KAPITEL 7 / *CHAPTER 7* [7]
THE ZERO TRUST MODEL: THEORY, PRACTICE, AND PROSPECT

DOI: 10.30890/2709-2313.2025-37-01-006

Вступ

З постійним ростом загроз інформаційних та фізичних систем, звичні моделі захисту, що передбачають наявність контрольованої зони та довірених користувачів і ресурсів, не здатні задовольнити в повній мірі вимоги щодо їх безпеки. Звично побудова інформаційних систем передбачає існування внутрішньої (контрольованої, безпечної) та зовнішньої (небезпечної) зон. Безпека внутрішньої зони досягається використанням міжмережевих екранів, систем виявлення і запобігання вторгнень для захисту від зовнішніх загроз, а вже аутентифіковані об'єкти та суб'єкти внутрішньої зони отримують, залежно від застосовуваних політик розмежування доступу, ті чи інші права та дозволи. Проте у сучасних мережах часто користувачі та ресурси знаходяться за межами контрольованої зони чи не належать до неї, як приклад: хмарні сервіси, програмне забезпечення як послуга, віддалені працівники чи працівники, що доступаються до організаційних ресурсів з особистих пристроїв. Ці явища унеможливлюють створення контрольованої зони та забезпечення надійності внутрішньої зони. Відповідно, успішно проникнувши у систему чи так звану безпечну зону, порушник здатний перебувати в ній необмежену кількість часу, несанкціоновано доступатись до системних ресурсів, переміщуватись по мережі та, використовуючи різноманітні методи і засоби, збільшувати свої привілеї. У серпні 2020 року Національним інститутом стандартів та технологій було опубліковано стандарт NIST SP 800-207, що описує інноваційну модель побудови інформаційних систем – безпека нульової довіри. Дана модель зосереджена на захисті всіх мережевих ресурсів та заснована на ідеї, що довіра ніколи не гарантується. З метою дослідження цієї моделі, вважається, що певна невідома кількість зловмисників уже присутня в мережі.

---

[7]***Authors:*** *Korobeinikova Tetiana Ivanivna*
Number of characters: *46051*
Author's sheets: *1,15*

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

Об'єктом дослідження є інформаційні системи корпоративних мереж, що функціонують у сучасному кіберпросторі, з акцентом на забезпеченні їх безпеки.

Предметом дослідження є методи й технології забезпечення безпеки корпоративних інформаційних систем, які базуються на концепції нульової довіри, а також їх впровадження для захисту даних і запобігання несанкціонованому доступу.

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 периметрових підходах, 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 дозволяє їм отримати неконтрольований доступ до даних і критичних ресурсів.

7.1. Аналіз останніх досліджень і публікацій

Упродовж останніх років концепція "нульової довіри" (Zero Trust) привертає увагу дослідників і практиків як потенційно більш ефективний підхід до забезпечення кібербезпеки [1–2]. Багато наукових праць присвячено принципам Zero Trust, зокрема його архітектурі [3–4] та основним компонентам, таким як автентифікація та авторизація користувачів [5–6], динамічний контроль доступу [7], багатофакторна автентифікація (MFA) та сегментація мережі [8–9].

Стандарти, як-от NIST SP 800-207, пропонують докладні настанови щодо реалізації Zero Trust, що стимулює подальше вивчення та впровадження цієї моделі [10–11].

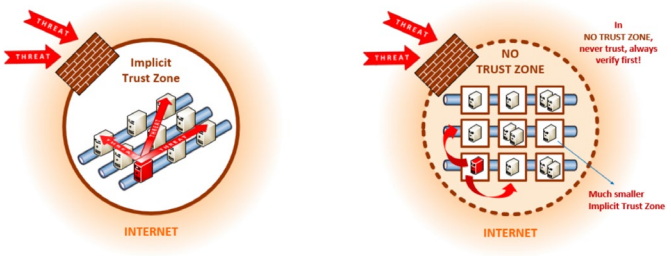
В Україні питаннями принципу нульової довіри в корпоративних мережах активно займаються Журавчак Д., Глущенко П., Опанович М., Дудикевич В., Піскозуб А. і в своїй роботі [12] розвивають підхід до захисту Active Directory від загроз, пов'язаних з програмами-вимагачами, що стають все більш надзвичайно небезпечними для корпоративних інформаційних систем. Вчені А. Єсін, В., Вілігура, В. та ін.і в [13–14] досліджують про теоретичний та практичний потенціал принципу нульової довіри; сучасні виклики та підходи щодо стратегії захисту від APT атак, з особливим фокусом на архітектурі нульової довіри 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 і інформаційних системах Інтернету речей; питаннями впровадженню децентралізованих технологій для зберігання даних із застосуванням принципів нульової довіри прцюють Іскрижицький, А. та Задорожній, А. в [17].

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

7.2. Модель безпеки нульової довіри

Головною метою моделі безпеки нульової довіри (ZTM, zero trust model) є

запобігання несанкціонованому доступу до даних та сервісів, створення максимально деталізованого контролю доступу. Основна увага приділяється автентифікації, авторизації усіх процесів та зменшенню кількості зон умовної довіри, створюючи безпечну та ефективну мережу.



а) б)

Рисунок 1 Відмінності традиційної мережі (а) і мережі з ZTM (б)

Авторська розробка на основі [1–4]

Для досягнення поставленої у роботі мети оглянемо стандарт NIST SP 800-207, і відобразимо аналітичний огляд у таблиці 1.

Таблиця 1 – Порівняння моделей безпеки з використанням контрольованої зони та нульової довіри

З використання контрольованої зони	*З використанням нульової довіри*
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

1) Ресурсами вважаються усі джерела даних та інформаційно-обчислювальні сервіси/системи (всі пристрої та програми, що можуть отримати доступ до даних, мають бути захищеними).
2) Уся комунікація підлягає захисту незважаючи на розташування задіяних ресурсів у мережі. Тобто активність, що відбувається навіть на пристроях організації, налаштованих організацією та, які знаходяться у її ж мережі, все одно повинна пройти всі необхідні перевірки, а конфіденційність та цілісність комунікації – захищені.
3) Доступ до кожного ресурсу в мережі надається на сесійній основі і тільки після перевірки користувача/процесу. Доступ надається 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 за допомогою динамічної політики, що враховує поточний стан ідентичності користувача/процесу, програми/сервісу та ресурсу, 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) Усі власні і орендовані ресурси знаходяться під постійним контролем, і жодний ресурс не вважається надійним "за замовчуванням". Здійснюється постійний контроль за ресурсами після їх розгортання та початкових налаштувань з метою своєчасного виявлення та усунення несправностей. 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 щодо стану ресурсів, інфраструктури, комунікацій, та використовується для посилення безпеки. Дана інформація повинна документуватись і використовуватись для покращення діючих політик безпеки і оцінки ризиків при наданні доступу.

7.3. Актори ZTM

У моделі безпеки нульової довіри всі об'єкти і суб'єкти, які взаємодіють між собою в мережі мають бути захищеними. Вирізняють 5 основних категорій сутностей, до яких слід застосовувати принципи даної моделі (ідентичності, обладнання, програми, інфраструктура та мережі, дані.

Ідентичностями можуть бути користувачі, сервіси, обладнання, що мають ресурси для успішного проходження ідентифікації та авторизації, а також призначені їм атрибути та привілеї 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 або ж бути власністю користувачів і клієнтів, і до них також застосовуються принципи ZTM, якщо з них здійснюється доступ до ресурсів організації. 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, характерні для конкретних 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 є класифікацією, маркуванням та шифруванням даних і передбачається під час усіх операцій здійснюваних над даними, незалежно від того чи здійснюється це локально, чи використовуючи орендовані ресурси, а також використання механізмів для виявлення та припинення витоку даних.

Застосування політик безпеки нульової довіри до всіх об'єктів і суб'єктів створює несприятливі умови для здійснення несанкціонованого доступу до ресурсів організації. Навіть при отриманні несанкціонованого доступу, усі дії зловмисника фіксуються і обробляють, 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 несанкціонованих дії, навіть, якщо зловмисник вже добре ознайомлений з структурною організації мережі при атаках типу програма-вимагач, спробах зміни налаштувань засобів безпеки чи компонентів мережі, зміни/видалення/модифікації/викрадення даних.

7.4. 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) [5].

Архітектура нульової довіри (Zero Trust Architecture, ZTA) 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 [6].

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 2 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 [2].

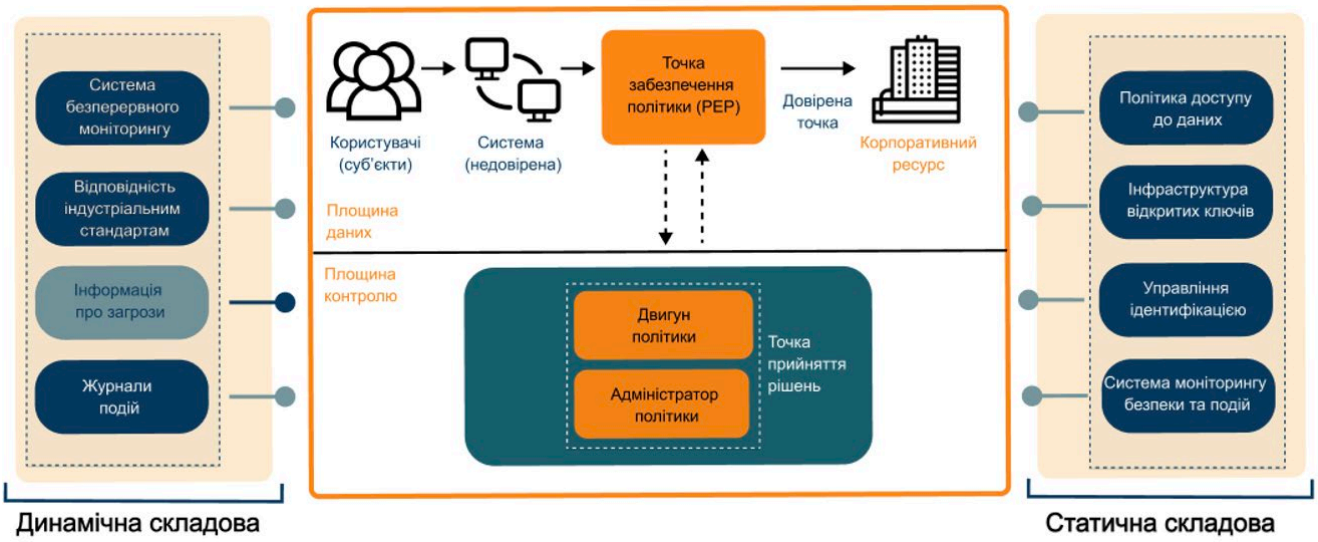


Рисунок 2 – Логічні компоненти ZT

Авторська розробка на основі [2, 7, 8]

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, 19].

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, 19].

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, 20, 21]. Передача даних між суб'єктом і мережевими ресурсами відбувається в площині даних, яка охоплює площину суб'єкта.

Оскільки архітектура ZTA охоплює широкий спектр випадків використання додатків, процес автентифікації більше не обмежується перевіркою ідентичності користувача, але також включає 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, 22].

7.5. Виклики, пов'язані із недотриманням принципів нульової довіри.

Дотримання принципів нульової довіри пов'язане із багатьма труднощами. CISA [19] 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 в передбачає ряд труднощів під час переходу від моделі безпеки на основі контрольованої до ZTM:

1. Використання застарілої архітектури, що часто відображає єдину мережу, де комунікація між ресурсами не є контрольованою та не завжди передбачає відповідний рівень безпеки. Подібні застарілі системи не здатні запобігти несанкціонованому руху між ресурсами мережі.
2. Створення нової політики контролю безпеки, що передбачає динамічну автоматизацію.
3. Потреба в ідентифікації та динамічній авторизації вимагає більш

комплексного підходу, пов'язаного з мінливим станом системи та параметрів ресурсів.

7.6. Кращі практики сучасного світу

Одним з найважливіших аспектів нульової довіри є визначення ресурсів, що мають бути захищені, а саме: 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 архітектури нульової довіри та створення нових політик безпеки. Надалі передбачається проведення постійного контролю, підтримки і оновлення. Даний підхід був описаний аналітиком з Forrester Research Джоном Кіндервагом (John Kindervag) та наведений на рисунку 3 [23].

Тут ключовим підходом до побудови ZTA є використання мікросегментації і для цього використовується технологія VLAN. 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 VLAN'ами можливий виключно тоді, якщо явно заданий у конфігурації, а одна VLAN не може бути каналом зв'язку між іншими VLAN'ами.

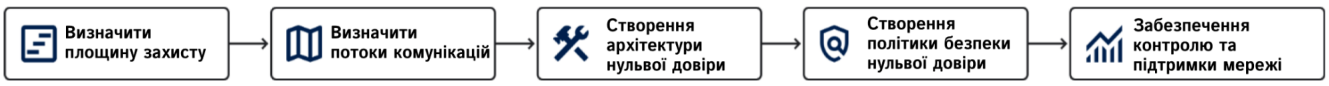


Рисунок 3 – Підхід впровадження ZTM

Авторська розробка на основі [23]

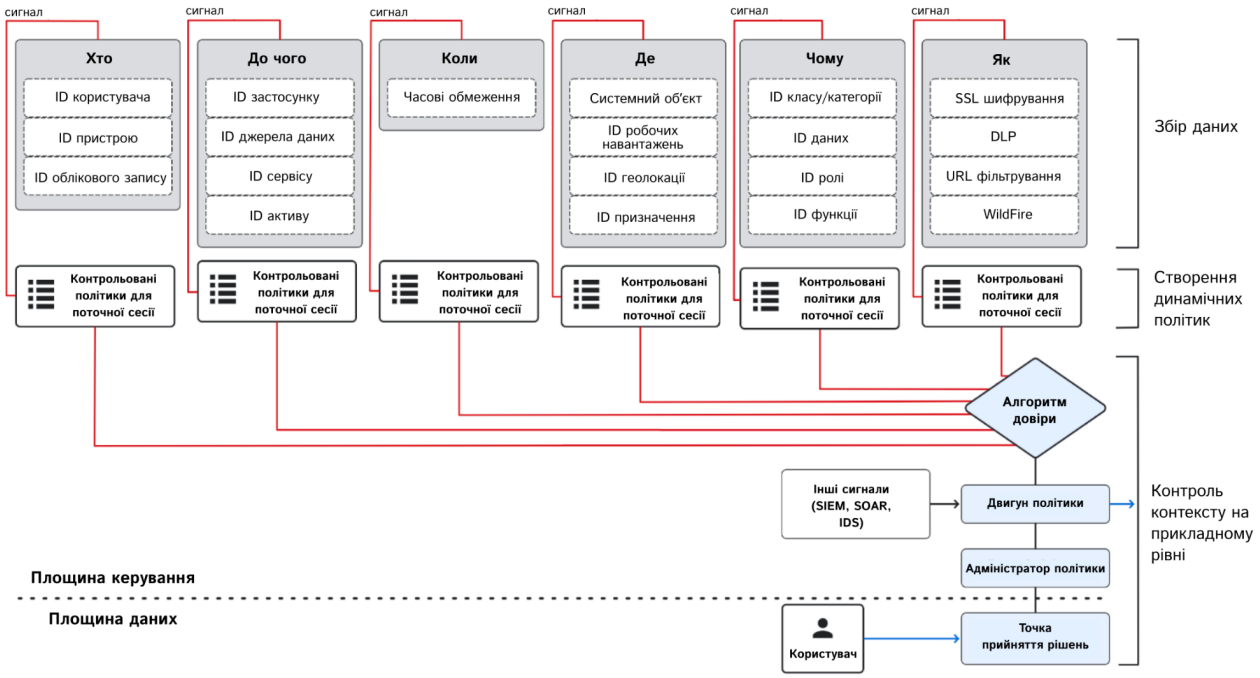
Додатково розгортання мережі передбачає використанням технології Hub&Spoke, де з'єднання між мережами можливе виключно напряму. Усі комунікації шифруються відповідними протоколами та контролюються на 3-4 рівнях моделі TCP/IP. Даний метод передбачає безпечну шифровану

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 4), що стає основою для створення динамічних політик безпеки, які в свою чергу використовуються алгоритмом довіри [23, 24].

Як видно з рисунку 4, 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" (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.



Raouda, Hani. (2023). Zero Trust context aware authorization . Retrieved June 10, 2023

Рисунок 4 – Приклад механізму авторизації

Авторська розробка на основі [23, 24]

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) [25, 26]. Альтернативним підходом є використання біометрики для забезпечення "безперервної оцінки доступу", що називається "поведінкова багатофакторна аутентифікація". У даному 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 довіри використовується безперервно для динамічного аналізу поведінки користувача і дозволяє або автоматично аутентифікувати його без перебоїв у сесії, або відмітити підозрілу поведінку та повернутись до багатофакторної аутентифікації.

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): Це підхід, при якому система аналізує дії користувача протягом сесії, зокрема 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 дозволяє динамічно підвищувати або знижувати рівень довіри під час сесії.

Багатофакторна автентифікація (MFA): Багатофакторна автентифікація вже стала стандартом для забезпечення безпеки. Вона 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): Ця технологія стає все більш популярною, оскільки вона знижує ризик крадіжки паролів. Безпарольна автентифікація 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 пуш-сповіщень, що дозволяє знижувати залежність від паролів, підвищуючи безпеку.

Комбінація фізичних пристроїв та біометрії: у деяких випадках організації впроваджують комбіновані рішення. Наприклад, фізичні пристрої (флешки або смарт-карти) можуть бути поєднані з біометричними методами автентифікації. Це підвищує рівень безпеки за рахунок двох різних типів ідентифікації: фізичного об'єкта та біометрії. Такий підхід надає більше захисту в порівнянні з використанням лише одного методу. Сервіси автентифікації: сучасні сервіси автентифікації, такі як Okta, Auth0 та Microsoft Azure Active Directory, пропонують широкий набір інструментів для керування ідентичностями та доступом. Вони підтримують як MFA, так і безпарольну автентифікацію, інтегруючись з іншими корпоративними системами. Ці сервіси дозволяють організаціям автоматизувати управління доступом, покращити контроль за ідентифікаціями користувачів та процесів, а також запровадити динамічну аутентифікацію.

7.7. Дослідження прогалин у існуючих технологіях та пошук рішень

У сучасних ZTA центральну роль виконує важливий компонент системи безпеки (Policy Engine, PE), який здійснює керування доступом на основі оцінки рівня довіри користувачів та пристроїв. Одним з основних недоліків можна

виокремити централізовану модель прийняття рішень, що створює потенційну точку відмови, оскільки збої у роботі PE або помилки в алгоритмах довіри можуть спричинити серйозні порушення доступу до критично важливих ресурсів. Без надійної стратегії резервного копіювання та відновлення залежність від одного вузла становить значний ризик, оскільки може призвести до необґрунтованого блокування доступу для авторизованих користувачів або надання несанкціонованого доступу стороннім суб'єктам.

Водночас безпосередньо розробка PE потребує організації підходу для забезпечення повної ефективності та надійності системи. Надмірно жорсткі обмеження створюють перешкоди для виконання процесів, тоді як більш ліберальні політики підвищують ризик небажаного доступу. Налаштування PE – це довготривалий та складний процес, оскільки потребує значних часових і ресурсних витрат, залучення висококваліфікованих спеціалістів, що ускладнює реалізацію у великих організаціях.

Недостатній баланс між зручністю використання та безпекою є однією з основних причин несправності систем безпеки та викликом для організацій, які запроваджують ZTA сьогодні. Можна спостерігати конфлікт між підходом до безпеки та комфортом для IT-відділів та користувачів. Забезпечення безпеки – це важка робота як з точки зору користувача, так і з точки зору архітектури, але вона не повинна перешкоджати зручності використання та підтримувати хорошу взаємодію з користувачем. З одного боку, підвищена безпека передбачає постійні перевірки, багатофакторну автентифікацію та обмежений доступ до систем. З іншого боку, для IT-підрозділів та користувачів зручніше мати доступ до ресурсів без складних перевірок.

Одним із вирішень цієї проблеми є використання довготривалих стратегій імплементації моделі нульової довіри. Проте важливо передбачити в ній тренінги для звичайного персоналу, тобто кінцевих користувачів системи. Тренінги повинні ознайомлювати працівників з новими правилами та політиками безпеки, а також надавати поради щодо уникнення труднощів через інтеграції нового функціоналу.

Багато організацій продовжують використовувати традиційні моделі периметрової безпеки та на даному етапі не готові від них відмовитися. Однак інтеграція периметрових рішень із хмарними середовищами, які є основою для нульової довіри, створює вразливості. Організації переходять на хмару через її різноманітні переваги – масштабованість, економічність і охоплення. Наприклад, невірна конфігурація доступу або помилки при розмежуванні прав можуть зробити мережу вразливою до атак. Це особливо актуально для великих організацій, які використовують гібридні інфраструктури.

Новітні системи безпеки вимагають постійної перевірки ідентичності користувачів, однак це може спричинити затримки та погіршити загальну продуктивність систем [27, 28]. MFA може потребувати значних обчислювальних ресурсів, що буде створювати додаткове навантаження на інфраструктуру, особливо у великих організаціях. У ZTA ідентифікація може стосуватися не лише користувачів або пристроїв, але й процесів (наприклад, служб або мікросервісів). Однак, якщо ці процеси не підтримують MFA або інші форми надійного підтвердження, це може створити серйозні вразливості. Недостатньо автентифіковані процеси можуть стати ціллю для зловмисників, що підвищує ризик компрометації.

Постійний моніторинг, перевірка доступу можуть впливати на загальну продуктивність системи. Затримки в обробці доступу мінімальні, але в масштабних системах, де одночасно обробляються сотні або тисячі запитів, це може стати серйозною проблемою.

Використання сигналів і методів, таких як метод Кіплінга, може підвищити ефективність інвентаризації в ZTA, однак існують суттєві недоліки в сучасних рішеннях, які варто враховувати.

По-перше, залежність від даних про поведінку користувачів і пристроїв може призвести до хибних висновків, якщо сигнали є не точними або неповними. Це може зашкодити організаціям, що розраховують на автоматизований аналіз, проте не зможуть швидко виявити аномалії або потенційні загрози. Таким чином, можна простежити сильну залежність від поведінкових даних.

По-друге, використання сигналів і методів може бути вразливим до атак та маніпуляцій з боку зловмисників. Зловмисники можуть намагатися змінити або сфальсифікувати поведінкові дані, щоб обійти систему безпеки. Якщо організація покладається на ці дані для прийняття рішень, це може призвести до помилкових висновків і ненадійних результатів.

Використання фреймворків, як MITRE ATT&CK – глобально доступна база знань про тактику і методи діяльності зловмисників, заснована на реальних спостереженнях, що надає структурований підхід до аналізу загроз і вразливостей, може допомогти в ідентифікації точок входу для зловмисників, проте вибір методу має бути адаптований до специфічних потреб організації, її ресурсів та типу інформації, яку потрібно захистити. Для максимізації ефективності MITRE ATT&CK має інтегруватися з іншими інструментами кібербезпеки, такими як SIEM-системи, засоби управління вразливостями та платформи Threat Intelligence.

Ідентифікаційні дані, а саме ідентичності, стали ключовим компонентом захисних систем на основі нульової довіри. Враховуючи паралельний перехід до технології SaaS (програма як послуга), працівники організацій почали використовувати широке різноманіття додатків, які допомагають виконувати їм робочі завдання. Дані застосунки можуть бути безкоштовними або з пробним періодом та зазвичай потребують для реєстрації тільки пошту та пароль, що призвело до явища “розростання ідентичностей”. Це створило величезні ризики для компаній, адже працівники використовують конфіденційні дані в цих несанкціонованих SaaS-додатках. Оскільки модель нульової довіри передбачає інвентаризацію всіх ресурсів, а в цьому сценарії організація не контролює кінцеву точку, метод аутентифікації або мережеве з'єднання. Відповідно для зловмисників з’явилась можливість отримати конфіденційні дані.

Прямолінійним рішенням цієї проблеми є встановлення чітких політик безпеки проти використання додатків, що не є інтегрованими у мережу організації. Досягти цього можна налаштувавши обмеження на використання корпоративних облікових записів. Якщо ж використовується корпоративний

пристрій для створення з'єднання, дану загрозу можна лімітувати використовуючи відповідно сконфігуровані міжмережеві екрани. Оптимальним рішенням є створення власних додатків для полегшення роботи або ж інтеграції вже існуючих у мережу. Як приклад, використання штучного інтелекту як ChatGPT набуло максимального поширення у всіх сферах діяльності. З метою захисту конфіденційних даних деякі організації вже працюють над створенням власного штучного інтелекту.

Стрімке зростання популярності SaaS-додатків, що стають будівельним блоками мережі нульової довіри, може призводити до труднощів у ланцюгах поставки. У цифровому ланцюгу поставок не завжди можливо здійснити автентифікацію та авторизацію кожного залученого суб'єкта через велику кількість учасників і динамічний характер взаємодій. Тобто організація може використовувати рішення створенні, як приклад, її партнером, проте він у свою чергу покладається на застосунки інших третіх сторін. Хоч мережі на основі нульової довіри передбачають розширення та динамічну інтеграцію, здатні вони реалізувати це виключно при інвентаризації всіх ресурсів. Також створення складних взаємодій може розширити площину атаки та створити нові поки невідомі вразливості.

Можливим рішенням цієї проблеми є створення динамічних і тимчасових ідентичностей. Організація-партнер, що є посередником між двома незалежними організаціями, виступає гарантом безпечного з'єднання. Кожна організація проводить моніторинг цілісності та надійності сесії на основі поведінкових атрибутів, таких як зміна джерела даних, зміна геолокації ресурсу в мережі і т.д. При виявленні однією з сторін підозрілих змін чи поведінки, спостереження передається посереднику, котрий термінує сесію. Паралельно організація-посередник здійснює автоматизований контроль за станом зв'язку з кожним із партнером. Це рішення передбачає застосування вже реалізованого методу Кіплінга між партнерами, а також методу Оно Таїті, що відомий за своїм принципом: "чому?". Нульова довіра передбачає, що довіра до одного ресурсу не гарантує довіру до іншого, тому пропонується перевірка

посередницької системи контролю, тобто "чому це не є проблемою? чому я довіряю джерелу?"

На прийняття рішень щодо надання доступу чи його продовження впливають багато факторів, що забезпечує повноцінну картину. Проте, використання мінливих параметрів може пов'язуватись з багатьма проблемами. Масова атака на відмову в обслуговуванні може бути перенесена від генератора рішень до системи контролю ідентичностей та системи збору даних. Підробка чи фальсифікація інформації цих систем призведе до помилкових відмов у автентифікації ідентичностей, користувачів, пристроїв та застосунків.

Організаціям необхідно забезпечити захищений збір даних про поточний стан усіх її ресурсів. Одним із рішень може бути використання перевірок зібраних даних на адекватність і правильність. Під цим розуміється, перевірка зібраних даних на вмістимість шкідливого коду, який призведе до відмови двигуна політики; перевірка даних на контекст, тобто, якщо спробу з'єднання було відхилено, забезпечити можливість виявлення і відстеження помилок у зборі даних.

Висновки

У науковому дослідженні проведено огляд сучасних методів забезпечення безпеки інформаційних систем у корпоративних мережах на основі концепції нульової довіри (Zero Trust). Розглянуто ключові принципи моделі Zero Trust, її основні переваги та виклики, з якими стикаються організації при впровадженні цієї моделі. Проведений аналіз дозволяє виявити найбільш ефективні стратегії захисту даних і запобігання кіберзагрозам у корпоративних мережах. Результати дослідження можуть бути використані для підвищення рівня інформаційної безпеки у великих організаціях та підприємствах.

Наукова цінність дослідження полягає в узагальненні та систематизації сучасних підходів до безпеки інформаційних систем на основі моделі нульової

довіри, а також у виявленні ключових переваг і недоліків їх використання в корпоративних мережах. Визначено перспективні напрями подальшого розвитку підходу Zero Trust в умовах зростаючих кіберзагроз.

Практична цінність дослідження полягає в можливості використання отриманих результатів для впровадження систем безпеки в корпоративних мережах, що дозволяє підвищити рівень захищеності інформації від внутрішніх і зовнішніх загроз. Викладені рекомендації можуть бути застосовані як у приватних компаніях, так і в державних установах для забезпечення комплексного захисту даних.

Проведений аналіз підтверджує, що традиційні моделі захисту не повністю відповідають актуальним загрозам, які виникають у зв'язку з використанням хмарних сервісів, віддаленого доступу та зростаючої складності інфраструктури мереж. Виявлено, що модель ZTM відмовляється від концепції довіри до будь-яких компонентів системи та зосереджується на постійному контролі доступу через автентифікацію та авторизацію всіх запитів, що суттєво знижує ризики несанкціонованого доступу.

Визначено, що ZTM впроваджує принцип найменших привілеїв та акцентує увагу на постійному моніторингу і аналізі поведінки користувачів, що дозволяє своєчасно виявляти підозрілі дії. Впровадження MFA та безперервної оцінки сесій дозволяє підвищити рівень контролю і зменшити ризики несанкціонованого доступу.

Однак проведене дослідження демонструє, що перехід до моделі ZTM супроводжується викликами. Виявлено, що модель потребує модернізації архітектури, впровадження автоматизованих політик контролю доступу та адаптацію систем до динамічної авторизації й автентифікації. Це вимагає інвестицій, значних змін у підходах до управління безпекою, адаптації до проблем продуктивності через збільшене навантаження на обчислювальні ресурси.

Визначено, що впровадження ZT вимагає модернізації інфраструктури, автоматизації політик доступу та адаптації до зростаючого навантаження на

системи. Зростання SaaS-додатків також створює нові вразливості в цифрових ланцюгах постачання. Як рішення запропоновано впровадження динамічних ідентичностей, де посередники гарантують безпечне з'єднання та контроль доступу.