Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 004.056
DOI: 10.32447/20784643.30.2024.07

Т. І. Коробейнікова, І. М. Журавель,
А. О. Бодак, Д. В. Бороденко
Національний університет «Львівська політехніка», м. Львів, Україна
ORCID: https://orcid.org/0000-0003-2487-8742 – Т. І. Коробейнікова
https://orcid.org/0000-0003-1114-0124 – І. М. Журавель
https://orcid.org/0009-0001-7140-0728 – А. О. Бодак
https://orcid.org/0009-0006-4978-0118 – Д. В. Бороденко
✉tetiana.i.korobeinikova@lpnu.ua

КОНЦЕПЦІЯ НУЛЬОВОЇ ДОВІРИ: СУЧАСНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В КОРПОРАТИВНИХ МЕРЕЖАХ

Проблема сучасних корпоративних мереж полягає в зростанні кількості кіберзагроз, які ставлять під сумнів ефективність традиційних моделей захисту. Стандартні підходи безпеки, що базуються на довірі до внутрішньої мережі й використанні периметрових захисних рішень, втрачають актуальність у зв'язку з поширенням хмарних сервісів, віддаленої роботи та використанням пристроїв користувачів. Таким чином, традиційні методи вразливі перед сучасними атаками, а порушники можуть безперешкодно проникати у внутрішню мережу, залишаючись непоміченими та отримуючи необмежений доступ до ресурсів.

Мета статті полягає в аналізі концепції "нульової довіри" (ZT, Zero Trust) для забезпечення кібербезпеки корпоративних мереж. Автори прагнуть виявити найбільш ефективні методи захисту, що відповідають сучасним вимогам до кібербезпеки, дослідити їх впровадження та забезпечити безперервний моніторинг й управління ризиками в умовах зростаючих кіберзагроз.

Методи дослідження включають теоретичний аналіз стандарту NIST SP 800-207, що регламентує принципи нульової довіри, та аналітичний огляд літературних джерел. Окрім цього, проведено порівняння моделей захисту на основі традиційної периметрової безпеки та моделі нульової довіри (ZTM, ZT Model), що дає змогу ідентифікувати ключові розбіжності та переваги обох підходів.

Основні результати дослідження свідчать, що впровадження нульової довіри забезпечує більш детальний контроль доступу, де кожен користувач та пристрій проходять автентифікацію і авторизацію перед отриманням доступу до ресурсів. Завдяки принципам мінімальних привілеїв та динамічним політикам доступу на основі поведінкових атрибутів і контекстної інформації, модель суттєво зменшує ризики несанкціонованого доступу навіть у разі проникнення зловмисників у мережу. Впровадження архітектури нульової довіри також передбачає використання технологій сегментації, багатофакторної автентифікації (MFA), безперервної оцінки доступу та поведінкової автентифікації, що значно підвищує рівень безпеки в корпоративних мережах.

У висновках запропоновано рекомендації щодо інтеграції ZTM в корпоративні мережі для забезпечення гнучкого й адаптивного захисту. Відзначено, що перехід до ZTM потребує значних інвестицій, модернізації інфраструктури та автоматизації контролю доступу. Розглянуто виклики, пов'язані з продуктивністю, через підвищене навантаження на обчислювальні ресурси та зростання кількості запитів на авторизацію, а також рекомендації для усунення ризиків, спричинених масштабуванням SaaS-додатків.

Ключові слова: Нульова довіра, модель нульової довіри, кібербезпека, корпоративні мережі, модель загроз, контроль доступу, сегментація, автоматизація, безперервний моніторинг.

T. I. Korobeinikova, I. M. Zhuravel,
A. O. Bodak, D. V. Borodenko
Lviv Polytechnic National University, Lviv, Ukraine

ZERO TRUST CONCEPT: MODERN METHODS OF ENSURING CYBERSECURITY IN CORPORATE NETWORKS

Introduction. The problem with modern corporate networks is the growing number of cyber threats that call into question the effectiveness of traditional security models. Standard security approaches based on internal network trust and perimeter protection solutions are losing relevance due to the proliferation of cloud services, remote work, and the

use of personal devices. Consequently, traditional methods are vulnerable to modern attacks, allowing attackers to infiltrate the internal network undetected, thereby gaining unrestricted access to resources.

Purpose. This article analyzes the zero trust (ZT, Zero Trust) concept to ensure cybersecurity in corporate networks. The authors aim to identify the most effective security methods that meet modern cybersecurity requirements, explore their implementation, and provide continuous monitoring and risk management in the face of growing cyber threats.

Methods. The research methods include a theoretical analysis of the NIST SP 800-207 standard, which governs ZT principles, and an analytical literature review. Additionally, a comparison between traditional perimeter-based security models and the Zero Trust model (ZTM, ZT Model) was conducted to identify key differences and advantages of both approaches.

Results. The main research findings indicate that implementing ZTM provides more detailed access control, where each user and device undergoes authentication and authorization before accessing resources. With the principles of least privilege and dynamic access policies based on behavioral attributes and contextual information, the model significantly reduces the risk of unauthorized access, even in the event of an intruder's presence within the network. The implementation of ZT architecture also involves technologies such as segmentation, multi-factor authentication (MFA), continuous access evaluation, and behavioral authentication, which collectively enhance corporate network security.

The conclusions propose recommendations for integrating the ZTM into corporate networks to ensure flexible and adaptive protection. It is noted that transitioning to ZTM requires substantial investment, infrastructure modernization, and automated access control. Challenges related to performance due to the increased load on computational resources, the growing number of authorization requests, and recommendations for mitigating risks associated with scaling SaaS applications are also considered.

Keywords: Zero Trust, Zero Trust Model, cybersecurity, corporate networks, threat model, access control, segmentation, automation, continuous monitoring.

Вступ

Постановка проблеми. 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. В таких умовах традиційні засоби захисту стають вразливими, а порушники можуть безперешкодно проникати у внутрішні мережі, залишаючись непоміченими, що дає змогу їм можливість отримати неконтрольований доступ до даних і критичних ресурсів.

Аналіз останніх досліджень і публікацій

Упродовж останніх років концепція ZT привертає увагу дослідників і практиків як потенційно більш ефективний підхід до забезпечення кібербезпеки [1–2]. Багато наукових праць присвячено принципам ZT, зокрема архітектурі ZT – ZTA [3–4] та основним компонентам, таким як автентифікація та авторизація користувачів [5–6], динамічний контроль доступу [7], MFA та сегментація мережі [8–9]. Стандарти, як-от NIST SP 800-207, пропонують докладні настанови щодо реалізації ZT, що стимулює подальше вивчення та впровадження цієї моделі [10–11].

В Україні питаннями принципу нульової довіри в корпоративних мережах активно займаються Журавчак Д., Глущенко П., Опанович М., Дудикевич В., Піскозуб А. і в своїй роботі [12] розвивають підхід до захисту Active Directory від загроз, пов'язаних з програмами-вимагачами, що стають все більш небезпечними для корпоративних інформаційних систем. Вчені А. Єсін, В., Вілігура, В. та ін. в [13–14] досліджують теоретичний та практичний потенціал принципу нульової довіри; сучасні виклики та підходи до стратегії захисту від APT атак, з особливим фокусом на ZTA у [15] розглядає Опанович М.; група вчених Маліновський, В. , Куперштейн Л. , Лукічов В., та Дудатьєв А. у роботі [16] працюють в парадигмі нульової довіри під час кіберзахисту під час передачі даних у IoT і захищеної криптографічної обробки і передачі інформації у приладах та інформаційних системах Інтернету речей; питаннями впровадженню децентралізованих технологій для зберігання даних із застосуванням принципів нульової довіри працюють Іскрижицький, А. та Задорожній, А. в [17].

Попри значний прогрес у дослідженні ZT, залишається низка невирішених питань, зокрема, виклики, пов'язані з впровадженням ZT в організаціях з великою кількістю користувачів, масштабними інфраструктурами та різноманітними бізнес-процесами. Таким чином, розробка підходів до ефективного впровадження ZT без шкоди для продуктивності та з урахуванням особливостей управління ризиками та доступом у великих корпоративних середовищах є актуальною проблемою кібербезпеки.

Метою статті є аналіз сучасних методів забезпечення безпеки інформаційних систем у корпоративних мережах на основі підходу нульової довіри з метою визначення найбільш ефективних практик для підвищення рівня захищеності корпоративних мереж від сучасних кіберзагроз.

Методи дослідження

Для проведення дослідження використано стандартні методики аналізу інформаційних систем безпеки в контексті концепції ZT. Основою методології слугує теоретичний аналіз та порівняння традиційних моделей периметрової безпеки із ZT, що дає змогу оцінити їхні переваги та недоліки в умовах сучасного кіберсередовища. Основним матеріалом для дослідження є стандарт NIST SP 800-207 із його рекомендаціями щодо ZTM. Було також проведено огляд сучасних наукових праць, присвячених аналізу та практичному застосуванню ZT, щоб виділити актуальні методи і технології в цій сфері. Додатково використовувались аналітичні матеріали з кібербезпеки, щоб виявити взаємозв'язок між ефективністю захисту та застосуванням динамічних політик доступу і мінімальних привілеїв.

Дослідження здійснювалось шляхом систематизації основних принципів ZT, таких як MFA, безперервний моніторинг, динамічна авторизація та сегментація мережі. Використовувались методи аналітичного порівняння для оцінки ефективності ZT відносно традиційних методів безпеки на основі периметра.

Хід дослідження включав порівняння моделей захисту за такими критеріями: контроль доступу, ідентифікація та аутентифікація користувачів, сегментація, а також можливості автоматизації безперервного моніторингу та оцінки ризиків. Отримані результати дали змогу сформувати рекомендації щодо впровадження ZTM в корпоративних мережах з урахуванням можливих викликів та специфічних потреб великих інфраструктур.

Обговорення результатів досліджень

В роботі пропонується застосування моделі безпеки нульової довіри – ZTM, метою якої є запобігання несанкціонованому доступу (НСД) до даних та сервісів, створення максимально деталізованого контролю доступу.

Основна увага приділяється автентифікації, авторизації усіх процесів та зменшенню кількості зон умовної довіри для створення безпечної та ефективної мережі. Оглянемо стандарт NIST SP 800-207 [10] і відобразимо огляд у таблиці 1:

1. Ресурси, джерела даних та інформаційні сервіси та системи мають бути захищеними.

2. Усі комунікації (зовнішні і внутрішні) мають бути захищеними.

3. Доступ до кожного ресурсу надається на сесійній основі, на основі мінімальних привілеїв, на визначений період часу та не може свідчити про надання доступу до інших ресурсів чи для інших користувачів.

4. Доступ до ресурсів визначається динамічною політикою, що враховує поточний стан ідентичності автору, що здійснює запит, а також може включати інші поведінкові атрибути або атрибути середовища. За замовчуванням доступ до ресурсів не надається або ж є відхиленим. Захист ресурсів передбачає визначення чіткої політики розмежування доступу для всіх користувачів і процесів методом мінімальних привілеїв. Оцінка ризику здійснюється на основі інтерпретації усіх можливих факторів.

5. Власні і орендовані ресурси знаходяться під постійним контролем, жоден не вважається надійним «за замовчуванням». До ресурсів, в яких було виявлено несправності, встановлення довіри може відрізнятись від ресурсів, що визнано придатними.

6. Автентифікація та авторизація ресурсів є динамічною і виконується перед наданням доступу. Передбачається постійний цикл сканування та оцінки ризиків, надання доступу та постійної переоцінки безпеки комунікацій та мережі, що вимагає ефективної системи управління ідентифікацією, обліковими даними та доступом (ICAM).

7. Здійснюється збір усієї можливої актуальної інформації про стан ресурсів, інфраструктури, комунікацій, та використовується для посилення безпеки, покращення діючих політик безпеки і оцінки ризиків під час надання доступу.

Таблиця 1

Порівняння моделей безпеки з використанням контрольованої зони та ZTM

З використання контрольованої зони	ZTM
Довіра за замовчуванням	Верифікація є обов’язковою
Захист фокусується на периметрах контрольованої зони	Захист фокусується на ресурсах
Доступ надається на основі статичних рішень, доступ є бінарним	Доступ надається на основі динамічної політики в реальному часі
Не передбачається обов'язкове використання політик розмежування доступу	Передбачається обов'язкове використання політик розмежування доступу на основі мінімальних привілеїв
Ручне управління ризиками	Автоматизоване управління ризиками

Авторська розробка на основі аналізу відкритих джерел

Актори ZTM. У ZTM всі об’єкти і суб’єкти в мережі мають бути захищеними. Виокремлюють 6 основних категорій сутностей, до яких слід застосовувати принципи даної моделі

ідентичності, обладнання, програми, інфраструктура та мережі, дані [10, 18].

Ідентичностями можуть бути користувачі, сервіси, обладнання, що мають ресурси для успішного проходження ідентифікації та авторизації на основі мінімальних привілеїв. Побудова та захист ідентичностей є критично важливим компонентом ZTM, оскільки вони використовуються для логування, проведення аудиту, а також для створення сесій до ресурсів у мережі. Організація не може застосовувати внутрішні політики до зовнішніх акторів, проте політики ZTM мають стосуватись працівників, партнерів, вендорів, клієнтів і т.д.

Пристрої можуть належати організації, бути власністю користувачів і клієнтів і до них застосовуються принципи ZTM. Для цього використовується динамічна інвентаризація всіх активів, включаючи їхнє обладнання, ПЗ тощо, а також їхні конфігурації та пов'язані з ними вразливості, коли вони стають відомими.

Програми здійснюють обробку, збереження та поширення даних організації, отже доступ до них повинен бути аутентифікований та авторизований незалежно чи ці програми є власністю організації, чи є орендованими. Введення детального контролю доступу та інтегрованого захисту від загроз можуть забезпечити краще розуміння ситуації та зменшити загрози для додатків.

Мережа та налаштування її інфраструктури повинні гарантувати безпечний доступ до ресурсів, а кожна взаємодія в мережі має бути перевірена. Передбачається використання вже відомих методів захисту мережі (міжмережеві екрани, сегментація, ізоляція хостів, керування потоками) з використанням контекстно-орієнтованим керування доступу та динамічних політик, враховуючи попередньо зібрану інформацію про поведінкові атрибути та середовище.

Захист даних передбачає класифікацію, маркування та шифрування даних і забезпечується під час усіх операцій над усіма даними.

Застосування політик ZTM до всіх об’єктів і суб’єктів створює несприятливі умови для здійснення НСД до ресурсів організації. Навіть при отриманні НСД, усі дії зловмисника фіксуються, створюючи поведінкові атрибути для переоцінки ризиків під час створенні нової сесії. Використання динамічних політик і актуальних засобів безпеки на всіх рівнях зменшує ризики через виконання НСД, навіть, якщо зловмисник вже добре ознайомлений з структурною організації мережі при атаках типу програма-вимагач, спробах зміни налаштувань засобів безпеки чи компонентів мережі, та під час зміни/видалення/модифікації/викрадення даних.

Архітектура нульової довіри. «Архітектура нульової довіри – це план кібербезпеки підприємства, який використовує концепції нульової довіри та охоплює зв’язки компонентів, планування робочого процесу та політики доступу» – Національний інститут стандартів і технологій (NIST) [19–20].

Архітектура нульової довіри (ZTA, ZT Architecture,) спрямована на трансформацію підходів до кібербезпеки, переосмислюючи традиційні моделі захисту інформаційних систем. Вона заперечує наявність заздалегідь встановленого рівня довіри як всередині, так і за межами мережі, забезпечуючи сувору перевірку кожного запиту доступу незалежно від його джерела.

Традиційні підходи до безпеки мережі базуються на концепції «периметра», де захист будується навколо периметра корпоративної мережі та часто включає учасників (кінцевих користувачів, програми та інших, які запитують доступ до системних елементів). Основне припущення полягає в тому, що загрози в основному походять із зовнішнього середовища, а внутрішнім ресурсам і користувачам можна довіряти.

Основна концепція захисту на основі периметра полягає в наданні довіреним користувачам доступу до внутрішньої мережі та блокуванні ненадійних користувачів [7]. Однак прогрес у таких технологіях, як хмарні сервіси та віддалена робота, стирає межі корпоративних мереж і знижує ефективність захисту периметра. ZTA зосереджується на захисті самих ресурсів, а не периметра мережі, оскільки мережеве розташування більше не розглядається як головний компонент рівня безпеки, необхідного для ресурсу.

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 [21].

Є багато логічних компонентів, які складають розгортання ZTA на підприємстві. Ці компоненти можуть працювати як локальна служба або через хмарну службу. Модель концептуальної основи на рисунку 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 [18].

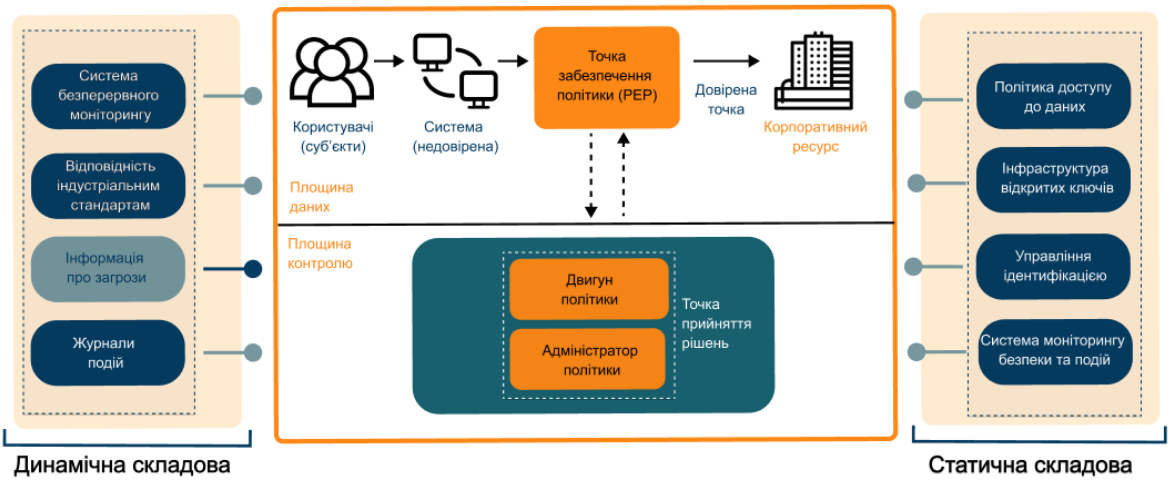

Рисунок 1 – Логічні компоненти ZT

Авторська розробка на основі [10, 22]

У традиційній площині керування ZTA точка прийняття рішень (PDP) поділяється на двигун політики (PE) і адміністратор політики (PA) для прийняття та виконання рішень [2].

Оцінка довіри є основним алгоритмом PE, який оцінює надійність суб'єкта на основі даних із різних джерел. PE вирішує, чи надавати суб'єкту доступ до ресурсів на основі оцінок довіри за допомогою наданих облікових даних. PE – це, по суті, контроль доступу до ідентифікаційних даних користувача та пристроїв. Тому, щоб досягти точності та своєчасності контролю доступу, аутентифікації та авторизації, необхідно автоматизувати процес оцінки довіри та динамічно коригувати рішення шляхом оновлення значення довіри в режимі реального часу на основі інформації, що постійно збирається [7].

Політика доступу (PA) в першу чергу відповідає за встановлення шляху зв'язку між об'єктом, що запитує доступ, і необхідним ресурсом, а також за генерацію даних автентифікації для конкретного сеансу.

Ядро ZTA покладається на дані з кількох периферійних пристроїв для встановлення та контролю з'єднань. Модулі можуть бути частиною статичної складової ядра (у правій частині зображення) або динамічної складової (у лівій частині). Статичні модулі складаються з політики доступу до даних, інфраструктури відкритих ключів (PKI), керування ідентифікацією (ID) і галузевої відповідності. Ці модулі спільно встановлюють правила політики безпеки для безпечного зв'язку та перевірки цілісності. Ядро ZTA може динамічно змінювати правила політики. ZTA характеризується унікальними динамічними модулями. Компоненти складаються з постійної діагностики і пом'якшення (CDM), розвідка про загрози для виявлення нових вразливостей безпеки, журнали активності, що надають дані про поведінку користувачів, активи та мережевий трафік, а також інформація про безпеку та керування подіями (SIEM) для збору інформації про загальний стан безпеки та можливі загрози [8].

Механізм обробки PDP – це механізм інтелектуальної політики (IPE), який використовує статичні та динамічні правила для прийняття рішення щодо дозволу доступу. ZTA розділяє мережу на три чіткі логічні та, можливо, фізичні площини [12]. Передача даних між суб'єктом і мережевими ресурсами відбувається в площині даних, яка охоплює площину суб'єкта.

Оскільки ZTA охоплює широкий спектр випадків використання додатків, процес автентифікації більше не обмежується перевіркою ідентичності користувача, але також містить інші перевірки автентичності.

ZTA припускає, що жодна сутність, будь то внутрішня чи зовнішня, не може бути надійною за своєю суттю, і, таким чином, кожен користувач і пристрій повинні постійно автентифікувати та перевіряти свою особу та дозволи [9]. Точна автентифікація є ключовим фактором у мінімізації ризику атак, спричинених підробленою ідентифікацією, тому її варто розглядати у двох аспектах: автентифікація користувача та автентифікація пристрою. Існуючі технології автентифікації можна розділити на біометричну ідентифікацію та автентифікацію фізичного рівня, які використовуються для автентифікації користувачів і пристроїв відповідно.

Сучасні підходи, такі як біометричні методи та автентифікація на фізичному рівні (PLA), пропонують високоефективні рішення для забезпечення достовірності суб'єктів доступу.

Застосовуючи суворий контроль доступу, безперервний моніторинг і оцінку ризиків у реальному часі, ZTA гарантує, що лише авторизовані особи можуть отримати доступ до певних ресурсів, пом'якшуючи потенційний вплив скомпрометованих пристроїв або зловмисників [10].

Безперервна автентифікація спрямована на постійну перевірку ідентичності кінцевої точки під час сеансу зв'язку. PLA на основі штучного інтелекту розглядається як потенційне рішення, де алгоритми штучного інтелекту можуть ефективно отримувати функції пристрою з каналу зв'язку та постійно перевіряти ідентичність користувачів і пристроїв [11].

Виклики, пов'язані із недотриманням принципів нульової довіри. Дотримання принципів нульової довіри пов'язане із багатьма труднощами. CISA описує це так: «Застарілі системи часто покладаються на «неявну» довіру, в якій доступ і авторизація рідко оцінюються на основі фіксованих атрибутів; це суперечить основному принципу адаптивної оцінки довіри. Існуючі інфраструктури, побудовані на неявній довірі, потребують інвестицій та технологій для зміни систем, щоб краще відповідати принципам нульової довіри».

Отже імплементуючи ZTM, невід'ємною частиною є створення автоматизованого контролю політик безпеки, що передбачає ряд труднощів під час переходу від моделі безпеки на основі контрольованої зони до ZTM:

1. Використання застарілої архітектури, де комунікація між ресурсами не є контрольованою та не передбачає відповідного рівня безпеки. Застарілі системи не здатні запобігти несанкціонованому переміщенню між ресурсами мережі.

2. Створення нової політики контролю безпеки, що передбачає динамічну автоматизацію.

3. Потреба в ідентифікації та динамічній авторизації потребує більш комплексного підходу, пов'язаного з мінливим станом системи та параметрів ресурсів.

Кращі практики сучасного світу. ZTM чи ZTA не є продуктом чи послугою, а сукупністю людей, процесів та технологій [23]. Одним з найважливіших аспектів нульової довіри є визначення ресурсів, що мають бути захищені: дані, застосунки, активи, сервіси, користувачі, пристрої, враховуючи пристрої категорії BYOD. Важливо зрозуміти як між ними відбувається комунікація, які є комунікаційні канали, що є основою для побудови ZTA та створення нових політик безпеки. Надалі передбачається проведення постійного контролю, підтримки і оновлення. Цей підхід був описаний аналітиком з Forrester Research Джоном Кіндервагом (John Kindervag) та наведений на рисунку 2.

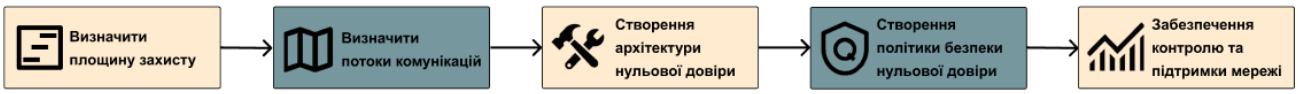

Рисунок 2 – Підхід впровадження ZTM

Джерело [23]

Тут ключовим підходом до побудови ZTA є використання мікросегментації і для цього використовується технологія vNET. Мережевий трафік контролюється між підмережами, між інтернетом і підмережею через віртуальну мережу. Тобто з'єднання з ресурсами однієї підмережі не гарантує з'єднання з ресурсами іншої. Масштабованість реалізується використанням Peered Networks, і тоді зв'язок між vNET'ами можливий виключно при явно заданій конфігурації, а одна vNET не може бути каналом зв'язку між іншими vNET 'ами. Додатково розгортання мережі передбачає використання технології Hub&Spoke, де з'єднання між мережами можливе виключно напряму. Усі комунікації шифруються відповідними протоколами та контролюються на 3-4 рівнях моделі TCP/IP. Цей метод передбачає безпечну шифровану комунікацію, локалізацію загроз на найнижчому рівні сегментації – підмережі.

Забезпечення автоматизованого контролю політик безпеки досягається створенням інвентарю з використанням сигналів, тобто індикаторів стану безпеки. Одним із підходів може бути метод Кіплінга [23] (рисунок 3), що стає основою для створення динамічних політик безпеки, які в свою чергу використовуються алгоритмом довіри.

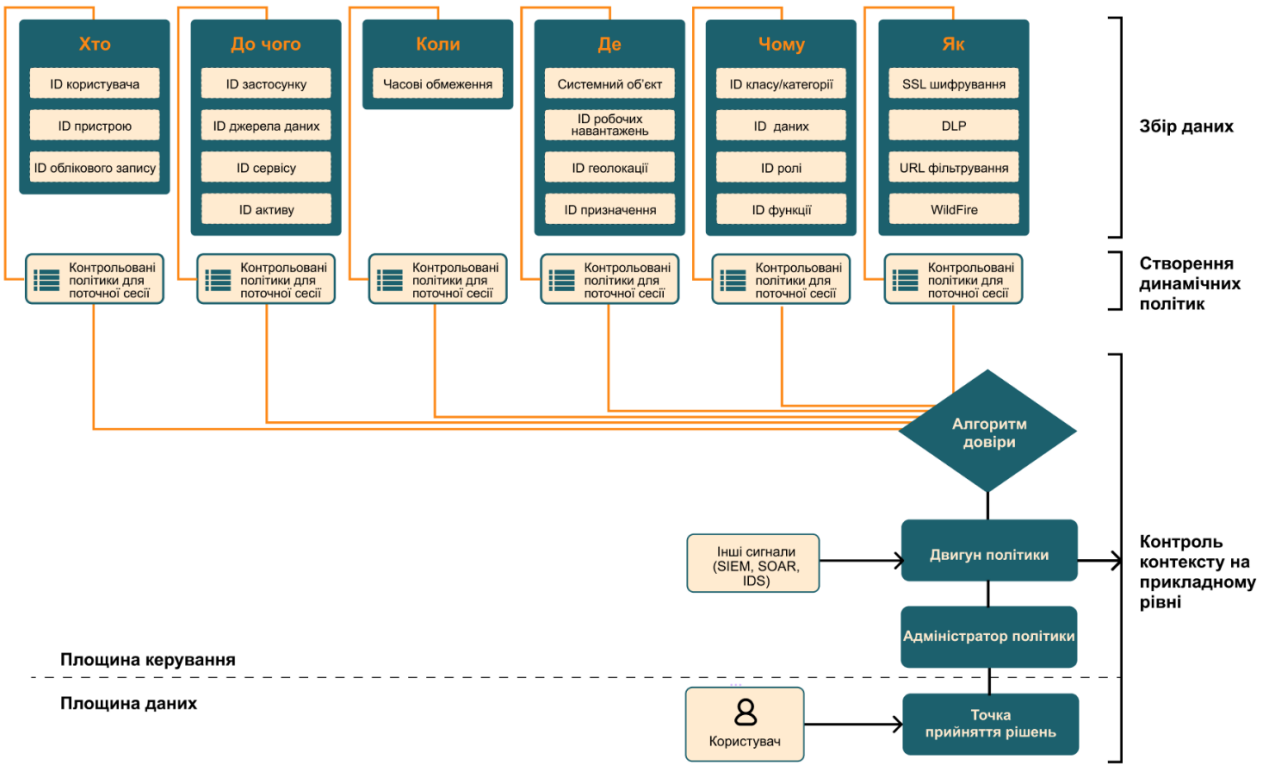

Рисунок 3 – Приклад механізму авторизації

Розроблено на основі [23]

Як видно з рисунка 3, схема використовує політики безпеки для створення кожного окремого з'єднання, враховуючи поточні параметри. Також передбачаються моніторингові сигнали від таких служб: системи керування захистом інформації (SIEM), оркестрація, автоматизація й реагування системи безпеки (SOAR), системи виявлення вторгнень (IDS).

За успішного встановлення сесії, здійснюється її контроль. Одним із рішень є «безперервна оцінка доступу» (CAE, Continuous Access Evaluation), коли дійсність токена сесії визначається надійністю і цілісністю сесії та може бути перервана в будь-який момент. Рішення про термінацію сесії приймаються під час «діалогу» між сервісом, що видав токен, і ресурсом, до якого видано токен. Ресурс може зафіксувати певні зміни характеристик зв'язку і відповідно повідомити сервісу видачі токенів, який у свою чергу термінує сесію (проте з можливою часовою затримкою). Альтернативним підходом є використання біометрики для забезпечення «безперервної» оцінки доступу, що називається «поведінкова багатофакторна аутентифікація». У цьому методі дійсність токена сесії обмежена часовими рамками, при припинені дії токена, користувач повинен повторно автентифікуватись. ПЗ, використовуючи машинне навчання та пасивну біометрію, створює унікальний поведінковий профіль для кожного користувача. Тобто, після створення поведінкового профілю, підтвердження особи користувача та автентифікація відбувається не за тим, що він робить, а за тим, *як* він це робить, генеруючи рівень довіри для кожної взаємодії у фоновому режимі. Цей показник використовується для динамічного аналізу поведінки користувача і дає змогу або автоматично аутентифікувати його без перебоїв у сесії, або відмітити підозрілу поведінку та повернутись до MFA.

Забезпечення контролю ідентичностей пов'язане з багатьма можливими реалізаціями. Одним із важливих аспектів у нульовій довірі є ідентифікація користувачів та пристроїв. В сучасних рішеннях особливу увагу приділяють тому, щоб ідентифікація була не лише надійною, але й ефективною з точки зору продуктивності та зручності.

Поведінкова багатофакторна автентифікація (Behavioral MFA): система аналізує дії користувача протягом сесії, його поведінкові патерни: як він натискає клавіші, рухає мишкою або використовує мобільні пристрої. Після створення поведінкового профілю кожного користувача система може аутентифікувати його не лише на основі того, що він робить, але і як саме він це робить. Це дає можливість динамічно підвищувати або знижувати рівень довіри під час сесії.

MFA: поєднує кілька рівнів підтвердження: щось, що користувач знає (пароль), щось, що він має

(смартфон, токен), та щось, чим він є (біометричні дані). Біометричні методи (відбитки пальців, розпізнавання обличчя, голосу) забезпечують високий рівень безпеки, але можуть викликати затримки через необхідність їхньої обробки.

Безпарольна автентифікація (Passwordless Authentication): знижує ризик крадіжки паролів, базується на фізичних пристроях, таких як USB-ключі з підтримкою стандарту FIDO2 (наприклад, YubiKey), або на біометричних даних, які автоматично підтверджують особу користувача. Безпарольні рішення також можуть включати використання одноразових кодів або push-сповіщень, що знижує залежність від паролів, підвищуючи безпеку.

Комбінація фізичних пристроїв та біометрії: фізичні пристрої (флешки або смарт-карти) можуть бути поєднані з біометричними методами автентифікації. Це підвищує рівень безпеки завдяки двом різним типам ідентифікації: фізичному об'єкту та біометрії. Такий підхід надає більше захисту порівняно з використанням лише одного методу.

Сервіси автентифікації: Okta, Auth0 та Microsoft Azure Active Directory, пропонують інструментарій для керування ідентичностями та доступом. Вони підтримують як MFA, так і безпарольну автентифікацію, інтегруючись з іншими корпоративними системами дозволяють автоматизувати управління доступом [24–26], покращити контроль за ідентифікаціями користувачів та процесів, запровадити динамічну аутентифікацію.

Дослідження прогалин у існуючих технологіях та пошук рішень. Проблема_1: Ненадійність традиційних підходів до безпеки критичної інфраструктури. Характеристика: Традиційні моделі безпеки, що ґрунтуються на периметровому захисті та довірі до внутрішніх мереж, більше не відповідають вимогам безпеки сучасної критичної інфраструктури, яка все частіше зазнає нових кіберзагроз і атак. Рішення: Впровадження парадигми ZT –кожен запит на доступ перевіряється незалежно від його джерела, завдяки чому всі користувачі та пристрої проходять автентифікацію та авторизацію перед отриманням доступу до ресурсів.

Проблема_2: Виклики автентифікації та контролю доступу в ZT Architectures (ZTA). Характеристика: Сучасні механізми автентифікації та контролю доступу стикаються з труднощами в інтеграції в ZT, що може знижувати ефективність та надійність захисту при реалізації ZTA. Рішення: Використання новітніх методів автентифікації та контролю доступу, зокрема MFA та поведінкових моделей автентифікації, що дозволяє забезпечити точний і динамічний контроль доступу.

Проблема_3: Недостатня сегментація мережі та управління трафіком. Характеристика: Відсутність належної мікросегментації у традиційних мережах дозволяє порушникам вільно пересуватися після проникнення, що підвищує ризик компрометації критичних ресурсів. Рішення: Реалізація мікросегментації з використанням технологій, таких як Software-Defined Perimeter (SDP), яка дозволяє динамічно контролювати рух трафіку та обмежувати доступ між сегментами мережі, підвищуючи загальний рівень захисту.

Проблема_4: Автоматизація безпеки та обробка загроз у режимі реального часу. Характеристика: Сучасні системи безпеки не завжди забезпечують належну автоматизацію, що ускладнює своєчасну реакцію на загрози та управління ризиками в реальному часі. Рішення: Впровадження рішень для автоматизації безпеки, включаючи інструменти моніторингу та аналізу загроз, що дозволяє швидше і точніше оцінювати ризики, виявляти загрози та обмежувати потенційні атаки в реальному часі.

Проблема_5: Відсутність вимог до подальших досліджень та інновацій для ZT. Характеристика: Для успішного впровадження ZT у критичну інфраструктуру необхідні подальші дослідження щодо вдосконалення моделей довіри та підходів до динамічного управління ризиками. Рішення: Ідентифікація напрямків майбутніх досліджень, які включають розвиток технологій для обчислення рівня довіри та оптимізації політик контролю доступу, що забезпечить можливість гнучкого застосування ZT у критичних системах.

Проблеми, що виокремили в цій статті саме ми:

Проблема_6: "Сплеск" ідентичностей у SaaS застосунках Характеристика: Використання неінтегрованих SaaS додатків для виконання робочих завдань є поширеною практикою, що передбачає створення облікового запису, зазвичай з електронною поштою і паролем. Проте на одного працівника може припадати багато подібних облікових записів, що часто захищені простим паролем, це дозволяє зловмисникові з правильно підібраним ключем отримати доступ до конфіденційних даних у SaaS додатку та залишатись непоміченим довгий період часу. Рішення: Усунення людського фактора при створенні паролів у SaaS застосунках, використовуючи менеджера ідентичностей, або застосування MFA чи безпарольної аутентифікації.

Проблема_7: Ризики пов’язані з ланцюгом поставок не є охопленими. Характеристика: Послуги SaaS стали новими будівельними

блоками, що створюють низку систем, пов'язаних різними мережами та інтерфейсами. Проте здійснити аутентифікацію та авторизацію кожного суб'єкта й об'єкта, залученого до ланцюга поставок, не можливо через велику кількість учасників і динамічний характер подій. Рішення: Сегментація ланцюга поставок, використовуючи локальні політики нульової довіри; при виявленні ризику на одному із сегментів, інші учасники обов'язково проінформовані про подію, а з'єднання обмежене чи перерване.

Висновки

У цій статті представлено огляд сучасних методів забезпечення кібербезпеки корпоративних мереж на концепції нульової довіри. Розглянуто фундаментальні принципи ZT, її ключові переваги та основні виклики, з якими стикаються організації під час її впровадження. Аналіз дав змогу виділити найефективніші стратегії для захисту даних та запобігання кіберзагрозам, що робить ZT важливим підходом до кібербезпеки в умовах сучасних загроз.

Наукова цінність роботи полягає в узагальненні та систематизації сучасних підходів до забезпечення безпеки інформаційних систем на основі моделі нульової довіри – ZTM, а також у виявленні основних переваг і обмежень її застосування в корпоративних мережах. Дослідження підкреслює перспективні напрямки розвитку концепції ZT з акцентом на потреби критичної інфраструктури, що постійно зазнає зростаючого тиску кіберзагроз.

Практична цінність роботи полягає в можливості застосування отриманих результатів для розробки та впровадження ефективних систем безпеки, орієнтованих на захист корпоративних мереж від внутрішніх і зовнішніх загроз. Викладені рекомендації можна реалізувати і в різних установах для забезпечення цілісного захисту даних.

Аналіз підтверджує, що традиційні моделі захисту не відповідають актуальним загрозам, обумовленим використанням хмарних сервісів, віддаленим доступом та зростаючою складністю мережевих інфраструктур. З'ясовано, що ZTM повністю відмовляється від концепції апріорної довіри до будь-яких елементів системи і фокусується на детальному контролі доступу через постійну автентифікацію та авторизацію всіх запитів, що суттєво знижує ризики НСД. Ключові аспекти ZT включають принцип найменших привілеїв і акцент на безперервному моніторингу та аналізі поведінки користувачів, що дав змогу оперативно виявляти підозрілі дії та реагувати на них. Використання MFA і безперервної оцінки сесій підвищує рівень контролю та мінімізує ризики НСД.

Проте перехід до ZTM супроводжується значними викликами, що потребують модернізації архітектури, впровадження автоматизованих політик контролю доступу та адаптації систем до динамічної авторизації й автентифікації. Це, у свою чергу, потребує інвестицій, оновлення підходів до управління безпекою та адаптації до можливих проблем продуктивності, викликаних підвищеним навантаженням на обчислювальні ресурси.

Впровадження ZT потребує глибокої модернізації інфраструктури, автоматизації політик доступу і пристосування до зростаючого навантаження на системи. Збільшення використання SaaS-додатків створює нові вразливості в цифрових ланцюгах постачання. Як перспективне рішення запропоновано використання динамічних ідентичностей, де посередники можуть забезпечувати безпечне з'єднання та контроль доступу, що сприяє зниженню ризиків у складних та динамічних мережах.

Список літератури:

1. Zero Trust Architecture (ZTA): A Comprehensive Survey / [N. F. Syed, S. W. Shah, A. Shaghaghi та ін.]//IEEE Access. 2022. №10. С. 57143–57179.
2. Zero Trust Security Paradigm: A Comprehensive Survey and Research Analysis / Journal of Electrical Systems. 2023. №19(2). С. 28–37.
3. 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. №27. С. 101227.
4. 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. №18(9). С. 2665–2691.
5. Pooja S., Chandrakala C. Secure Reviewing and Data Sharing in Scientific Collaboration: Leveraging Blockchain and Zero Trust Architecture / IEEE Access. 2024. №12. С. 92386–92399.
6. ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Ensuing Usage Control Model / [S. Ameer, L. Praharaj, R. Sandhu та ін.] // ACM Transactions on Privacy and Security. 2024. №27(3). С. 22.
7. Toward a modern secure network based on next-generation firewalls: recommendations and best practices / [O. Lamdakkar, I. Ameur, M. M. Eleyatt та ін.] // Procedia Computer Science. 2024. №238. С. 1029–1035.
8. Web-Biometrics for User Authenticity Verification in Zero Trust Access Control / [T. Sasada, Y. Taenaka, Y. Kadobayashi та ін.] // IEEE Access. 2024. №12. С. 129611–129622.

9. A Micro-Segmentation Method Based on VLAN-VxLAN Mapping Technology / [D. Li, Z. Yang, S. Yu та ін.] // Future Internet. 2024. №16. С. 320.

10. Zero Trust Architecture [Електронний ресурс] / S.Rose, O. Borchert, S. Mitchell, S. Connelly // COMPUTER SECURITY. 2020. Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

11. Automation and Orchestration of Zero Trust Architecture: Potential Solutions and Challenges / [Y. Cao, S. Pokhrel, Y. Zhu та ін.] // Machine Intelligence Research. 2024. №21. С. 294–317.

12. Концепція нульової довіри для захисту Active Directory для виявлення програм-вимагачів / [Д. Журавчак, П. Глущенко, М. Опанович та ін.] // Кібербезпека: освіта, наука, техніка. 2023. №2(22).

13. Єсін В., Вілігура В., Узлов Д. Огляд існуючих моделей та основних принципів нульової довіри / Радіотехніка. 2024. №2(217). С. 39–54.

14. Єсін В., Вілігура В., Сватовський І. Забезпечення безпеки у розподілених інформаційних системах: основні аспекти / Радіотехніка. 2023. №3(214). С. 32–64.

15. Опанович М. Аналіз кібератак та діяльності APT груп в Україні / Кібербезпека: освіта, наука, техніка. 2024. №4(24). С. 172–184.

16. Проблематика і підходи підвищення рівня захисту в каналах передачі даних систем і пристроїв Інтернету речей / В. І.Маліновський, Л. М. Куперштейн, В. В. Лукічов, В. В. Дудатьєв. // Вісник Вінницького політехнічного інституту. 2024. №4. С. 105–115.

17. Іскрижицький А., Задорожній А. Дослідження наявних методів та технологій для децентралізованого зберігання та адміністрування публічних даних / Технічні науки та технології. 2024. №2(36). С. 137–150.

18. Zero Trust Steps Up to Shut Down Threat Actors [Електронний ресурс] // ThreatConnect – Режим доступу до ресурсу: https://threatconnect.com/blog/zero-trust-steps-up-to-shut-down-threat-actors.

19. Zero Trust Architecture [Електронний ресурс] // ColorTokens – Режим доступу до ресурсу: colortokens.com/blogs/zero-trust-architecture/.

20. Zero Trust Cybersecurity: 'Never Trust, Always Verify.' [Електронний ресурс] // NIST – Режим доступу до ресурсу: https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify.

21. Zero Trust Architecture Project Description [Електронний ресурс] // NCCoE – Режим доступу до ресурсу: https://www.nccoe.nist.gov/sites/default/files/legacy-files/zta-project-description-final.pdf.

22. Phiayura S., Teerakanok A. A Comprehensive Framework for Migrating to Zero Trust Architecture / IEEE Access. 2023. №11. С. 19487–19511.

23. Zero Trust Implementation Guide [Електронний ресурс] // Google Services – Режим доступу до ресурсу: https://services.google.com/fh/files/misc/zt_implem_guide_800_27.pdf.

24. Silva G., Macedo D., Santos A.. Zero Trust Access Control with Context-Aware and Behavior-Based Continuous Authentication for Smart Homes / Anais do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. 2021. С. 43–56.

25. Захарченко С. М., Трояновська Т. І., Бойко О. В.. Побудова захищених мереж на базі обладнання компанії Cisco. Вінниця: ВНТУ, 2017. 133 с.

26. Коробейнікова Т. І., Захарченко С. М. Технології захисту локальних мереж на основі обладнання CISCO / Львів: Видавництво Львівської політехніки, 2021. 232 с.

References:

1. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access*, *10*, 57143–57179. https://doi.org/10.1109/access.2022.3174679.

2. Ashfaq, E. a. S. (2024). Zero Trust Security Paradigm: A Comprehensive Survey and Research Analysis. *Deleted Journal*, *19*(2), 28–37.https://doi.org/10.52783/jes.688.

3. Azad, M. A., Abdullah, S., Arshad, J., Lallie, H., & Ahmed, Y. H. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*, *27*, 101227. https://doi.org/10.1016/j.iot.2024.101227.

4. Kim, Y., Sohn, S., Kim, K. T., Jeon, H. S., Lee, S., Lee, Y., & Kim, J. (2024). Exploring Effective Zero Trust Architecture for Defense Cybersecurity: A Study. *KSII Transactions on Internet and Information Systems*, *18*(9). https://doi.org/10.3837/tiis.2024.09.011.

5. Mukta, R., Pal, S., Hitchens, M., Paik, H., & Kanhere, S. S. (2024). Poster: Zero Trust Driven Architecture for Blockchain-Based Access Control Delegation. *Zero Trust Driven Architecture for Blockchain-Based Access Control Delegation*, 48–50. https://doi.org/10.1145/3672202.3673737.

6. Ameer, S., Praharaj, L., Sandhu, R., Bhatt, S., & Gupta, M. (2024). ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Ensuing Usage Control Model. *ACM Transactions on Privacy and Security*. https://doi.org/10.1145/3671147.

7. Lamdakkar, O., Ameur, I., Eleyatt, M. M., Carlier, F., & Ibourek, L. A. (2024). Toward a modern secure network based on next-generation firewalls: recommendations and best practices.

Procedia Computer Science, *238*, 1029–1035. https://doi.org/10.1016/j.procs.2024.06.130.

8. Sasada, T., Taenaka, Y., Kadobayashi, Y., & Fall, D. (2024). Web-Biometrics for User Authenticity Verification in Zero Trust Access Control. *IEEE Access*, 1. https://doi.org/10.1109/access.2024.3413696.

9. Li, D., Yang, Z., Yu, S., Duan, M., & Yang, S. (2024). A Micro-Segmentation Method Based on VLAN-VxLAN Mapping Technology. *Future Internet*, *16*(9), 320. https://doi.org/10.3390/fi16090320.

10. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. https://doi.org/10.6028/nist.sp.800-207.

11. Cao, Y., Pokhrel, S. R., Zhu, Y., Doss, R., & Li, G. (2024). Automation and Orchestration of Zero Trust Architecture: Potential Solutions and Challenges. *Deleted Journal*, *21*(2), 294–317. https://doi.org/10.1007/s11633-023-1456-2.

12. Zhuravchak, D., Hlushchenko, P., Opanovych, M., Dudykevych, V., & Piskozub, A. (2023). Zero Trust concept for active directory protection to detect ransomware. *Cybersecurity Education Science Technique*, *2*(22), 179–190. doi.org/10.28925/2663-4023.2023.22.179190.

13. Yesin, V., Vilihura, V., & Uzlov, D. (2024c). Review of existing models and basic Zero Trust principles. *Radiotekhnika*, *217*, 39–54. https://doi.org/10.30837/rt.2024.2.217.03

14. Yesin, V., Vilihura, V., & Svatowsky, I. (2023). Ensuring security in distributed information systems: major aspects. *Radiotekhnika*, *214*, 32–64. https://doi.org/10.30837/rt.2023.3.214.04

15. Opanovych, M. (2024). Analysis of cyber attacks and the activities of apt groups in Ukraine. *Cybersecurity Education Science Technique*, *4*(24), 172–184. https://doi.org/10.28925/2663-4023.2024.24.172184.

16. Malinovskyi, V. I., Kupershtein, L. M., Lukichov, V. V., & Dudatiev, A. V. (2024). Problematyka i pidkhody pidvyshchennia rivnia zakhystu v kanalakh peredachi danykh system i prystroiv Internetu rechei [Challenges and approaches for increasing the level of security in data transmission channels of IoT systems and devices]. *Visnyk Vinnytskoho politekhnichnoho instytutu*, 4, 105–115.

17. Iskryzhytskyi, A., & Zadorozhnii, A. (2024). Doslidzhennia naiavnykh metodiv ta tekhnolohii dlia detsentralizovanoho zberihannia ta administruvannia publichnykh danykh [Research of existing methods and technologies for decentralized storage and administration of public data]. *Tekhnichni nauky ta tekhnolohii – Technical Sciences and Technologies*. № 2(36). 137–150. doi.org/10.25140/2411-5363-2024-2(36)-137-150.

18. *Zero Trust Steps Up to Shut Down Threat Actors*. (n.d.). threatconnect.com. Retrieved November 1, 2024, from https://threatconnect.com/blog/zero-trust-steps-up-to-shut-down-threat-actors/.

19. *Zero Trust Architecture*. (n.d.). colortokens.com. Retrieved October 28, 2024, from colortokens.com/blogs/zero-trust-architecture/.

20. *Zero Trust Cybersecurity: 'Never Trust, Always Verify.'* (n.d.). www.nist.gov. Retrieved October 26, 2024, from https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify.

21. *Implementing a Zero Trust architecture*. (2020, October). www.nccoe.nist.gov. Retrieved September 30, 2024, from https://www.nccoe.nist.gov/sites/default/files/legacy-files/zta-project-description-final.pdf.

22. Phiayura, P., & Teerakanok, S. (2023). A Comprehensive Framework for Migrating to Zero Trust Architecture. *IEEE Access*, *11*, 19487–19511. https://doi.org/10.1109/access.2023.3248622

23. *Applying Zero Trust on Google Cloud*. (n.d.). Retrieved October 9, 2024, from https://services.google.com/fh/files/misc/zt_implem_guide_800_27.pdf.

24. Da Silva, G. R., Macedo, D. F., & Santos, A. L. D. (2021). Zero Trust Access Control with Context-Aware and Behavior-Based Continuous Authentication for Smart Homes. *Anais Do Simpósio Brasileiro De Segurança Da Informação E De Sistemas Computacionais*, 43–56. https://doi.org/10.5753/sbseg.2021.17305.

25. Zakharchenko, S. M., Troianovska, T. I., & Boiko, O. V. (2017). *Pobudova zakhyshchenykh merezh na bazi obladnannia kompanii Cisco.* Vinnytsia: VNTU.

26. Korobeinikova T. I. & Zakharchenko S. M. (2021) *Tekhnolohii zakhystu lokalnykh merezh na osnovi obladnannia CISCO*. Lviv: Vydavnytstvo Lvivskoi politekhniky.

Науково-методична стаття.
Надійшла до редакції 12.11.2024.
Прийнято до публікації 18.12.2024.