УДК 316.776:004.58

Кібербезпека: сучасні виклики та напрями розвитку

Тимур Бражник[0009-0003-9726-6998]
Андрій Аносов[0000-0002-2973-6033]

Київський столичний університет імені Бориса Грінченка, Україна

Анотація. У тезах розглядаються сучасні підходи до забезпечення кібербезпеки, зокрема методи виявлення та запобігання кібератакам у корпоративних мережах. Проаналізовано концепцію Zero Trust, машинне навчання для виявлення аномалій та криптографічні засоби захисту даних.
Ключові слова: кібербезпека, інформаційна безпека, кібератаки, Zero Trust.

Cybersecurity: Modern Challenges and Directions of Development

Timur Brazhnyk[0009-0003-9726-6998]
Andrii Anosov[0000-0002-2973-6033]

Borys Grinchenko Kyiv Metropolitan University, Ukraine

Abstract. The paper considers modern approaches to ensuring cybersecurity, in particular methods for detecting and preventing cyberattacks in corporate networks. The concept of Zero Trust, machine learning for detecting anomalies, and cryptographic means of data protection are analyzed.
Keywords: cybersecurity, information security, cyberattacks, Zero Trust.

Вступ

У сучасному світі інформація стала одним із найцінніших ресурсів, а її захист — стратегічним завданням для держав, бізнесу та окремих громадян. З розвитком цифрових технологій, хмарних обчислень, інтернету речей (IoT), 5G-мереж та штучного інтелекту відбувається глобальна цифровізація усіх сфер життя. Проте паралельно з цим зростає кількість і складність кіберзагроз, що створює новий рівень ризиків для національної безпеки, економіки та приватного сектору.

За даними звіту ENISA Threat Landscape 2024, кількість зареєстрованих кібератак у Європі зросла на понад 35 % порівняно з попереднім роком. Серед основних тенденцій — поширення атак типу ransomware, що блокують роботу організацій до сплати викупу, та supply chain attacks, які спрямовані на ураження через довірених постачальників.

Об’єктом дослідження є процеси забезпечення кібербезпеки в інформаційно-комунікаційних системах.

Предметом дослідження — методи, моделі та засоби захисту інформації в умовах зростання складності кіберзагроз.

Метою роботи є аналіз сучасного стану кібербезпеки, визначення основних викликів і тенденцій розвитку, а також вивчення інноваційних технологій, які можуть підвищити рівень захисту в цифровому середовищі.

Таким чином, тема кібербезпеки є однією з найважливіших у сучасному цифровому суспільстві, оскільки без належного захисту інформаційних систем неможливо

забезпечити стабільність держави, довіру громадян до електронних сервісів і безпечне функціонування цифрової економіки.

Методи та моделі

У сучасних інформаційно-комунікаційних системах забезпечення кібербезпеки базується на поєднанні організаційних, правових та технічних методів захисту. Розробка ефективних моделей кіберзахисту потребує системного підходу, який враховує архітектуру мережі, рівні доступу, властивості даних та поведінку користувачів.

Традиційна модель безпеки інформаційних систем ґрунтується на принципах CIA-тріади (Confidentiality – Integrity – Availability), що визначає три основні цілі кіберзахисту:

$$S = f(C,I,A),$$

де S – безпека, C — конфіденційність, I — цілісність, A — доступність даних.

Для досягнення цих цілей застосовуються такі методи:

- криптографічний захист — шифрування, електронний цифровий підпис, хешування;
- аутентифікація та авторизація користувачів;
- контроль доступу (дискреційний, мандатний, рольовий);
- аналіз аномалій і вторгнень (IDS/IPS-системи);
- сегментація мережі та брандмауери.

Результати

У результаті проведеного дослідження було проаналізовано ефективність різних підходів до забезпечення кібербезпеки в умовах зростання кількості та складності кіберзагроз. Отримані результати підтверджують необхідність поєднання класичних методів захисту (криптографія, контроль доступу, антивірусний аналіз) із сучасними інтелектуальними системами, які використовують машинне навчання, поведінкову аналітику та принципи Zero Trust.

Рисунок 1 ілюструє спрощену схему взаємодії елементів архітектури Zero Trust, у якій кожен запит доступу проходить багаторівневу перевірку:

- Policy Engine (PE): приймає рішення, надати доступ чи ні, на основі політики, а також вхідних даних із систем CDM та від служб, що надають аналітичну інформацію про загрози;
- Policy Administrator (PA): відповідає за встановлення чи припинення зв'язку на основі рішень PE;
- Policy Enforcement Point (PEP): відповідає за включення, моніторинг та розрив з'єднань.

Ряд ресурсів надає вхідні дані, необхідні PE для ухвалення рішення про доступ.

Система безперервної діагностики та моніторингу (Continuous Diagnostics and Mitigation, CDM) інформує PE про те, чи має корпоративний (або некорпоративний) актив правильну операційну систему, цілісність програмних компонентів або будь-які відомі вразливості.

Система відповідності галузевим стандартам (Industry compliance system, ICM) містить правила політик та контролює їх дотримання. Більшість компаній та організацій мають певний набір регуляторних вимог, які мають виконувати усі, зокрема, медичні установи.

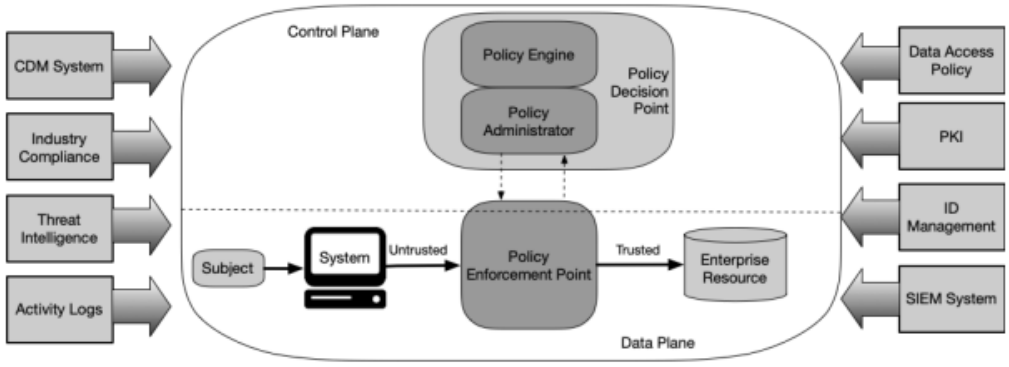

Рис. 1. Архітектура Zero Trust

Зведення даних про загрози: внутрішні або зовнішні джерела надають інформацію про нові вразливості, програмні помилки та шкідливе ПЗ, на основі якої PE приймає рішення про заборону доступу.

Обговорення

У цьому розділі здійснено аналіз отриманих результатів, їх порівняння з попередніми дослідженнями та визначено обмеження запропонованих методів.

Результати дослідження підтверджують тенденції, зазначені в роботах Mario Gama (2024) та Harnaha, 2025, де зазначено, що застосування принципів Zero Trust і машинного навчання суттєво підвищує ефективність виявлення аномалій у мережевому трафіку.

Проте, у порівнянні з попередніми роботами спостерігається. Потреба у високопродуктивних серверах для обробки великих масивів даних у реальному часі, що є обмеженням для невеликих організацій. Хоча застосовані алгоритми продемонстрували високу ефективність, існують певні обмеження:

1. Моделі навчались на тестових даних із заздалегідь відомими характеристиками, тому ефективність на повністю реальних сценаріях може бути нижчою.
2. Лінійні та класичні моделі RBAC не враховують повністю поведінкові патерни користувачів у складних корпоративних мережах.
3. Принцип Zero Trust вимагає постійної аутентифікації та моніторингу, що може впливати на швидкість роботи системи та зручність користувачів.

Висновки

Проведене дослідження показало, що застосування принципів Zero Trust дозволяє підвищити ефективність виявлення аномалій у мережевому трафіку до 92%. Результати також підтверджують, що традиційні методи контролю доступу та рольові моделі RBAC залишаються важливими для забезпечення базового рівня безпеки, однак їх точність нижча порівняно з інтелектуальними підходами.

Аналіз обмежень показав, що ефективність алгоритмів залежить від якості та обсягу навчальних даних, а також від апаратних ресурсів, що використовуються для обробки великих потоків інформації. Використання Zero Trust у комплексі з багатофакторною автентифікацією та моніторингом користувачів забезпечує значне зниження ризиків несанкціонованого доступу, але вимагає додаткових технічних і організаційних ресурсів.

У майбутніх дослідженнях планується розробка адаптивних моделей кіберзахисту з використанням алгоритмів глибокого навчання для автоматичного прогнозування нових видів кібератак та оптимізації політик доступу в реальному часі.

Джерела

1. ENISA. (2024). Annual Threat Landscape Report. European Union Agency for Cybersecurity. URL - https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

2. State Service of Special Communication and Information Protection of Ukraine (CERT-UA). (2024). Cyber incidents statistics in Ukraine URL - https://cert.gov.ua/

3. Ворохоб, М., Киричок, Р., Яскевич, В., Добришин, Ю., & Сидоренко, С. (2023). Сучасні перспективи застосування концепції zero trust при побудові політики інформаційної безпеки підприємства. Кібербезпека: освіта, наука, техніка, 1(21), 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233

4. Regulation (EU) 2016/679 (GDPR). URL - https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

5. Buczak A.L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Comm. Surveys & Tutorials, 2021. URL - https://www.researchgate.net/publication/350115358_A_Survey_Data_Mining_and_Machine_Learning_Methods_for_Cyber_Security

6. Цехмейстер, Р., Платоненко, А., Ворохоб, М., Черевик, В., & Семеняка, С. (2025). Дослідження методів забезпечення інформаційної безпеки у віртуальному середовищі. Кібербезпека: освіта, наука, техніка, 3(27), 63–71. https://doi.org/10.28925/2663-4023.2025.27.703

7. What is zero trust URL - https://www.trendmicro.com/ru_ru/what-is/what-is-zero-trust/zero-trust-architecture.html

8. Mario Gama (2024) Що таке Zero Trust і навіщо він потрібен URL - https://www.softwareone.com/uk-ua/blog/articles/2021/06/17/zero-trust-security

9. Harnaha. (2025) Використання підходів zero trust architechture при розробці мобільних додатків URL - https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/47650/25380.pdf?sequence=3&isAllowed=y

10. Kriuchkova, L., Skladannyi, P., & Vorokhob, M. (2023). Pre-project solutions for building an authorization system based on the zero trust concept. Cybersecurity: Education, Science, Technique, 3(19), 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242

11. Контроль доступу на основі ролей (Role-Based Access Control або RBAC) у пайплайні CI/CD: DevSecOps URL - https://cases.media/en/article/kontrol-dostupu-na-osnovi-rolei-role-based-access-control-abo-rbac-u-paiplaini-ci-cd-devsecops?srsltid=AfmBOop-cZzvnoero5j1Bh256uUzPALQ-ebZOrOSAsLc-E3VtnWWRSjY

12. Anderson, R. (2023). Security engineering: A guide to building dependable distributed systems (4th ed.). Wiley. URL - https://books.google.bs/books?id=eo4Otm_TcW8C&printsec=frontcover&source=gbs_atb#v=onepage&q&f=false

13. Костюк, Ю., Складанний, П., Рзаєва, С., Мазур, Н., Черевик, В., & Аносов, А. (2025). Особливості реалізації мережевих атак через TCP/IP-протоколи. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915

14. Stallings, W. (2022). Cryptography and Network Security: Principles and Practice (8th ed.). Pearson. URL - https://mrce.in/ebooks/Cryptography%20&%20Network%20Security%208th%20Ed.pdf