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)

САМОВДОСКОНАЛЮВАНІ ВІРУСИ ШТУЧНОГО ІНТЕЛЕКТУ: РИЗИКИ, ВИЯВЛЕННЯ ТА МЕТОДИ ПРОТИДІЇ

Лавренко Дмитро

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

Штучний інтелект (ШІ) перетворився на подвійний інструмент сучасної кіберзлочинності, де генеративні моделі застосовуються для створення персоналізованих фішингових кампаній, реалістичних deepfake-медіа та імітації людської поведінки з метою обходу систем безпеки. Europol у звіті 2023 року фіксує стрімке зростання злочинів, де ШІ відіграє ключову роль у фальсифікації цифрових доказів, автоматизованому хакінгу та підтримці багатовекторних атак [1]. Це формує технологічне підґрунтя для появи принципово нового класу загроз – самовдосконалюваних шкідливих агентів, здатних адаптувати власну поведінку без прямого втручання оператора.

Під самовдосконалюваними вірусами ШІ розуміють шкідливі програмні агенти з механізмами машинного навчання та адаптації, що дозволяють змінювати стратегії дій, генерувати нові інструкції або модифікувати структуру коду в процесі виконання. Розвиток трансформерних архітектур з механізмами self-attention [2], методів навчання з підкріпленням та еволюційних алгоритмів створює технічні передумови для таких систем. Хоча масових випадків повністю автономних самовдосконалюваних вірусів у відкритому середовищі ще не зафіксовано, задокументовані прототипи демонструють життєздатність цієї парадигми. Зокрема, шкідлива програма PromptLock, проаналізована ESET, застосовувала локально розгорнуту мовну модель для генерації payload-ів у реальному часі, адаптуючи команди до специфіки цільової системи без попередньо захардкоженої логіки атаки [3]. Google Threat Intelligence Group документує зростання кампаній із застосуванням генеративних моделей для варіації шкідливого коду та обходу сигнатурних детекторів [4].

Механізми самовдосконалення реалізуються через трансформерні архітектури, які аналізують контекст і генерують контекстуально оптимізовані інструкції, через навчання з підкріпленням, де дії з високою «винагородою» (успішна ексфільтрація, обхід захисту) підвищують ймовірність повторення подібних стратегій, або через еволюційні алгоритми з мутацією та селекцією варіантів коду на основі метрик ефективності. Найнебезпечнішим є сценарій онлайн-навчання у продуктивному середовищі, коли модель змінює параметри під час виконання, чим ускладнює відтворення її поведінки. Реалізація таких агентів вимагає вибору між локальним розгортанням моделей, що підвищує автономність але обмежене ресурсами, та

використанням віддалених C2-сервісів із потужнішими моделями, що створює виявлювані мережеві індикатори.

Динамічний характер поведінки самовдосконалюваних агентів робить традиційні сигнатурні системи детекції неефективними. Протидія має базуватися на поведінковому аналізі з моделюванням нормальної активності системи та виявленням аномалій у багатовимірному просторі метрик (CPU/IO навантаження, мережеві патерни, частота викликів ML-моделей). Моніторинг інференсу через аналіз нетипового використання ресурсів для inference та кореляція подій у часі можуть виявляти сліди діяльності агента. Sandbox-аналітика має ускладнитись включенням еволюційного тестування: симуляцією різних конфігурацій середовища, імітацією захисних реакцій та відслідковуванням мутацій у стратегіях поведінки.

Наслідки виникнення самовдосконалюваних вірусів є багатовимірними. Технічно це означає зниження ефективності класичних методів виявлення та збільшення часу невиявленої компрометації через варіативність коду. Інфраструктурно підвищується вразливість промислових систем SCADA, енергомереж та транспорту, де адаптивний агент може специфікувати атаки під характеристики обладнання. Економічно прогнозується суттєве здешевлення складних багатоетапних атак через автоматизацію та зростання витрат на постійний захист. Стратегічно виникає потенціал автономної кіберзброї з низьким рівнем людського контролю, що може призводити до незворотних наслідків у критичних сценаріях.

Ефективна протидія вимагає поєднання технічних, організаційних та нормативних заходів. Технічні інструменти включають розширений моніторинг інференсу моделей, виявлення отруєння даних (data poisoning) та контроль доступу до моделей і тренувальних наборів. Організаційні заходи охоплюють політики обмеження запуску неверифікованих моделей у продуктивних середовищах, впровадження принципів Zero Trust та регулярний аудит ML-інфраструктури через SIEM-рішення для кореляції подій. На нормативному рівні необхідні правила автономності моделей, вимоги до сертифікації для критичних застосувань та механізми міжнародного обміну даними про інциденти.

Самовдосконалювані віруси ШІ є реальною науково-технічною загрозою, технічні передумови якої вже створені. Протидія вимагає системної трансформації підходів до кіберзахисту через перехід від сигнатурних методів до поведінкової детекції, інструментування інференсу, захист тренувальних даних та введення нормативних обмежень на автономність моделей. Без цього поширення самонавчальних шкідливих агентів може кардинально змінити ландшафт кіберзлочинності та посилити ризики для критичної інфраструктури й суспільної безпеки.

Список використаних джерел:

1. AI bias in law enforcement. *Europol*. 27.07.2025. URL: https://www.europol.europa.eu/publications-events/publications/ai-bias-in-law-enforcement
2. Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A. N., Kaiser Ł., Polosukhin I. Attention is all you need. *Advances in Neural Information Processing Systems*. 2017. Vol. 30. P. 5998–6008. URL: https://proceedings.neurips.cc/paper/2017/hash/3f5ee243547dee91fbd053c1c4a845aa-Abstract.html
3. ESET discovers PromptLock, the first AI-powered ransomware. *ESET Research.* 27.08.2025. URL: https://www.eset.com/us/about/newsroom/research/eset-discovers-promptlock-the-first-ai-powered-ransomware .
4. GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools. *Google Threat Intelligence Group.* 6.11.2025. URL: https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools/

Ключові слова: самовдосконалювані віруси, штучний інтелект, ШІ, трансформерні архітектури.
Keywords: self-improving viruses, artificial intelligence, AI, transformative architectures.

Науковий керівник: к.т.н., доцент Трофименко О.Г.

МАШИННЕ НАВЧАННЯ У ПЕРЕВІРЦІ ПРОГРАМНИХ КОДІВ: ЕФЕКТИВНІСТЬ АЛГОРИТМУ RANDOM FOREST

Григор'єв Олександр

студент 2 курсу магістратури факультету кібербезпеки та інформаційних технологій Національний університет «Одеська юридична академія»

Перевірка лабораторних робіт з програмування є складним завданням для викладачів, оскільки вимагає великих зусиль як у плані часу, так і когнітивних витрат. Використання методів машинного навчання (МН) дозволяє створити інтелектуальну систему, яка може автоматизувати аналіз програмного коду, виявляти помилки та оцінювати стиль програмування. Для цього рекомендується використовувати алгоритм Random Forest, який поєднує високу точність класифікації з прийнятною швидкістю роботи, забезпечує можливість інтерпретації результатів та виявляє високу стійкість до шумових даних.

Алгоритм Random Forest – це метод машинного навчання, який використовує незалежні дерева рішень, побудовані на основі навчальної вибірки з відомими класами. Кожне дерево навчається на випадковій підмножині даних, враховуючи лише деякі ознаки при формуванні вузлів. Узагальнене рішення моделі визначається шляхом голосування дерев для класифікації або усереднення їхніх прогнозів для регресії [1].

ЗМІСТ