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)

СИСТЕМИ РАНЖУВАННЯ ТА АНАЛІЗУ ІНФОРМАЦІЇ ПРИ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Кухаренко Сергій

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

Сидорчук Владислав

Національний університет «Одеська юридична академія», PhD в галузі права, доцент кафедри кримінального процесу

Стрімке зростання кількості кіберінцидентів потребує створення ефективних систем їх обробки та аналізу. За даними CERT-UA, у 2024 році було опрацьовано 4315 кіберінцидентів, що на 69,8% більше порівняно з 2023 роком [1]. Це актуалізує необхідність впровадження автоматизованих систем ранжування та інтелектуального аналізу даних для оптимізації протидії кіберзлочинам.

Метою дослідження є розробка практичної системи ранжування інформації про кіберінциденти та визначення ключових напрямків аналізу даних для ефективної протидії кіберзлочинам.

1. Методи збору інформації про кіберінциденти

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки в Україні", кіберінцидент визначається як подія або ряд несприятливих подій, які становлять загрозу безпеці електронних комунікаційних систем та створюють імовірність порушення їх штатного режиму
функціонування [2].

Для ефективного збору інформації про кіберінциденти застосовуються різноманітні методи та технології:

1.1. Системи виявлення та запобігання вторгненням (IDS/IPS) здійснюють моніторинг мережевого трафіку в режимі реального часу, виявляючи підозрілу активність. До таких систем належать Snort, Suricata, Zeek та Cisco Firepower [3]. Основною перевагою є автоматичне блокування атак, проте вони характеризуються високим рівнем помилкових спрацювань.

1.2. SIEM-системи (Security Information and Event Management) забезпечують централізований збір, аналіз і кореляцію логів з різних джерел. Популярні рішення включають Splunk, IBM QRadar, ArcSight та Elastic Stack [4]. Це потужний інструмент аналітики, але характеризується високою вартістю та складністю впровадження.

1.3. Threat Intelligence платформи спеціалізуються на зборі, аналізі та обміні даними про загрози. Використання таких платформ як MISP,

ThreatConnect, Anomali забезпечує проактивний захист та контекстуалізацію загроз [5].

1.4. DLP системи (Data Loss Prevention) запобігають витоку конфіденційних даних, контролюючи їх передачу. Рішення від Symantec, McAfee та Forcepoint DLP забезпечують compliance, але можуть обмежувати робочі процеси [6].

1.5. Honeypots/Honeynets – системи-приманки для залучення атакуючих, що дозволяють вивчати їх тактики та отримувати раннє попередження про загрози [7].

В Україні функціонує національна система реагування на кіберінциденти, ключовим елементом якої є CERT-UA. Цей орган здійснює моніторинг, накопичення та проведення аналізу даних про кіберінциденти на національному рівні [2]. Згідно з Порядком взаємодії суб'єктів національної системи реагування, CERT-UA невідкладно інформує СБУ про значні кіберінциденти щодо об'єктів критичної інфраструктури та Національну поліцію – про кібератаки на такі об'єкти [8].

2. Система ранжування кіберінцидентів

Зважаючи на постійне зростання кількості кіберінцидентів, критично важливою є розробка системи їх ранжування для визначення пріоритетності реагування (дивись рисунок 1).

Рисунок 1 – Алгоритм ранжування кіберінциндентів

2.1. Критерії ранжування

Запропонована система базується на шести ключових критеріях:

1. Об'єкт інциденту:
– об'єкт критичної інфраструктури або військовий об'єкт – 3 бали;
– державна або комунальна установа – 2 бали;
– приватна установа – 1 бал.
2. Ризики для обороноздатності держави:
– катастрофічні наслідки – 3 бали;
– значні наслідки – 2 бали;
– незначні наслідки – 1 бал;
– відсутні наслідки – 0 балів.
3. Розмір матеріального збитку:
– катастрофічний збиток – 3 бали;
– значний збиток – 2 бали;
– незначний збиток – 1 бал;
– відсутній збиток – 0 балів.
4. Джерело інциденту:
– зовнішнє джерело – 2 бали;
– внутрішнє джерело – 1 бал.
5. Рівень складності атаки:
– складна, багатоетапна атака – 3 бали;
– середній рівень складності – 2 бали;
– низький рівень складності – 1 бал;
– відсутні ознаки кібератаки – 0 балів.
6. Статус активності:
– активна загроза – 3 бали;
– неактивна загроза – 0 балів.

2.2. Формула розрахунку рангу.

Для визначення рангу кіберінциденту використовується формула:

$R = \Sigma(O)$

де O – оцінка за кожним критерієм.

Діапазон можливих значень: $2 \leq R \leq 17$

2.3. Класифікація за рівнями небезпеки

– Високий рівень небезпеки: 11-17 балів
– Середній рівень небезпеки: 5-10 балів
– Низький рівень небезпеки: 2-4 бали

Така система дозволяє автоматизувати процес пріоритизації реагування на інциденти та оптимізувати розподіл ресурсів служб кібербезпеки.

3. Напрямки аналізу даних за допомогою data mining

Data Mining – процес автоматичного виявлення прихованих закономірностей у необроблених даних, які мають практичну цінність та можуть бути інтерпретовані людиною [9]. При протидії кіберзлочинам технології Data Mining застосовуються у наступних напрямках:

3.1. Аналіз мережевого трафіку

Спрямований на виявлення несанкціонованого доступу (спроби підключення до закритих портів, експлуатація вразливостей), зловмисного програмного забезпечення (поширення вірусів, шифрування файлів) та витоку даних (несанкціонована передача конфіденційної інформації). Додатково здійснюється контроль дотримання політики безпеки.

3.2. Аналіз поведінки користувачів

Дозволяє виявляти аномальну активність користувачів, внутрішні загрози (співробітники, які викрадають дані або обходять політику безпеки) та будувати поведінкові профіли, що включають середній час активності, типи використовуваних файлів, характер мережевого трафіку та частоту авторизацій.

3.3. Аналіз фішингу

Застосовується для автоматичного виявлення фішингових листів через аналіз структури тексту, наявності підозрілих посилань та маніпулятивного стилю. Включає аналіз URL-адрес та доменів, виявлення фішингових доменів за схожістю до легітимних, знаходження новостворених доменів та аналіз підозрілих редиректів.

3.4. Аналіз вразливостей

Поділяється на два напрямки:

Аналіз «вразливостей» осіб: визначення категорій користувачів, схильних до ризикованої поведінки (відкриття небезпечних листів, відвідування підозрілих сайтів, використання слабких паролів). Формування індивідуальних профілів ризику дозволяє запобігти інсайдерським загрозам.

Аналіз технічних вразливостей: виявлення програмних вразливостей у системах, мережевих аномалій, слабкостей автентифікації, конфігураційних помилок та вразливостей у хмарних сховищах.

3.5. Кластеризація кіберзагроз та інцидентів

Дозволяє групувати однотипні атаки, виявляти приховані закономірності між інцидентами, будувати таксономію загроз, здійснювати пріоритизацію реагування та виявляти нові типи атак.

3.6. Асоціативний аналіз подій

Встановлює причинно-наслідкові зв’язки між подіями, виявляє залежності між кроками атаки, створює асоціативні правила типу "якщо-то", формує індикатори безпеки та автоматизує реагування на інциденти.

Висновки

1. Протидія кіберзлочинам потребує комплексного підходу, що включає використання різноманітних методів збору інформації про кіберінциденти – від систем IDS/IPS до SIEM-систем та Threat Intelligence платформ.

2. Розроблена система ранжування кіберінцидентів на основі шести критеріїв дозволяє автоматизувати процес визначення пріоритетності реагування та ефективно розподіляти ресурси служб кібербезпеки.

3. Застосування технологій Data Mining у протидії кіберзлочинам відкриває можливості для глибинного аналізу мережевого трафіку, поведінки користувачів, виявлення фішингу, аналізу вразливостей та кластеризації загроз.

4. Інтеграція систем ранжування з методами інтелектуального аналізу даних створює потужний інструментарій для проактивного запобігання кіберзлочинам та оперативного реагування на кіберінциденти.

5. Подальший розвиток систем протидії кіберзлочинам має включати впровадження технологій штучного інтелекту з обов'язковим контролем якості результатів та врахуванням потенційних ризиків автоматизованого прийняття рішень.

Список використаних джерел:

1. CERT-UA минулого року опрацювала 4315 кіберінцидентів. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv
2. Про основні засади забезпечення кібербезпеки в Україні : Закон України від 05 жовтня 2017 року, № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Що таке (IPS/IDS) і де застосовується. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujet-sya
4. Смірнова Т., Константинова Л., Конопліцька-Слободенюк О., Козлов Я., Кравчук О., Козірова Н., Смірнов О. Дослідження сучасного стану SIEM-систем. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2024. № 1(25). С. 6–18. https://doi.org/10.28925/2663-4023.2024.25.618
5. Дорохін О.О., Марченко В.В., Семенова І.Д. Технологія threat intelligence та методи її використання для захисту компанії від кіберзагроз. Сучасний захист інформації. 2021. № 3(47). С. 12-16.
6. Гайдур Г., Марченко В., Борсуковський Ю., Дмітрієв В., Царьова С. DLP-система як компонент протидії інсайдерським загрозам конфіденційності інформації. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2025. № 2(30). С. 583–592. https://doi.org/10.28925/2663-4023.2025.30.995
7. Притула А. В., Куперштейн Л. М. Технологія honeypot як альтенативний підхід виявлення вразливостей. Вінницький національний технічний університет, Вінниця. URL: https://surl.li/fujlqo

8. Порядок взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності : Постанова КМУ від 13 листопада 2025 року, № 1471. URL: https://zakon.rada.gov.ua/laws/show/1471-2025-п#n8
9. DataMining з використанням Python. Навчальний посібник // Юрченко І.В.– Чернівці: Чернівецький національний університет імені Юрія Федьковича, 2024.– 143 с. URL: https://surl.lu/szhxwy

Ключові слова: кібербезпека, управління кібербезпекою, кіберінцидент, кіберзлочин, ранжування кіберінциндентів, методи та засоби кібербезпеки.
Key words: cybersecurity, cybersecurity management, cyber incident, cyber crime, cyber incident ranking, cybersecurity methods and tools

БЕЗПЕКА ANDROID-ЗАСТОСУНКІВ НА KOTLIN ТА JETPACK COMPOSE

Манаков Сергій

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

Безпека мобільних застосунків у 2025 році стає актуальною компетенцією для розробників через швидку еволюцію загроз. Нативні Android-застосунки на Kotlin та Jetpack Compose вимагають особливого підходу до безпеки. Метадані компілятора Kotlin зберігають оригінальні імена навіть після обфускації, що спрощує зворотну розробку [1]. Дослідження показують, що жорстко закодовані API-ключі легко витягуються з APK, а багато застосунків використовують SharedPreferences без шифрування.

Основні загрози включають неправильне поводження з обліковими даними, слабку автентифікацію, недостатній захист бінарних файлів та небезпечне зберігання даних [2]. Особливої актуальності набула безпека ланцюга постачання для Compose-застосунків через інтенсивне використання залежностей та відсутність специфікації Software Bill of Materials. Важливою зміною 2025 року стала депрекація бібліотеки androidx.security:security-crypto, що вимагає міграції на пряме використання Android Keystore (база даних сертифікатів безпеки, яка створюється за допомогою програми keytool із пакету SDK для Java).

Практичні дослідження виявляють систематичні помилки безпеки в Kotlin-застосунках [3]. Серед найпоширеніших – жорстко закодовані облікові дані, зберігання секретів у налаштуваннях збирача проєктів gradle, ігнорування обфускації метаданих Kotlin та відсутність обробника винятків корутин CoroutineExceptionHandler. Специфічними для Compose помилками є зберігання чутливих даних у remember, витоки пам'яті через неправильне

ЗМІСТ