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)

6. Forrester Research. The Low-Code Market Could Approach $50 Billion By 2028. March 6, 2024. URL: https://www.forrester.com/blogs/the-low-code-market-could-approach-50-billion-by-2028/.
7. Microsoft Power Platform Blog. Microsoft named a Leader in 2024 Gartner Magic Quadrant for Enterprise Low-Code Application Platforms. July 3, 2025. URL: https://www.microsoft.com/en-us/power-platform/blog/power-apps/microsoft-named-a-leader-in-2024-gartner-magic-quadrant-for-enterprise-low-code-application-latforms/.
8. Gartner. Risk and Opportunity Index: Low-Code Application Platforms. May 24, 2024. URL: https://www.gartner.com/en/documents/5459763.
9. OutSystems. Exploring low-code trends in 2024. April 12, 2024. URL: https://www.outsystems.com/blog/posts/low-code-market/.
10. Kyiv Post. Ukraine's IT Sector Experienced Lowest Staff Outflow Since Russia's Invasion. February 20, 2025. URL: https://www.kyivpost.com/post/47405.

АРХІТЕКТУРНІ ТА АЛГОРИТМІЧНІ ВИКЛИКИ КІБЕРБЕЗПЕКИ У ПРОГНОСТИЧНИХ AR-СИСТЕМАХ НА ОСНОВІ МУЛЬТИМОДАЛЬНОГО АНАЛІЗУ

Чикунов Павло

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

Пучков Владислав

аспірант Національного університету «Одеська юридична академія»

Системи доповненої реальності (AR) переживають стрімку трансформацію, переходячи від інструментів пасивної візуалізації інформації до проактивних інтелектуальних асистентів. Новітнє покоління AR-систем спрямоване на реалізацію прогностичної взаємодії – здатності системи передбачати наміри та наступні дії користувача для надання випереджувальної допомоги. Фундаментом для такої функціональності є мультимодальний аналіз поведінки, що передбачає одночасний збір, синхронізацію та інтерпретацію даних з геть різнорідних джерел: відстеження погляду (eye-tracking), аналіз жестів, розпізнавання мови, моніторинг біометричних показників (наприклад, ЕЕГ або варіабельності серцевого ритму) та просторове позиціонування [1].

Такий глибинний аналіз поведінки, хоч і відкриває значні перспективи для підвищення ефективності взаємодії «людина-машина», водночас генерує безпрецедентні виклики у сфері кібербезпеки та приватності [2]. Дані, що збираються, є не просто персональними; вони є інтимно-персональними, оскільки дозволяють робити висновки про когнітивний стан, рівень стресу, наміри та навіть стан здоров’я користувача. Компрометація таких систем може призвести не лише до витоку даних, але й до маніпуляції поведінкою користувача через нав’язування хибних прогностичних підказок.

Метою даної роботи є системний аналіз загроз кібербезпеці, притаманних архітектурі прогностичних AR-систем, та ідентифікація вразливостей на алгоритмічному рівні, пов'язаних із застосуванням моделей машинного навчання (МН) для мультимодального аналізу. Дослідження фокусується на формулюванні вимог до безпечної архітектури, що відповідає принципам «безпека та приватність за проектуванням» (Security and Privacy by Design).

Побудова життєздатної прогностичної AR-системи вимагає складної, багатошарової архітектури, кожен компонент якої має унікальні вектори атак. Типова архітектура включає такі шари.

Шар сенсорів (Sensor Layer): набір апаратних засобів (камери, мікрофони, IMU, окулографи, біосенсори), відповідальних за збір необроблених мультимодальних даних.

Шар обробки та злиття даних (Data Fusion Layer): програмний модуль, що здійснює первинну обробку, очищення, синхронізацію та злиття даних з різних джерел у єдиний вектор ознак.

Прогностичний рушій (Prognostic Engine): ядро системи, зазвичай реалізоване на базі моделей МН (наприклад, рекурентних або трансформаторних нейронних мереж), яке аналізує вектор ознак та генерує гіпотези щодо майбутніх дій користувача.

Шар візуалізації та взаємодії (Rendering & Interaction Layer): компонент, що відповідає за відображення прогностичної інформації у полі зору користувача та обробку його реакцій.

З точки зору кібербезпеки, критичні вразливості виникають на стиках цих компонентів, особливо у контексті вибору обчислювальної парадигми (on-device, edge, or cloud computing) [4].

Вразливості передачі даних. Найбільш очевидною загрозою є перехоплення необроблених сенсорних даних під час їх передачі від AR-пристрою (окулярів) до обчислювального модуля (смартфон або хмарний сервер). Потоки відео, аудіо та біометричних даних, якщо вони не захищені надійними протоколами шифрування (наприклад, TLS 1.3) та взаємною автентифікацією пристроїв, можуть бути перехоплені (атака «людина посередині»), надаючи зловмиснику повний доступ до приватної інформації користувача [6].

Безпека обчислень (On-Device vs. Cloud). Обробка даних виключно на пристрої (on-device) є найбільш бажаною з точки зору приватності, оскільки чутливі дані ніколи не залишають контрольованого користувачем середовища. Для цього використовуються високоефективні мови програмування (наприклад, C++ або Swift) та спеціалізовані бібліотеки (ARKit, ARCore, OpenCV). Однак потужність мобільних пристроїв обмежена, і складні прогностичні моделі МН часто вимагають ресурсів хмарних платформ.

Гібридна (edge-cloud) архітектура, де первинна обробка відбувається локально, а складний аналіз – у хмарі (з використанням стеку Python, TensorFlow/PyTorch), створює додаткову поверхню атаки на хмарне сховище та API, через які відбувається взаємодія [3].

Вразливості сховища даних. Мультимодальні дані та навчені моделі МН повинні безпечно зберігатися. Неналежне шифрування даних у стані спокою (at-rest) або вразливості у системі керування базами даних можуть призвести до масових витоків.

Прогностичний рушій, що є серцем системи, сам по собі є мішенню для атак, специфічних для машинного навчання.

Атаки змагальності – це клас атак, де зловмисник цілеспрямовано створює вхідні дані (наприклад, специфічний жест, візуальний артефакт або аудіошум), які є непомітними для людини, але здатні кардинально змінити висновок моделі МН [3]. В контексті прогностичної AR-системи, зловмисник може згенерувати такий «змагальний» жест, щоб змусити систему видати хибний прогноз – наприклад, приховати важливе сповіщення про небезпеку або, навпаки, ініціювати неправдиву тривогу. Це перетворює AR-систему з помічника на вектор дезінформації або маніпуляції [5].

Атаки на приватність моделі. Навіть якщо самі дані захищені, зловмисник може спробувати відновити конфіденційну інформацію, аналізуючи лише вихідні дані (прогнози) моделі. Наприклад, атаки на виведення членства (membership inference) дозволяють визначити, чи були дані конкретної людини використані під час навчання моделі. Це особливо небезпечно при аналізі медичних або поведінкових патернів.

Соціальна інженерія на основі штучного інтелекту. Комбінація мультимодального аналізу та великих мовних моделей відкриває шлях до гіперефективної соціальної інженерії. Система, що розуміє емоційний стан користувача (через аналіз голосу та міміки) та його наміри (через аналіз погляду), може бути використана для генерації надзвичайно переконливих фішингових або маніпулятивних повідомлень у реальному часі [2].

Ефективний захист прогностичних AR-систем вимагає комплексного підходу, що інтегрує безпеку на кожному етапі життєвого циклу розробки програмного забезпечення.

Принцип «Приватність за проектуванням» [4] передбачає, що механізми захисту приватності інтегруються в архітектуру системи з самого початку, а не додаються як зовнішній шар.

Це включає:

мінімізацію даних – збір лише того обсягу даних, який є абсолютно необхідним для функціонування прогнозу;

анонімізацію та псевдонімізацію – тобто усі дані, що надсилаються у хмару, мають бути позбавлені прямих ідентифікаторів;

федеративне навчання – метод навчання глобальної моделі МН на децентралізованих даних (на пристроях користувачів) без передачі самих даних на сервер;

диференційну приватність – додавання статистичного «шуму» до даних або результатів запитів до моделі, що унеможливлює точне відновлення інформації про окремого користувача, зберігаючи при цьому загальну корисність моделі.

Захист на алгоритмічному рівні. Для протидії атакам змагальності необхідно впроваджувати техніки змагального навчання, коли модель МН під час навчання цілеспрямовано «годують» змагальними прикладами, роблячи її більш стійкою до таких маніпуляцій [3]. Також необхідна розробка систем моніторингу в реальному часі, які б виявляли статистичні аномалії у вхідних даних, що можуть свідчити про спробу атаки.

Контроль з боку користувача. Ключовим аспектом, що торкається соціальних та управлінських аспектів кібербезпеки, є надання користувачеві прозорого та гранулярного контролю над тим, які мультимодальні дані збираються, коли і з якою метою.

Висновки. Прогностичні AR-системи на основі мультимодального аналізу поведінки є технологією з подвійним потенціалом: вони можуть стати потужними когнітивними помічниками або ж інструментами безпрецедентного стеження та маніпуляції. Забезпечення кібербезпеки таких систем виходить за рамки традиційного захисту мереж та даних; воно вимагає розробки нових архітектурних рішень, орієнтованих на приватність (як-от федеративне навчання), та створення нового покоління алгоритмів МН, стійких до цілеспрямованих атак. Подальші дослідження у цій галузі мають бути зосереджені на створенні комплексних фреймворків безпеки, що збалансовують високу точність прогностичної взаємодії з гарантіями конфіденційності користувача.

Список використаної літератури:

1. Popa, D., Augmented Reality and Cyber Challenges Exploration. Proceedings of the 2016 8th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2016.
2. Chen, L., On the Feasibility of Using MultiModal LLMs to Execute AR Social Engineering Attacks, 2024.
3. Ghafoor, A., Adversarial Attack Detection in AI-Based AR Systems. International Journal of Computer Science and Network Security, 25(1), pp. 120-135, 2025.
4. Roesner, F., Kohno, T., & Molnar, D. Security and Privacy for Augmented Reality Systems. Communications of the ACM (CACM), 57(4), pp. 88-96, 2014.
5. Lebeck, K. Towards Security and Privacy for Multi-User Augmented Reality: Foundations with End Users. Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), pp. 53-69, 2018.

6. Al-Ghaili, M. Cybersecurity in the AI-Based Metaverse: A Survey. Applied Sciences, 2022.

Ключові слова: доповнена реальність (AR), прогностична взаємодія, мультимодальний аналіз, архітектура безпеки, кібербезпека, машинне навчання, конфіденційність даних, атаки змагальності, приватність за проектуванням.

Keywords: augmented reality (AR), predictive interaction, multimodal analysis, security architecture, cybersecurity, machine learning, data privacy, adversarial attacks, privacy by design.

АНАЛІЗ СУЧАСНИХ ІГРОВИХ РУШІЇВ GAMEDEV

Кутас Олександр

студент факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Упродовж останніх десятиліть сфера розробки відеоігор стрімко розвивається і стала одним із найдинамічніших напрямів інформаційних технологій. Важливою складовою цього процесу є створення або раціональний вибір рушія, що забезпечує технічну основу для побудови інтерактивного ігрового простору. Саме від потужності, гнучкості та оптимізації рушія значною мірою залежить якість кінцевого продукту, зручність розробки та можливість масштабування проєкту.

Раніше більшість компаній, які працювали над великобюджетними проєктами (AAA-сегментом), розробляли власні рушії, адаптовані під специфічні потреби ігор та внутрішні інструменти студій. Такий підхід забезпечував повний контроль над технічними аспектами, але вимагав значних ресурсів і часу. Натомість сучасна тенденція демонструє перехід до використання вже наявних універсальних рушіїв, як-от Unreal Engine, Unity чи Godot, які надають готові інструменти для графіки, фізики, штучного інтелекту та мережевої взаємодії. Це дозволяє розробникам зосередитися на творчій складовій ігрового процесу і не витрачати ресурси на створення базової технічної інфраструктури.

Ігровий рушій Unreal Engine має унікальні графічні можливості, які задають тенденції для всієї індустрії GameDev. Завдяки використанню низки інноваційних технологій рендерингу рушій забезпечує фотореалістичну якість зображення, яка раніше була доступна лише у високобюджетних кінематографічних середовищах. Так, технологія Nanite відповідає за віртуалізовану геометрію, що надає змогу працювати з моделями, які містять численні полігони, без втрати продуктивності [2]. Це відкриває перед розробниками нові можливості у створенні високодеталізованих світів, де навіть найдрібніші елементи залишаються чіткими та реалістичними. Система Lumen реалізує в Unreal Engine 5 глобальне освітлення та відбиття в реальному часі [1]. Вона дозволяє реалізувати максимально природне освітлення сцени без потреб тривалої попереднього оброблення або