УДК 004.056

Воєвода А.В.
Кирилащук Т.Г.

СТРАТЕГІЧНІ НАПРЯМИ РОЗВИТКУ КІБЕРБЕЗПЕКИ У 2026 РОЦІ: ВИКЛИКИ ТА ТЕХНОЛОГІЧНІ ТРЕНДИ

Вінницький національний технічний університет

Анотація
У тезах розглянуто ключові аспекти трансформації ландшафту кіберзагроз у 2026 році. Проаналізовано вплив автономного штучного інтелекту на методи ведення кібератак та стратегії захисту. Окреслено роль цифрової ідентифікації як нового периметра безпеки в умовах глобальної цифровізації.
Ключові слова: кібербезпека, штучний інтелект, дипфейки, цифрова ідентичність, Zero Trust, стійкість інфраструктури.

Abstract
The abstracts examine the key aspects of the cyber threat landscape transformation in 2026. The impact of autonomous artificial intelligence on cyberattack methods and defense strategies is analyzed. The role of digital identity as a new security perimeter in the context of global digitalization is outlined.
Keywords: cybersecurity, artificial intelligence, deepfakes, digital identity, Zero Trust, infrastructure resilience.

Сучасний стан розвитку інформаційних технологій у 2026 році характеризується глибокою інтеграцією агентного штучного інтелекту (Agentic AI) в усі рівні цифрової інфраструктури, що трансформує класичну модель кіберзагроз у динамічну екосистему автономних атак. На відміну від попередніх ітерацій генеративного ШІ, сучасні агентні системи здатні до самостійного цілепокладання, аналізу контексту та виконання складних послідовностей операцій без участі людини. Це створює безпрецедентні виклики для систем інформаційної безпеки, оскільки зловмисники використовують самонавчальні моделі для безперервного сканування глобальних мереж на предмет вразливостей у режимі реального часу. Такі автономні агенти здатні проводити високоточну розвідку на основі відкритих джерел (OSINT), миттєво корелювати дані з різних витоків та автоматично генерувати експлойти під виявлені специфічні вразливості нульового дня (0−day). Особливо критичним стає використання «поліморфного» ШІ-інструментарію, який модифікує свій код під час виконання атаки, що робить традиційні системи детектування (EDR/XDR), орієнтовані на статичні сигнатури, практично неефективними.

Трансформація векторів атак у 2026 році також демонструє критичне зростання загрози з боку дипфейків другого покоління (Deepfakes 2.0). Використання генеративно-змагальних мереж (GAN) та дифузійних моделей дозволило зловмисникам створювати гіперреалістичні підробки аудіо- та відеоданих, які в реальному часі обходять системи біометричної автентифікації та перевірки на «живість» (Liveness Detection). Це ставить під удар не лише фінансовий сектор, а й критичні державні сервіси, де віддалена ідентифікація є стандартом. Поряд із цим, спостерігається остаточне зникнення класичного мережевого периметра. У сучасних гібридних

середовищах фокус безпеки змістився на захист цифрової ідентичності (Digital Identity). Кількість машинних ідентичностей (IoT-пристроїв, хмарних сервісів, програмних ботів) у 2026 році перевищила кількість людських акаунтів у десятки разів. Більшість цих сутностей мають надлишкові привілеї, що робить їх ідеальними точками входу для атак на ланцюги постачання (Supply Chain attacks). Компрометація одного автоматизованого вузла може призвести до каскадного обвалу всієї інфраструктури через складну систему довірених зв'язків усередині хмарних екосистем.

Відповіддю на ці виклики стала еволюція концепції нульової довіри до стандарту Zero Trust 2.0. Ця модель передбачає впровадження систем безперервного адаптивного управління впливом загроз (CTEM), де кожна транзакція та запит на доступ оцінюються контекстуальним ШІ-модулем у реальному часі. Оцінка ризику тепер базується на сукупності факторів: від геопозиціонування та стану безпеки кінцевого пристрою до аналізу поведінкових патернів користувача. Будь-яка аномалія в діях адміністратора призводить до миттєвої ізоляції сегмента мережі за допомогою технологій мікросегментації. Окремим стратегічним напрямом є підготовка до постквантової епохи. З огляду на прогрес у створенні квантових обчислювачів, здатних зламувати алгоритми RSA та ECC, у 2026 році розпочався масовий перехід на постквантову криптографію (PQC). Впровадження алгоритмів на основі решіток (Lattice-based cryptography) стає критичним для захисту даних із тривалим терміном зберігання, зокрема державних реєстрів та банківських транзакцій.

Крім того, стратегія кібербезпеки 2026 року акцентує увагу на забезпеченні кіберстійкості (Cyber Resilience) критичної інфраструктури, зокрема енергетичних систем та космічних засобів зв'язку. В умовах геополітичної нестабільності захист підводних магістралей передачі даних та супутникових угруповань став пріоритетом національної безпеки. Сучасні системи захисту використовують SOAR-платформи (Security Orchestration, Automation, and Response) для автоматичного реагування на інциденти, що дозволяє локалізувати загрози за лічені мілісекунди. Таким чином, майбутнє кіберзахисту полягає в інтегрованому підході, який поєднує автономні системи реагування на базі ШІ, постквантову стійкість та тотальне управління цифровою ідентичністю в межах адаптивної моделі нульової довіри. Це єдиний шлях до збереження цифрового суверенітету та стабільності в умовах агресивного техногенного середовища.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Global Cybersecurity Outlook 2026 : Insight Report / World Economic Forum. Geneva : WEF, 2026. 42 p. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2026/ (дата звернення: 15.02.2026).
2. The 6 Cybersecurity Trends That Will Shape 2026 / ISACA. 2026. URL: https://www.isaca.org/resources/news-and-trends/industry-news/2026/the-6-cybersecurity-trends-that-will-shape-2026 (дата звернення: 15.02.2026).
3. Gartner Top Strategic Technology Trends for 2026 : Research Note. Stamford : Gartner, 2025. 18 p.
4. Cybersecurity in the Era of Agentic AI / SANS Institute. 2026. URL: https://www.sans.org/white-papers/agentic-ai-security/ (дата звернення: 20.02.2026).
5. Post-Quantum Cryptography: Readiness and Challenges / NIST Special Publication. 2025. № 1800. 65 p.
6. Дипфейки як загроза національній безпеці: методи протидії у 2026 році / Збірник наукових праць ВНТУ. Вінниця, 2026. С. 112–118.
7. Zero Trust Architecture 2.0: Implementation in Critical Infrastructure / IEEE Security & Privacy. 2026. Vol. 24, No. 1. P. 45–53.
8. Identity as the New Perimeter: Managing Non-Human Identities / Cybersecurity Insiders Report. 2026. URL: https://www.cybersecurity-insiders.com/report2026 (дата звернення: 01.03.2026).
9. Штучний інтелект у кібербезпеці: від автоматизації до автономних систем захисту / Матеріали конференції «IT-безпека». Київ, 2025. С. 89–94.
10. Supply Chain Security in 2026: Lessons Learned from Global Incidents / ENISA Annual Report. 2026. 58 p.

Воєвода Аліна Віталіївна – студентка групи 1БКС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail:alinavoievoda77@gmail.com

Науковий керівник : **Кирилащук Тетяна Геннадіївна** – асистент кафедри інформації захисту, Вінницький національний технічний університет, Вінниця. kgt0998@gmail.com