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)

7. Springer (2012). *Serious Games and Their Applications in Education.* URL: https://link.springer.com/chapter/10.1007/978-3-642-27355-1_3
8. *Journal of Multimedia Technology and Trends (2023).* URL: https://journal.educol-labs.org/index.php/JMTT/issue/archive

Ключові слова: генеративний ШІ.
Keywords: generative AI.

АНАЛІЗ СУЧАСНОГО СТАНУ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРЗАГРОЗАМ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Світличний Дмитро

Національний технічний університет «Харківський політехнічний інститут», аспірант кафедри кібербезпеки

У сучасному світі розвиток технологій призвів одночасно до вдосконалення та прогресу атак і загроз у сфері кібербезпеки на об'єкти критичної інфраструктури (ОКІ). Такі атаки відбуваються кожний день, або, якщо брати до уваги ОКІ по всій планеті, постійно. Це зумовлює високий пріоритет для створення захисту та протидії цим атакам. Першочерговим завданням є дослідження, аналіз та класифікація атак на ОКІ.

Сучасні дослідження [1-3] показують, що цифровізація, конвергенція управління інформацією та даними (Information Technology, IT) із управлінням і контролем фізичних процесів і устаткуванням (Operational Technology, OT) та масове підключення пристроїв збільшують площу атаки й створюють умови для складних кібератак на ОКІ з наслідками для нацбезпеки та економіки.

Найпоширеніші загрози для ОКІ [1]:

- шкідливе програмне забезпечення,
- програми-вимагачі,
- фішинг,
- розподілена атака типу "Відмова в обслуговуванні" (DDoS),
- атака нульового дня (zero-day),
- атаки на ланцюг постачання,
- довготривалі розширені постійні загрози.

Для енергетики ризики підсилюють легасі-системи, інтеграція IT та OT і швидке зростання Інтернету речей (Internet of Things, IoT) (сенсори, смарт-

лічильники, тощо), що розширює вектори атак і ускладнює захист операційних технологій. Згідно до роботи [1], підкреслюється основні три групи проблем:

- технічні (легасі системи контролю та збору даних, легасі системи промислового контролю, інтеграція IT та OT, IoT),
- організаційні (низька обізнаність, дефіцит кадрів, відсутність політик),
- регуляторні (строгі, але не завжди практичні вимоги).

Рішення: застосування штучного інтелекту (ШІ) та машинного навчання (МН) для виявлення аномалій у мережевому трафіку, блокчейну для захисту транзакцій і даних смарт-мереж, регулярних аудитів, інцидент-планів і тренінгів для персоналу. Важлива роль публічно-приватних партнерств для обміну даними.

Для виявлення атак на ОКІ існують різні технології на базі ШІ та МН. У роботі [4] було продемонстровано використання моделі МН Початок (Inception) для аналізу датасету UNSW-NB15. Результати: точність (частка правильно класифікованих прикладів, як атак, так і нормального трафіку) 98.40%, влучність (відсоток коректно визначених атак серед усіх, які модель позначила як загрози) 99%, впізнавання (здатність моделі виявляти реальні атаки серед усіх наявних атак) 97.9%, оцінка F1 (узагальнений показник, що поєднує влучність і впізнавання та свідчить про збалансовану роботу моделі) 98.5%. Порівняння з іншими моделями МН Випадковий ліс (Random Forest), k найближчих сусідів (k-Nearest Neighbors) та багатошаровий перцептрон (Multi-Layer Perceptron) довело перевагу глибокого навчання у масштабованості та точності. Практичні можливості для застосування на ОКІ:

- інтеграція сигнатурного, поведінкового та аномального аналізу;
- пояснюваний ШІ;
- застосування технології Оркестрації безпеки, автоматизації та реагування.

Для систематизації безпеки ОКІ використовуються рамки та стандарти (фреймворки). У роботі [2] через систематичний огляд спеціалізованої літератури було показано, що NIST фреймворк для кібербезпеки (Cybersecurity Framework, CSF), ISO/IEC 27001 та CIS Controls є найпоширенішими фреймворками. Вони задають основу для створення кібербезпеки ОКІ, але мають недоліки:

- нестача секторної адаптивності (енергетика, охорона здоров’я та інші),

- слабка інтеграція ШІ, МН та блокчейну,
- ігнорування людського фактора (помилки, необізнаність, соціальна інженерія та інші).

Пропонований новий фреймворк містить п’ять компонентів [2]:

- оцінка ризиків,
- інцидент-менеджмент,
- контроль доступу,
- розвиток стійкості,
- управління.

Валідовані кейси у сфері охорони здоров’я показали: скорочення часу реагування на 75%, зменшення несанкціонованого доступу на 40%, покращення стійкості на 60%.

Управління, процеси та людський фактор також розглядаються у роботі [3]. Було показано, що 12 із найчастіше описаних інцидентів у OKI пов’язані з людськими помилками:

- слабкі паролі,
- відсутність тренінгів,
- низька обізнаність керівництва.

В межах дослідження [3] для покращення протидії кіберзагрозам було зроблено мапування кіберзагроз на функції NIST CSF. Особливо було підкреслено наступні функції: ID.GV (управління), PR.AT (навчання), DE.CM (моніторинг), RS.RP (планування реагування) та RC.RP (план відновлення).

У підсумку, беручи до уваги наведені вище види кіберзагроз, вектори потенційних атак, засоби захисту, попередження та протидії небезпеці, управління та відновлення OKI, отримуємо наступні практичні рекомендації згідно до [1-4]:

1. Повна інвентаризація IT та OT активів та класифікація даних.
2. Сегментація мереж OT, нульовий рівень довіри доступу (Zero Trust), контроль доступу постачальників.
3. Використання ШІ та МН для виявлення аномалій у трафіку та предикативної аналітики.
4. Застосування блокчейну для безпечних транзакцій у енергомережах.
5. Регулярні аудити та навчання з ліквідації наслідків стихійних лих.
6. Тренінги співробітників та симуляції фішингових атак.

7. Перехід до кванто стійкої криптографії.
8. Забезпечення відповідності NIST, ISO/IEC 27001, IEC 62443, NERC-CIP.

Дослідження показало, що ефективний захист ОКІ можливий лише через комплексний підхід: фреймворки управління ризиками (NIST CSF та розширені моделі), використання ШІ, МН та блокчейну, посилення людського фактору через навчання, а також співпраця держави та приватних структур. Особливий акцент має бути на енергетиці, де поєднання легасі-систем та нових технологій створює критичні ризики.

Список використаної літератури:

1. Ajayi O., Alozie C., Abieba O. Enhancing Cybersecurity in Energy Infrastructure: Strategies for Safeguarding Critical Systems in the Digital Age. Trends in Renewable Energy. 2025. Vol. 11, No. 2. P. 201-212.
2. Alozie C., Chinwe E. Developing a Cybersecurity Framework for Protecting Critical Infrastructure in Organizations. Iconic Research And Engineering Journals. 2025. Vol. 8, No. 7. P. 562-576.
3. Shah S. Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure. Journal of Global Research in Electronics and Communication. 2025. Vol. 2, No. 2. P. 1-6.
4. Aljumaiah O., Jiang W., Addula S., Almaiah M. Analyzing Cybersecurity Risks and Threats in IT Infrastructure based on NIST Framework. Journal of Cyber Security and Risk Auditing. 2025. Vol. 2025, No. 2. P. 12-26.

Ключові слова: кібербезпека, об'єкти критичної інфраструктури (ОКІ), штучний інтелект (ШІ), NIST фреймворк для кібербезпеки.
Keywords: cybersecurity, critical infrastructure facilities (CIF), artificial intelligence (AI), NIST Cybersecurity Framework (NIST CSF).

АНАЛІЗ ІНСТРУМЕНТІВ ТА ПЛАТФОРМ ДЛЯ ТРЕКІНГУ ЕКСПЕРИМЕНТІВ

Савенко Михайло

Національний університет «Одеська юридична академія»,
студент факультету кібербезпеки та інформаційних технологій

У сучасному науковому середовищі, де машинне навчання стає ключовим елементом інноваційних розробок, трекінг експериментів набуває критичного значення як засіб забезпечення відтворюваності, порівнянності та ефективності дослідницьких процесів. Трекінг експериментів охоплює систематичний збір, зберігання та аналіз метаданих, параметрів, метрик продуктивності та артефактів, що виникають під час ітеративних циклів

ЗМІСТ