фінансові витрати організації, а й підвищити ефективність роботи обладнання, покращити надійність мережі та забезпечити більш екологічний підхід до експлуатації ІТ-інфраструктури.

Список використаних джерел:

1. Бондаренко В. О. Енергоефективність мережевої інфраструктури підприємств в умовах цифровізації. Комп'ютерні системи та мережі. 2024. № 3. С. 41–49.
2. Коваленко І. М. Сучасні підходи до оптимізації енергоспоживання серверного обладнання. Вісник комп'ютерної інженерії. 2023. Вип. 12. С. 88–95.
3. Мельник О. М. Адміністрування та енергоефективність інформаційних систем : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2024. 296 с.
4. Петренко В. І. Моніторинг та управління енергоспоживанням мережевої інфраструктури. Інформаційні технології та системи. 2025. № 1. С. 73–81.
5. Brown T., Wilson J. Energy-Efficient Network Infrastructure Management. 2nd ed. New York: Springer, 2025. 385 p.

УДК 004.8:004.056

ZERO TRUST ARCHITECTURE ЯК СУЧАСНА КОНЦЕПЦІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ

Ковальчук В.М.
vladislav72k@gmail.com
Черкаський державний фаховий бізнес-коледж
Захарова М.В.
м. Черкаси, Україна

Сучасні корпоративні мережі стикаються з безпрецедентним зростанням кіберзагроз, що ставлять під сумнів ефективність традиційних методів захисту. Стандартні моделі безпеки, засновані на довірі до внутрішньої мережі та зонах контролю, поступово втрачають актуальність через поширення хмарних сервісів,

віддаленої роботи та особистих пристроїв працівників, що використовуються для доступу до корпоративних ресурсів. Альтернативою класичному підходу є концепція Zero Trust Architecture (ZTA), яка базується на припущенні, що мережа вже потенційно скомпрометована.

Метою цієї роботи є дослідження архітектури Zero Trust як сучасної концепції забезпечення безпеки корпоративних мереж, аналіз її основних принципів, компонентів і механізмів контролю доступу.

Традиційні підходи до мережевої безпеки базуються на концепції «периметра», де захист будується навколо корпоративної мережі, формуючи умовну межу між довіреним внутрішнім середовищем і потенційно небезпечним зовнішнім. Така модель передбачає використання механізмів контролю доступу для користувачів, застосунків та інших компонентів, що взаємодіють із ресурсами. Її ключове припущення полягає в тому, що загрози походять переважно ззовні, тоді як внутрішнім суб'єктам можна довіряти. Однак із розвитком цифрових технологій і поширенням дистанційної роботи ці межі стають розмитими, що знижує ефективність периметрового підходу.

На відміну від цього, модель Zero Trust зосереджується безпосередньо на захисті ресурсів. У ній мережеве розташування не визначає рівень довіри: жоден користувач, пристрій чи сервіс не вважається надійним за замовчуванням. Доступ надається динамічно – лише після автентифікації, авторизації та оцінки контексту кожного запиту.

ZTA використовує принципи нульової довіри для планування та захисту корпоративної інфраструктури та робочих процесів. За дизайном середовище ZTA охоплює поняття відсутності неявної довіри до активів і суб'єктів, незалежно від їхнього фізичного чи мережевого розташування. Таким чином, ZTA ніколи не надає доступ до ресурсів, доки предмет, актив або робоче навантаження не будуть перевірені. Є багато логічних компонентів, які складають розгортання ZTA на підприємстві. Ці компоненти можуть працювати як локальна служба або через хмарну службу.

Таблиця 1 – Порівняння моделей безпеки

№	Захист «Периметр»	Zero Trust
1	Довіра за замовчуванням	Верифікація є обов’язковою
2	Захист фокусується на периметрах контрольованої зони	Захист фокусується на ресурсах
3	Доступ надається на основі статичних рішень	Доступ надається на основі динамічної політики в доступ є бінарним
4	Не передбачається обов'язкове використання	Передбачається обов'язкове використання політик політик розмежування доступу
5	Ручне управління ризиками	Автоматизоване управління ризиками

Модель концептуальної основи на рис.1 показує базовий зв’язок між компонентами та їх взаємодією. Точка прийняття рішень (PDP) розбивається на два логічні компоненти: механізм політики та адміністратор політики. Логічні компоненти ZTA використовують окрему площину керування для зв’язку, тоді як дані програми передаються на площині даних.

У моделі Zero Trust Architecture точка прийняття рішень (Policy Decision Point, PDP) є центральним логічним компонентом, що визначає можливість доступу користувача або пристрою до ресурсу. PDP складається з двох частин: двигуна політики (Policy Engine, PE) та адміністратора політики (Policy Administrator, PA).

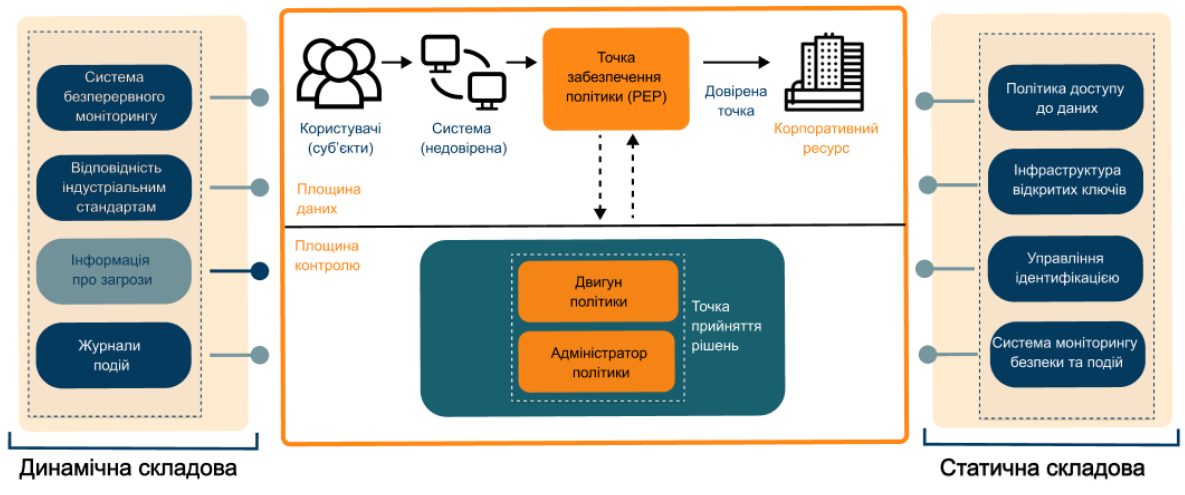

Рисунок 1 – Логічні компоненти Zero Trust

PE виконує аналітичну функцію, оцінюючи запит на основі політик безпеки, ідентичності користувача, стану пристрою та контексту підключення, після чого формує рішення про дозвіл або відмову. PA забезпечує виконання цього рішення, встановлюючи або розриваючи з'єднання, а також керуючи видачею тимчасових облікових даних чи токенів доступу.

Ядро Zero Trust Architecture використовує дані з різних джерел для контролю мережевих з'єднань і складається зі статичної та динамічної складових. До статичної належать політики доступу, інфраструктура відкритих ключів (PKI), системи керування ідентифікацією та механізми відповідності вимогам. Динамічна складова включає системи безперервної діагностики (CDM), розвідки загроз, журнали активності та системи SIEM, які забезпечують моніторинг і оцінювання рівня безпеки.

Обробка запитів у PDP здійснюється за допомогою інтелектуального механізму політик (IPE), що поєднує статичні й динамічні правила. У межах Zero Trust мережа поділяється на окремі площини, зокрема площину даних, яка відповідає за передачу трафіку між користувачем і ресурсами.

Процес автентифікації в Zero Trust виходить за межі перевірки ідентичності та враховує стан пристрою, мережевий контекст і поведінку користувача. Вона охоплює як автентифікацію користувача, так і пристрою, використовуючи, зокрема, біометричні методи та автентифікацію на фізичному рівні (PLA), що підвищує достовірність доступу.

У результаті проведеного аналізу встановлено, що Zero Trust Architecture формує новий підхід до захисту корпоративних мереж, орієнтований на контроль доступу з урахуванням контексту, стану пристроїв і поведінкових характеристик користувачів. Використання динамічних політик, безперервної автентифікації та моніторингу дозволяє адаптувати рішення відповідно до поточного рівня ризику. Поєднання статичних правил із динамічними даними забезпечує більш гнучке та ефективне управління доступом порівняно з традиційними моделями. Впровадження ZTA підвищує стійкість інформаційних систем до сучасних

кіберзагроз і забезпечує контрольовану взаємодію між користувачами, пристроями та ресурсами.

Список використаної літератури:

1. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2020. 59 p. (NIST Special Publication 800-207). Режим доступу: Zero Trust Architecture (NIST SP 800-207) (дата звернення: 07.04.2026).
2. Zero Trust Architecture / C. Green-Ortiz et al. Cisco Press, 2022.
3. Introductory Guide to Zero Trust Architecture. Zero Trust Education, 2024.
4. Zero Trust Security Paradigm: A Comprehensive Survey and Research Analysis / Journal of Electrical Systems. 2023. No19(2). С. 28–37.
5. Verify and trust: A multidimensional survey of zero-trust security in the age of IoT / [M. A. Azad, S. Abdullah, J. Arshad та ін.] // Internet of Things. 2024. No27. С. 101227.
6. Exploring Effective Zero Trust Architecture for Defense Cybersecurity: A Study / [Y. Kim, S. Sohn, K. T. Kim та ін.] // KSII Transactions on Internet and Information Systems. 2024. No18(9). С. 2665–2691.

УДК 004.4

DEVOPS - ПІДХОДИ В УПРАВЛІННІ РОБОТОТЕХНІЧНИМИ СИСТЕМАМИ

Мусієнко О.О.
musienkos1975@gmail.com
Черкаський державний фаховий бізнес-коледж
Литовченко В.О.
м. Черкаси, Україна

Сьогодні робототехнічні системи стають все складнішими. Вони поєднують у собі апаратну та програмну частини і часто працюють у режимі реального часу. Через це зростають вимоги до їх розробки, тестування та підтримки. Звичайні підходи не завжди добре справляються з такими задачами, тому все частіше використовують DevOps-підходи [2].