Dehghantanha A., Franke K., Watson S. Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications. IEEE Communications Surveys & Tutorials, 2018. URL: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9739
3. Kshetri N. 1 Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy. Telecommunications Policy, 2017. URL: https://www.sciencedirect.com/science/article/abs/pii/S0308596117302483
4. Бойко В., Василенко М., Слатвінська В. *Моделювання живучості та відновлення інформаційно-комунікаційних мереж в умовах дії кіберзагроз.* Інформаційні технології та суспільство, 2024, №1 (12), с. 13–19. URL: https://journals.maup.com.ua/index.php/it/article/view/3143
5. Lihua Song, Zongke Zhu, Menghen Li, Li Ma, Xinran Ju. A Novel Access Control for Internet of Things Based on Blockchain Smart Contract. IEEE Access, 2021. URL: https://ieeexplore.ieee.org/document/9390662
6. GDPR-Compliant Use of Blockchain for Secure Usage Logs – Zieglmeier V., Loyola Daiqui G, 2021. URL: https://arxiv.org/abs/2104.09971?utm_source=chatgpt.com

Ключові слова: блокчейн, журналювання, цілісність логів, система виявлення вторгнень, Hyperledger Fabric, SHA-512, цифрові докази, незмінність даних, криптографічний хеш-ланцюг.

Keywords: blockchain, logging, log integrity, intrusion detection system (IDS), Hyperledger Fabric, SHA-512, digital evidence, data immutability, cryptographic hash chain.

ПРОВЕДЕННЯ SQL-ІН'ЄКЦІЇ З ВИКОРИСТАННЯМ SQLMAP

Клевець Михайло

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

SQL-ін'єкції – одна з найстаріших та одночасно найефективніших технік компрометації вебзастосунків: при вдалому використанні вони дозволяють читати, змінювати або видаляти дані, отримувати облікові дані, а іноді й виконувати команди операційної системи.

Автоматизація атак (наприклад, із застосуванням SQLMap) значно знижує поріг входу для зловмисника і дозволяє за короткий час провести розвідку та екстракцію даних. Це робить регулярне тестування критично важливим для розробників і адміністраторів.

У даних тезах досліджуються методи проведення SQL-ін'єкцій та автоматизація таких атак із використанням утиліти SQLMap. З огляду на те,

ЗМІСТ