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)

9. Carlini N., Tramer F., Wallace E. et al. Extracting Training Data from Large Language Models. 30th USENIX Security Symposium (USENIX Security 21). 2021. P. 2633–2650.
10. Yeom S., Giacomelli I., Fredrikson M., Jha S. Privacy risk in machine learning: Analyzing the connection to overfitting. 2018 IEEE 31st Computer Security Foundations Symposium (CSF). 2018. P. 268–282.
11. Hu H., Salcic Z., Sun L. et al. Membership Inference Attacks on Machine Learning: A Survey. ACM Computing Surveys (CSUR). Vol. 54, No. 11s. 2022. P. 1–37.
12. Duan M., Suri A., Mireshghallah N. et al. Do membership inference attacks work on large language models? arXiv preprint arXiv:2402.07841. 2024.
13. Maini P., Jia H., Papernot N., Dziedzic A. LLM Dataset Inference: Did you train on my dataset? arXiv preprint arXiv:2406.06443. 2024
14. Bonawitz K., Ivanov V., Kreuter B. et al. Practical secure aggregation for privacy-preserving machine learning. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017. P. 1175–1191.
15. Yuan W., Yang C., Nguyen Q. V. H. et al. Interaction-level Membership Inference Attack Against Federated Recommender Systems. Proceedings of the Web Conference 2023. 2023. P. 1–10.

**Ключові слова:** Атака на виявлення належності, Великі мовні моделі, приватність, захисні механізми.
**Keywords:** Membership Inference Attack, Large Language Models, Privacy, Defence Mechanisms

## ВИЯВЛЕННЯ НЕТИПОВИХ ПОДІЙ У СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

***Чикунов Павло***

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

***Флюнт Владислав***

*студент Національного університету «Одеська юридична академія»*

Системи відеоспостереження є одним із інструментів моніторингу та забезпечення безпеки у громадських місцях, транспортних вузлах, промислових об’єктах, навчальних закладах і приватних структурах. Зі зростанням кількості камер та обсягу даних постає проблема оперативного аналізу відеопотоків. Оператор фізично не може відстежувати десятки джерел одночасно, тому автоматизовані системи відеоспостереження є критично необхідними.

Використання технологій штучного інтелекту дозволяє автоматизувати процеси виявлення нетипових або аномальних подій, таких як залишені предмети, поява людини у забороненій зоні, натовпова паніка, агресивна поведінка або порушення маршрутів руху. Ці події часто не піддаються формальному опису, що робить традиційні правило-орієнтовані методи

малоефективними. Актуальними є алгоритми машинного навчання, що здатні самостійно моделювати поняття аномальної поведінки без ручного налаштування правил.

Метою роботи є розроблення архітектури та створення прототипу системи автоматизованого виявлення нетипових подій у відеопотоках на основі глибинних нейронних мереж і GPU-прискорення.

Дослідження виявлення аномалій у відео активно розвиваються протягом останнього десятиліття. Автори роботи [1] запропонували використання конволюційного автоенкодера для навчання моделі «нормальної» поведінки. Автори роботи [2] удосконалили підхід через повнозгорткову нейромережу, що працює у реальному часі. У роботі [3] наведено результати реалізації ідеї прогнозування наступного кадра, визначаючи аномалії за відхиленням між очікуваним і фактичним відео. Дослідження [4] присвячено аналізу ефективності кластеризації патернів руху у комбінації з глибинними ознаками, а дослідники [5] запропонували підхід Continual Learning, що враховує зміну середовища.

Окрім академічних рішень, активно розвиваються комерційні системи. Avigilon UMD/UAD від Motorola Solutions впроваджує алгоритми автоматичного виявлення нетипових рухів без попереднього навчання на аномаліях. BriefCam інтегрує інструменти поведінкового аналізу та пошуку об’єктів у VMS Milestone XProtect. Irisity IRIS+ та Oosto Protect поєднують розпізнавання облич із поведінковими моделями. Axis Object Analytics реалізує базові rule-based сценарії на рівні edge-пристроїв.

SWOT-аналіз цих платформ показав, що комерційні рішення забезпечують стабільність і масштабованість, але мають обмежену можливість наукової модифікації алгоритмів; натомість відкриті бібліотеки (зокрема anomalib, OpenVINO, FiftyOne) дозволяють реалізувати академічні експерименти та дослідження на реальних наборах відео.

Для реалізації системи вибрано мову Python завдяки широкому набору бібліотек для комп’ютерного зору та глибинного навчання. До технологічного стеку програмної реалізації входять такі інструменти:

– OpenCV для захоплення та попередня обробка відеопотоку (нормалізація кадрів, фільтрація шумів, виявлення руху);

– PyTorch для побудови, навчання та інференсу нейромережевої моделі автоенкодера;

– TensorFlow для реалізації альтернативних архітектур (3D-CNN, Vision Transformer);

– NumPy / Pandas для обробки та статистичного аналізу наборів даних;

– Matplotlib / Seaborn для візуалізації результатів та графіків втрат;

– CUDA та cuDNN для апаратного прискорення обчислень на GPU.

Запропоновано таку структуру системи:

модуль попередньої обробки відео відповідає за формування потоків і підготовку кадрів для аналізу;

модуль виявлення аномалій реалізує навчання автоенкодера на звичайних даних і порівняння реконструкцій із вхідними кадрами;

модуль візуалізації та збереження результатів забезпечує відображення виявлених аномалій у відеопотоці й запис результатів у базу даних.

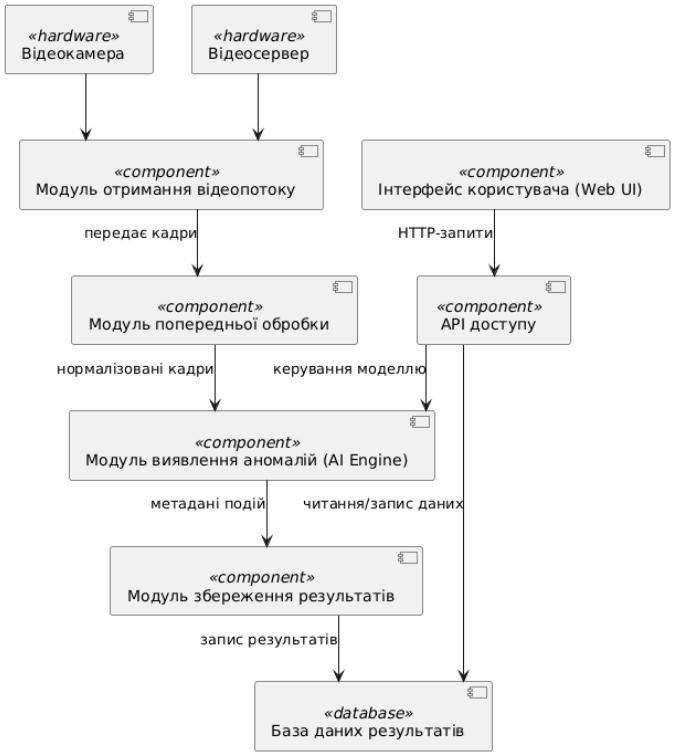


*Рисунок 1 – Компонентна діаграма системи автоматизованого виявлення нетипових подій*

Висновки. У роботі доведено актуальність застосування методів штучного інтелекту для автоматизованого виявлення нетипових подій у відеопотоках. Запропонована архітектура системи демонструє можливість побудови модульного рішення, яке поєднує попередню обробку відео, аналіз поведінкових ознак та візуалізацію виявлених подій. Подальший розвиток дослідження доцільно спрямувати на вдосконалення часових моделей, підвищення стійкості до змін середовища, зменшення кількості хибних спрацьовувань та інтеграцію рішення у більш складні інтелектуальні системи безпеки.

**Список використаної літератури:**

1. Hasan M., Choi J., Neumann J., Roy-Chowdhury A. K., Davis L. S. Learning Temporal Regularity in Video Sequences. IEEE CVPR, 2016.
2. Sabokrou M., Fathy M., Hoseini M., Klette R. Deep-Anomaly: Fully Convolutional Neural Network for Fast Anomaly Detection in Crowded Scenes. CVIU, 2018.
3. Liu W., Luo W., Lian D., Gao S. Future Frame Prediction for Anomaly Detection – A New Baseline. IEEE CVPR, 2018.

4. Ionescu R., Smeureanu S., Alexe B., Popescu M. Detecting Abnormal Events in Video Using Narrowed Normality Clusters. WACV, 2019.
5. Doshi K., Yilmaz Y. Continual Learning for Anomaly Detection in Surveillance Videos. IEEE Trans. Image Processing, 2021.

**Ключові слова**: відеоаналіз, аномальні події, штучний інтелект, нейронні мережі, автоенкодер, відеоспостереження.
**Keywords**: video analytics, anomaly detection, artificial intelligence, neural networks, autoencoder, surveillance.

## АНАЛІЗ ТА РЕДИЗАЙН МОБІЛЬНОГО ЗАСТОСУНКУ НА ОСНОВІ UX-ДОСЛІДЖЕННЯ ТА ПРОТОТИПУВАННЯ

***Селютін В'ячеслав***

*студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»*

Інтенсивний розвиток мобільних технологій та зростання частки користувачів, які взаємодіють із цифровими сервісами переважно через смартфони, актуалізує проблематику підвищення якості інтерфейсів мобільних застосунків. Сучасні дослідження у сфері human–computer interaction [1] показують, що ключовим чинником успішності мобільних продуктів є не лише функціональна повнота, але й оптимізований користувацький досвід, заснований на принципах когнітивної ергономіки, інформаційної архітектури та доступності [2].

Недостатня увага до юзабіліті часто призводить до збільшення когнітивного навантаження, дезорієнтації користувача, втрати мотивації до продовження роботи із застосунком. Актуальність дослідження полягає у необхідності комплексної оцінки інтерфейсу з позиції сучасних стандартів UX/UI, зокрема принципів людиноорієнтованого дизайну, дизайн-систем, моделювання сценаріїв поведінки та валідації користувацьких рішень через прототипування [3].

Мета дослідження полягає у розробленні оновленої концепції інтерфейсу мобільного застосунку шляхом проведення структурованого UX-аналізу, визначення проблем взаємодії та формування дизайн-системи, що забезпечує цілісність та відтворюваність інтерфейсних рішень.

Комплексний аналіз інтерфейсу виявив низку факторів, що потребують удосконалення. Встановлено порушення принципів візуальної ієрархії через нерівномірний розподіл акцентів, конкуренцію елементів за увагу та відсутність чіткої структури між основними та допоміжними діями. Виявлено нелогічну інформаційну архітектуру, що проявляється у дублюванні функціональних модулів у різних частинах інтерфейсу, фрагментованості шляхів взаємодії та недостатній передбачуваності навігації. Зафіксовано недотримання принципів доступності, зокрема низький контраст, малі