Ілюзія безпечності: сучасні виклики та нові підходи в корпоративній кібербезпеці

https://doi.org/10.31713/MCIT.2025.058

Володимир Герус
Національний університет водного
господарства та природокористування
Рівне, Україна
v.a.gerus@nuwm.edu.ua

Анотація **– У статті аналізується феномен «ілюзії захищеності», що виникає унаслідок повільного деградування традиційних засобів інформаційної безпеки, а також виклики, породжені стрімкою еволюцією кіберзагроз та інтеграцією AI / Zero Trust / DevSecOps у безпекові стратегії. Запропоновано практичні підходи та рекомендації для переходу до поведінково-орієнтованих систем, автоматизації та контекстного аналізу користувачів і систем.**

Ключові слова – кібербезпека, ілюзія захищеності, поведінковий аналіз, автоматизація, Zero Trust, DevSecOps

I. Актуальність і постановка проблеми

У новому цифровому світі, корпоративна кібербезпека більше не є прерогативою лише відділу ІБ, вона інтегрується у всі бізнес-процеси. Однак багато організацій досі покладаються на застарілі підходи, що працювали в епоху шаблонних атак. Основна загроза полягає в тому, що ці системи не «ламаються» одномоментно- вони деградують поступово, створюючи хибне відчуття безпеки. У критичний момент вони просто не зреагують, і наслідки виявляться фатальними.

II. Швидкість еволюції загроз та вимога до оперативності

Сучасні загрози розвиваються з експоненціальною швидкістю: час від публікації інформації про вразливість до появи її експлуатації становить іноді лічені години. Щоб адекватно реагувати, потрібна прозора інвентаризація активів, прозора система управління вразливостями (vulnerability management) і патч-менеджмент. У протилежному випадку класичні вразливості стануть легким полем для атак.

Традиційні системи (антивіруси на основі сигнатур, IDS/IPS, SIEM зі статичними правилами) добре працювали під час масових шаблонних атак. Проте нові атаки є поліформні (fileless), атаки з використанням легітимних інструментів (Living off the Land) залишаються невидимими. Сигнатурні та прості правила недостатні для розпізнавання невеликих відхилень. Необхідно перейти до моделей поведінкового аналізу та побудови цифрових профілів систем і користувачів, які дозволяють фіксувати аномалії до появи класичних атак.

Класичні DLP-системи створювались як універсальні «все в одному», але їх універсальність стала слабкістю: для конкретних загроз з'явилися більш вузькі та ефективні рішення. Аналіз тексту за тематичними словниками також має обмеження:

- Надто вузькі- упускають важливі повідомлення
- Надто широкі- породжують помилкові спрацювання.

Лише аналіз за змістом і контекстом із використанням великих мовних моделей дозволяє підвищити точність виявлення ризикової поведінки.

У 2025 році ручне управління патчами, аудитом конфігурацій чи управлінням доступом- це спроба «наздогнати ракету пішки». Такі підходи вже не просто неефективні- вони небезпечні. Автоматизація має стати фундаментом: інтеграція у CI/CD, політики Zero Trust Network Access (ZTNA), взаємодія з IAM/PAM. Людина лишається залученою лише для винятків і перевірки складних випадків.

Навіть сучасні моделі можуть швидко застаріти. Наприклад, push-MFA вже піддається атакам MFA fatigue, коли користувач, зазнавши численних push-запитів, випадково підтверджує їх. Моделі «однократної перевірки» (after-login trust) втрачають актуальність, після аутентифікації потрібно постійне оцінювання поведінки.

Інтеграція AI у безпеку відкриває нові горизонти, але й породжує ризики: передача конфіденційних даних у хмарні сервіси без анонімізації, надмірна довіра до висновків моделей, відсутність політик використання. Zero Trust сприймають неправильно. Це не продукт, це ціла методологія та культура. Основною помилкою є відсутність інвентаризації активів, ігнорування постійного моніторингу. DevSecOps теж часто реалізується формально без інструментів, без змін у культурі, що в свою чергу веде до ігнорування або обхідного шляху.

Особливостями Українських умов залишається проблема відмови від іноземного ПЗ та переходу до

вітчизняних систем. Деякі частини інфраструктури продовжують працювати на застарілому або неліцензійному ПЗ. У таких випадках необхідно не просто замінити, а створити додаткові шари захисту навколо legacy-систем, із ізоляцією й посиленим моніторингом

III. Рекомендації для практики

• Відмовитися від:

- Сигнатурних антивірусів як єдиного засобу
- Ручного управління патчингом / аудитом у великих інфраструктурах
- MFA через SMS чи push без контекстного аналізу
- Формальних щорічних тренінгів
- Excel-таблиць для управління доступом
- Моделі «однократної довіри»

• Впровадити насамперед:

- Системи поведінкового аналізу з машинним навчанням
- Автоматизацію критичних процесів безпеки
- Неперервний моніторинг і кореляцію подій у реальному часі
- Програми мікронавчання та практичні симуляції
- Архітектурні елементи Zero Trust із постійною верифікацією
- Повне впровадження DevSecOps з включенням безпеки на ранніх етапах.

IV. Висновок

У 2025 році відмова від застарілих підходів в ІБ це не теоретичний вибір, а стратегічний імператив виживання. Організації, що оперативно адаптують культуру, процеси й інструментарій під нові загрози, отримають конкурентну перевагу. Решта ризикують стати легкою мішенню у динамічному світі кіберзлочинності

Література

[1] S. Rose, O. Borchert, S. Mitchell, S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, 2020.

[2] Z. Ge, T. Li, Q. Zhu, “Scenario-agnostic zero-trust defense with explainable threshold policy: a meta-learning approach,” arXiv preprint arXiv:2303.03349, 2023.

[3] G. Freed, M. Jackson, “Zero trust architecture in AI-driven cybersecurity: a machine learning perspective,” ResearchGate preprint, 2025.

[4] L. Prates et al., “DevSecOps practices and tools,” International Journal of Secure Software Engineering, vol. X, 2025.

[5] X. Zhao et al., “Identifying the primary dimensions of DevSecOps: a multi-method study,” ScienceDirect, 2024.

[6] F. Binbeshr, M. Imam, “Comparative analysis of AI-driven security approaches in DevSecOps: challenges, solutions and future directions,” 2025 (unpublished).

[7] S. Ahmadi, “Autonomous identity-based threat segmentation in zero trust architectures,” arXiv preprint arXiv:2501.06281, 2025.

[8] H. Khan et al., “AI-driven cybersecurity framework for software,” PMC Article, 2025.

[9] S. Kommera, “Enhancing zero trust architecture with AI-driven threat intelligence in cloud environments,” International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2025.

[10] A. Alghawli et al., “Resilient cloud cluster with DevSecOps security model,” ScienceDirect, 2024..