Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Факультет комп'ютерних наук
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

«Допущено до захисту»
В.о. завідувач кафедри БІСТ
Мелкозьорова О.М.
_____
« » 2024 р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

на тему: «Аналіз підходів та моделей розгортання архітектури нульової довіри у сучасних умовах»

оцінка « » Керівник : д. т. н., професор
Голова ЕК Єсін В.І.
Лемешко О.В. _____ Рецензент: к.т.н., Бобух В. А.
Виконавець : студентка групи КБ-42
Біланович А.О.

Харків – 2024

РЕФЕРАТ

Робота складається із 51 сторінки, 9-ти рисунків, 3 таблиць, 3 розділів та 18 джерел за переліком посилань.

Дослідження, що проводились у роботі, спираються на публікації різних міжнародних авторитетних видань (у тому числі стандартів та деяких урядових організацій по всьому світу), присвячених концепції нульової довіри, а також досвід деяких провідних міжнародних компаній, які впроваджують даний підхід на практиці.

Враховуючи те, що рішення нульової довіри є інноваційним, воно ще не є достатньо дослідженою ланкою інформаційної безпеки, а також не отримало широкого розповсюдження на сьогоднішній день. Актуальність роботи полягає у нестачі інформації про підхід нульової довіри та способів її реалізації. Робота має узагальнити та доповнити наявні відомості про правила роботи із моделлю нульової довіри, щоб забезпечити якомога більшу доступність такого рішення безпеки для підприємств та полегшити роботу з її розгортання як способу максимізації безпеки мереж.

Мета роботи – аналіз підходів та моделей розгортання архітектури нульової довіри в сучасних умовах для надання практичних рекомендацій щодо реалізації концепції zero-trust на типовому підприємстві.

Об'єктом дослідження є процес впровадження концепції нульової довіри на підприємстві.

Предметом дослідження є підходи та моделі розгортання архітектури нульової довіри в сучасних умовах.

У роботі докладно описані особливості моделі нульової довіри та введення її в експлуатацію, представлені всі можливі плюси та мінуси від такого рішення, а також можливі проблеми при розгортці. Крім цього, у роботі наведено практичні рекомендації покрокової розгортки архітектури нульової довіри на підприємстві із зазначенням усіх можливих рішень забезпечення максимальної

безпеки. Власні висновки та практичні рекомендації у цій роботі були сформульовані на основі аналізу результатів досліджень Національного інституту стандартів та технологій (NIST), компаній Fortinet, Oracle, ETSI та IBM.

У результаті роботи мета була досягнута, і користувачі мають змогу використовувати надані напрацювання у якості методичних рекомендацій та способу детального ознайомлення із підходом нульової довіри, усіх його переваг та особливостей.

У роботі були описані найактуальніші на сьогоднішній день підходи та моделі розгортання архітектури нульової довіри, проте, для майбутніх досліджень можливий пошук нових варіантів архітектури нульової довіри або детальний розгляд можливостей поєднання кількох існуючих підходів для реалізації безпеки комбінованим способом.

Ключові слова: МОДЕЛЬ НУЛЬОВОЇ ДОВІРИ, АРХІТЕКТУРА НУЛЬОВОЇ ДОВІРИ, ІДЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ, ZTA, VPN, PA, PE, PEP.

ABSTRACT

The work consists of 51 pages, 9 figures, 3 tables, 3 chapters and 18 sources for the list of references.

The research conducted in this paper is based on the publications of various internationally reputable publications (including standards and some governmental organizations around the world) on the concept of zero-trust, as well as the experience of some leading international companies that implement this approach in practice.

Given that the zero-trust solution is innovative, it is not yet a sufficiently researched area of information security, nor has it been widely distributed to date. The relevance of the work lies in the lack of information about the approach of zero-trust and methods of its implementation. The work should generalize and complement the existing information on the rules of working with the zero-trust model to ensure that such a security solution is as widely available to enterprises as possible and to facilitate its deployment as a way to maximize network security.

The purpose of the study is to analyze the approaches and models for deploying the zero-trust architecture in modern conditions in order to provide practical recommendations for implementing the zero-trust concept at a typical enterprise.

The object of the study is the process of implementing the concept of zero-trust in an enterprise.

The subject of the study is approaches and models for deploying zero-trust architecture in modern conditions.

The work describes in detail the features of the zero-trust model and its implementation, presents all possible pros and cons of such a solution, as well as the possibility of a problems during deployment. In addition, the work provides practical recommendations for a step-by-step implementation of the architecture of zero trust at enterprises, indicating all possible solutions to ensure maximum security. The conclusions and practical recommendations in this paper are based on the analysis of

the results of research by the National Institute of Standards and Technology (NIST), Fortinet, Oracle, ETSI, and IBM.

As a result of the work, the goal was achieved, and the users could use the provided work as methodological recommendations and a way to familiarize themselves with the zero-trust approach, all its advantages and features.

The paper describes the most relevant approaches and deployment models of the zero-trust architecture, but for future research it is possible to search for new variants of the zero-trust architecture or consider in detail the possibilities of connecting several existing approaches to implement a combined security method.

Keywords: ZERO-TRUST MODEL, ZERO-TRUST ARCHITECTURE, IDENTIFICATION, AUTHORIZATION, ZTA, VPN, PA, PE, PEP.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС	операційна система
BYOD	Bring your own device – використання власного обладнання на підприємстві
CDM	Continuous Diagnostics and Mitigation – система постійної діагностики та пом’якшення наслідків
CSP	Cloud Solution Provider – постачальник хмарних послуг
DDoS	Distributed Denial of Service – розподілена відмова в обслуговуванні
DNS	Domain Name System – система доменних імен
EIAM	Enterprise Infrastructure Entitlement Management – управління правами доступу до інфраструктури підприємства
EIG	Enhanced Identity Governance - посилене управління обліковими даними
IDS/IPS	Intrusion Detection System/Intrusion Prevention System – система виявлення вторгнень/система попередження вторгнень
IT	Information Technology – інформаційні технології
NAC	Network Access Control – управління доступом до мережі
NGFW	Next Generation Firewall – міжмережевий екран наступного покоління
NIST	National Institute of Standards and Technology – Національний інститут стандартів і технологій
PA	Policy Administrator – адміністратор політики
PE	Policy Engine – механізм політики
PEP	Policy Enforcement Point – точка застосування політики
PKI	Public Key Infrastructure – інфраструктура відкритого ключа
RBD	Resource-Based Deployment – розгортання на основі ресурсів
SDWAN	Software-Defined networking in a Wide Area Network – програмно-визначувана глобальна мережа

SIEM	Security information and event management – система управління інформаційною безпекою та подіями безпеки
SOAR	Security orchestration, automation and response - оркестрація, автоматизація й реагування системи безпеки
SSO	Single Sign-On – система єдиного входу
SWG	Secure Web Gateway – безпечний веб-шлюз
VLAN	Virtual Local Area Network – віртуальна локальна комп'ютерна мережа
VPN	Virtual Private Network – віртуальна приватна мережа
WAN	Wide Area Network – глобальна мережа
ZT	Zero-trust – нульова довіра
ZTA	Zero-Trust Architecture – архітектура нульової довіри

ВСТУП

Довіра є необхідним елементом відносин між двома або більше сторонами, вона є впевненістю у тому, що інші учасники є доброчесними. Раніше довіру до джерела виявляли у зв'язку з його геолокацією: якщо процес існував у межах корпоративної мережі, він автоматично вважався безпечним, так як усі робітники компанії вважалися перевіреними. З огляду на це, небезпечнеми вважалися тільки ті процеси, що надходять із зовнішньої мережі. Проте, практика показала, що загрози різними методами можуть проникати до системи, уникаючи перевірки на наявність зовнішніх втручань. Лише одне підприємство може містити декілька внутрішніх мереж для комунікації, десятки офісів із власними інфраструктурами, а також застосовувати хмарні сервіси для збереження даних. У такому випадку для підприємства не існує одного периметру з чітко визначеною геолокацією. Ця особливість прямо продемонструвала необхідність створення стратегії, де усі учасники процесу за замовчуванням вважалися б недоброчесними. Вперше подібну модель запропонував Стівен Пол Марш, стверджуючи, що довіру можна змоделювати за допомогою математики [1].

Архітектура нульової довіри (Zero-trust (ZT) architecture, ZTA) ґрунтується на тому, що довіряти неможна жодному, незважаючи на їх місцезнаходження чи роль у компанії. Нульова довіра напрямлена на захист персональних даних, таких як паролі, облікові записи, активи та ін. Подібний захист передбачає також розширення використовуваних методів і підходів захисту інформації. Сучасна версія нульової довіри вперше була описана у 2004 році на форумі Jericho при обговоренні деперіметрації організаційних кордонів для IT-систем (Information Technology systems) таким чином, щоб неявна довіра застосовувалася і у кожному сегменті мережі, так і у єдиній системі в цілому [2].

На даний момент Zero-trust є однією з оптимальних моделей безпеки, так як вона орієнтується на правило, що загрози існують як поза мережею, так і всередині неї. Це забезпечує кращий захист усіх існуючих в системі даних. За

допомогою цього правила модель нульової довіри усуває будь-які можливості неявної довіри до усіх служб, елементів та вузлів мережі, потребуючи постійного підтвердження дозволу на доступ у реальному часі. Ця модель безпеки постійно припускає можливість порушень, чи те, що порушення вже було втілене, через що завжди сканує мережу на нетипову для неї активність та обмежує доступ до ресурсів, надаючи лише необхідну вказану у запиті інформацію. Таким чином, zero-trust architecture може реалізувати і концепцію надання найменш привілейованого доступу для кожного запиту, забороняючи або надаючи доступ лише до тих ресурсів, що необхідні для виконання роботи.

Проте, системи, що розробляються із використанням моделі нульової довіри, потребують детального планування та глибокого розуміння принципів їх роботи. Ця робота спрямована на те, щоб повністю проаналізувати підходи та моделі розгортання архітектури нульової довіри у сучасних умовах, щоб надати практичні рекомендації для втілення концепції zero-trust у системи та висвітлити переваги такого підходу до реалізації безпеки.

Актуальність роботи полягає у нестачі інформації про підхід нульової довіри та способів її реалізації. Робота має узагальнити та доповнити наявні відомості про правила роботи із моделлю нульової довіри, щоб забезпечити якомога більшу доступність такого рішення безпеки для підприємств та полегшити роботу з її розгортання.

Завданням дослідження є формування практичних рекомендацій щодо застосування архітектури нульової довіри на підприємствах. Архітектура zero-trust містить у собі усі керівні принципи підходу нульової довіри та забезпечує найбільшу захищеність робочої системи на сьогоднішній день.

Відповідно до завдання був створений поетапний план досягнення цілей, який включає:

a) огляд особливостей підходу нульової довіри;
b) визначення вимог та концепцій архітектури нульової довіри;
c) ознайомлення з існуючими реалізованими архітектурами нульової довіри;

d) визначення переваг і недоліків моделі нульової довіри;
e) порівняння підходів неявної довіри із підходом нульової довіри для безпеки мереж;
f) розробка практичних рекомендацій для розгортання архітектури нульової довіри на підприємстві;
g) формування висновків щодо здійсненої роботи.

1. АНАЛІЗ МОДЕЛІ НУЛЬОВОЇ ДОВІРИ

1.1. Особливості моделі нульової довіри

Нульова довіра – це модель безпеки, що складається із власних принципів проектування системи, грунтуючись на прийнятому факті існування загроз як поза межами мережі, так і всередині неї. Довіра у такій системі ніколи не надається неявно і постійно оцінюється. Модель zero-trust надає можливість максимально зменшити невизначеність рішень надання доступу для кожного запиту, застосовуючи при цьому й політику надання доступу із найменшими привілеями. Таким чином, модель нульової довіри постійно ставить під сумнів усі випадки неявної довіри, наприклад, передумови доступу користувачів, місце розташування пристроїв чи встановлених мережевих компонентів. Через це zero-trust підхід має власні особливості, які включають [3]:

- комплексний моніторинг безпеки;
- захист даних у режимі реального часу;
- автоматизовану систему безпеки;
- контроль доступу, заснований на можливих ризиках для системи;
- можливість застосування принципу найменш привілейованого доступу.

Використання моделі нульової довіри потребує конкретного підходу до середовища загроз. Для якісного захисту необхідно допускати припущення, що будь-які запити і мережевий трафік в цілому можуть містити небезпеку, а також припускати, що усі пристрої та інфраструктура можуть бути нестійкими до атак. Ці припущення передбачають наявність постійного скоординованого моніторингу системи, як і керованого управління нею. Усі дозволи доступу до даних також пов’язані з ризиком, тому система має бути готовою до швидкого реагування на загрози і подальшого відновлення роботи.

Zero-trust модель має власні керівні принципи, на основі яких і повинна розроблятися конкретна система [3]:

- Перший і головний принцип, що був згаданий раніше – «довіряти не можна нікому». Принцип передбачає аналіз усіх користувачів, пристроїв, програм та потоків, так як ніколи не можна бути впевненими у їх надійності. Цей підхід також передбачає авторизацію користувачів із наданням їм лише найменших необхідних для роботи привілеїв, виключаючи їх можливість доступу до усіх ресурсів системи.
- «Порушення вже відбулося» - принцип, що припускає наявність порушника або зловмисника у системі за замовчуванням. Він передбачає захист ресурсів таким чином, щоб усі пристрої, користувачі та запити на доступ були забороненими до завершення перевірки. Також усі дії в системі будуть постійно відстежуватись, аналізуючи середовище на виникнення підозрілої діяльності.
- Третій принцип, що працює на основі другого – «явна перевірка». Цей принцип передбачає використання декількох рівнів надійності для здійснення доступу до інформації, використовуючи для цього як статичні, так і динамічні атрибути рішень.

Розробка середовища з моделлю нульової довіри також має під собою особливості, які необхідні для її якісної імплементації.

По-перше, необхідно визначити вимоги захисту та дані з активами, що найбільш потребують захищенності.

По-друге, захист даних за вимогами захисту передбачає застосування «архітектури зсередини» - рішення, де основними для захисту є визначена раніше критично важлива інформація та усі шляхи доступу до неї.

Третім кроком забезпечення якісного функціонування моделі нульової довіри є створення політик безпеки. Цей крок допомагає визначити, які користувачі потребують доступу до даних, розділити середовище на категорії, для яких необхідні власні політики безпеки, наприклад, глобальної чи локальної мережі, мобільного зв’язку, центру обробки даних тощо. Він передбачає і подальше застосування політик у задокументованих частинах середовища.

Після усіх виконаних етапів необхідно підготувати систему таким чином, щоб вона постійно аналізувала увесь трафік на всіх рівнях роботи середовища, виявляючи будь-які підозрілі дії чи запити.

1.2. Архітектура моделі нульової довіри

Архітектура нульової довіри є планом кібербезпеки, що розробляється із урахуванням робочих процесів, принципів нульової довіри та зв'язків між компонентами робочої мережі. Така архітектура має під собою наскрізний підхід до усіх корпоративних ресурсів та даних. Це допомагає дослідити усі існуючі матеріальні та нематеріальні об'єкти на наявність вразливостей чи потенційної небезпеки. На самому початку увага приділяється реалізації політики мінімальних привілеїв, тобто обмеженні усіх працівників дозволами лише того рівня, який буде необхідний їм для подальшої роботи, а вже надалі розглядаються шляхи забезпечення надійного інтернет-з'єднання, безперервного аналізу сеансу та ін. В цілому, архітектура zero-trust є мережевою інфраструктурою, як фізичною, так і віртуальною, і сукупністю операційних політик, які функціонують як продукт плану архітектури з нульовою довірою.

Для подальшого розгляду архітектури нульової довіри необхідно розглянути вимоги, можливості та концепти щодо побудування архітектури нульової довіри.

Вимогами до архітектури нульової довіри є [4]:

- скоординований і агресивний моніторинг системи, управління системою та можливості оборонних операцій;
- припущення, що всі запити на критичні ресурси та весь мережевий трафік можуть бути шкідливими;
- припущення, що всі пристрої та інфраструктура можуть бути скомпрометовані;
- визнання того, що всі дозволи на доступ до критично важливих ресурсів пов'язані з ризиком, готовність завдання швидких і скоординованих

атак у відповідь, швидке реагування на відмови чи порушення безпеки критичних елементів архітектури;

- готовність до швидкого реагування і виконання операцій з відновлення контролю над пристроями в архітектурі.

Оскільки система з використанням моделі нульової довіри не може гарантувати нульову вірогідність злому в будь-який момент часу, вона повинна мати механізми максимального обмеження доступу до ресурсів у ній. Також архітектурі необхідне рішення швидкого реагування щодо питань викрадення, видалення або редагування ресурсів зловмисниками у разі доступу до них будь-яким способом: резервуванням, блокуванням, багатофакторною автентифікацією або ін.

Дотримання вищеописаних концепцій і вимог до архітектури нульової довіри фактично гарантує передачу необхідного ресурсу до користувача, якому цей ресурс доступний. При цьому ніякої гарантії щодо можливого злому самого користувача архітектура не надає. Через це процес авторизації користувачів має проводитися із використанням зовнішніх ресурсів для збільшення безпеки передачі даних до авторизованих осіб.

Архітектура нульової довіри має виконувати наступні концепції [3]:

- ніколи не довіряйте, завжди перевіряйте;
- постійне припущення порушення безпеки;
- явна перевірка доступності до ресурсів за запитами;
- перевірка усього трафіку в мережі нульової довіри.

Вищеописані концепції допомагають виконати основне завдання архітектури нульової довіри: забезпечення конфіденційного і безпечного доступу до ресурсів автентифікованим особам за умовою наявності у них дозволу на доступ до цього ресурсу. З цього виходить постійний моніторінг усього трафіку і подальший запис підозрілих дій у журнал для оперативного реагування відповідних механізмів безпеки.

Архітектура нульової довіри загалом складається з двох компонентів [5]:

- Певний довірений шлюз чи проксі-сервер. Завдання такого компоненту – перехоплення запитів на доступ до ресурсів. В залежності від відповіді надає негативну або задовільну відповідь на доступ.
- Контролер доступу. Завдання компоненту – здійснення автентифікації і приймання рішень для проксі-серверів. В більшості моделей контролер розділяється на два окремі компоненти: той, який аналізує дані та той, що відправляє команди.

1.3. Приклади реалізації моделі нульової довіри

1.3.1. Абстрактна модель нульової довіри

Справжнім існуючим прикладом моделі zero-trust є модель NIST (рис. 1.1) [6]. Модель підтримує як роботу з локальної мережі, так і з хмарної. Розроблена ідея пропонує забезпечити не лише стійкість до злому, а й стійкість до відмов: у сформованій теорії один актив може виконувати функції кількох логічних компонентів, і так само логічний компонент може складатися з кількох апаратних або програмних елементів для виконання завдання.

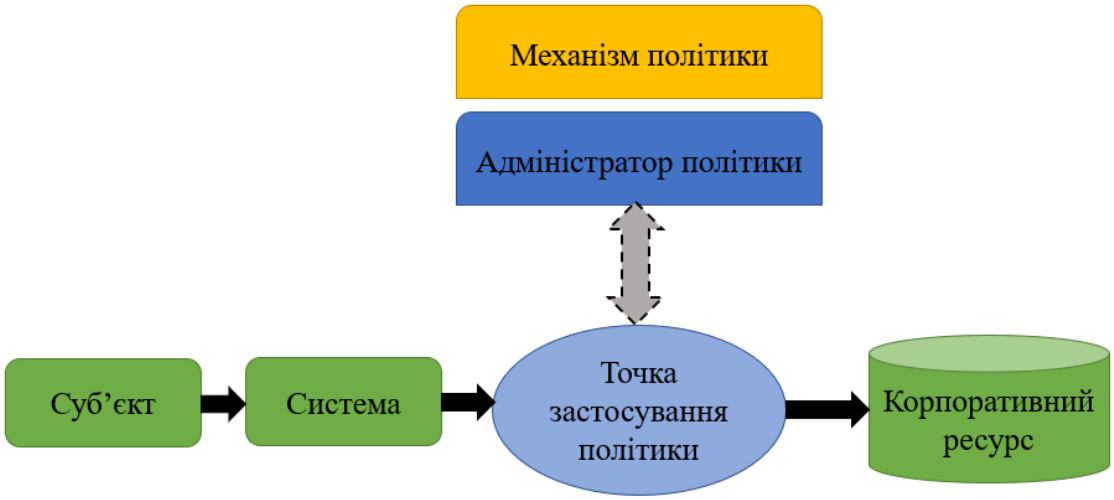

Рисунок 1.1 – Логічні компоненти моделі нульової довіри

Модель має наступні основні складові [6]:

- Суб’єкт (Subject). Ця складова позначає користувача системи, певний пристрій або програму, які працюють з даними системи і безпосередньо мають до них доступ.
- Корпоративний ресурс (Enterprise Resource). Ресурс, що перебуває під контролем системи, є її власністю (документи, таблиці даних, програми тощо).
- Механізм політики (Policy Engine, PE). Працює в якості надавача доступу до ресурсів. Для надання доступу використовує дані з різних джерел і внутрішній алгоритм довіри.
- Адміністратор політики (Policy Administrator, PA). Надає токен автентифікації клієнта. За допомогою таких токенів клієнт може отримати дозвіл на запит доступу до ресурсів.
- Точка застосування політики (Policy Enforcement Point, PEP). Компонент, підпорядкований адміністратору моделі. Складається з клієнтської та серверної частини. Завдання компоненту – створення і завершення з’єднання між клієнтом і ресурсом, його моніторинг.

Робота у системі NIST (National Institute of Standards and Technology) починається з політики доступу до даних, якими займається компонент PE. Система постійної діагностики та пом’якшення наслідків (Continuous Diagnostics and Mitigation, CDM) надає адміністратору інформацію про різні статистичні данні пристроїв в мережі (стан ОС, версія ОС, вразливості, підозрілість тощо), займається відшукуванням сторонніх пристроїв в корпоративній мережі. Система інформації про інфраструктуру відкритих ключів (Public Key Infrastructure, PKI) займається генерацією і зберіганням сертифікатів сервісів та програм.

Архітектура Zero Trust може різнитися залежно від потреб компанії. За рахунок цієї особливості, пропонується декілька варіантів розробки внутрішньої системи із таким підходом [5].

Перший варіант полягає у посиленому управлінні обліковими даними (Enhanced Identity Governance, EIG). В ньому одним з головних критеріїв доступу будуть привілеї конкретних суб'єктів. Рекомендації до застосування є наступними [5]:

- Гарне рішення для компаній, що застосоововують модель відкритої мережі з гостьовим доступом;
- Підходить для компаній із великою кількістю власних пристроїв користувачів, що підключаються до мережі. (У цьому випадку доступ до мережі надається усім, але до корпоративних ресурсів доступ можуть отримати лише привілейовані особи).
- Підходить до компаній, які використовують хмарні сервіси, де немає можливості розгорнути власні компоненти Zero Trust.

Недоліком цього варіанту є те, що зловмисники все ж можуть мандрувати мережею або запускати DDoS-атаки.

Другий варіант полягає у принципі мікросегментації. Метод передбачає розділення ресурсів на окремі групи із використанням інтелектуальних комутаторів, NGFW (Next Generation Firewall) або спеціальних шлюзів. Також метод можна реалізувати за допомогою використання програмних агентів та мережевих екранів на пристроях отримування. Такі шлюзи і комутатори мають швидко змінювати конфігурацію, що буде гарантувати адаптацію до нових загроз і варіацій потоків даних у мережі.

Третій варіант полягає в організації програмно-визначуваних периметрів. У ній адміністратор виступає за контролера, має можливість динамічної зміни конфігурації мережі. Такі зміни засновані на результатах виводу компоненту PE.

Четвертий варіант моделі – розгортання на основі ресурсів (Resource-Based Deployment, RBD). У цій моделі шлюз (PEP) вбудований таким чином, щоб він розгортався безпосередньо перед ресурсом як окремий компонент або одразу на ресурсі. Особливістю такої моделі є постійна наявність неявної довіри, зона якої коливається в залежності від рішень розгортання. Рядом інших недоліків такого

підходу є висока можливість конфліктів між компонентами ресурсів та шлюзами, а також те, що створений для такої моделі захищений тунель може викликати блокування вже наявних вбудованих пристроїв чи елементів, які є еквівалентно необхідними для захисту системи і керування безпекою.

П’ятим можливим варіантом архітектури є використання точки реалізації політик перед попередньо об’єднаними сукупностями ресурсів. Такі ресурси можуть бути пов’язані між собою логічно (наприклад, поєднання серверів) чи фізично (наприклад, ресурси всередині одного відділу компанії). У такому способі сукупності ресурсів при будь-якому зв’язку все одно мають працювати виключно у локальній мережі, яка керується підприємством. Хоча ресурси всередині об’єднання можуть і, можливо, будуть контактувати один з одним поза видимістю і контролем точки реалізації політик, єдиний спосіб для суб'єктів за межами зони довіри контактувати із сукупностями ресурсів – це проходження через PEP, через що не виникає незареєстрованих порушень безпеки. Серед позитивних сторін моделі можна визначити такі, як [6]:

- Модель здадна підлаштовуватися під динамічні середовища.
- Для використання точок реалізації політик не треба здійснювати жодних змін у ресурсах.
- Можна суттєво зменшити кількість таких використовуваних точок.

І шостим визначеним NIST варіантом є маршрутизація через хмарне середовище: у такій моделі увесь трафік спочатку має пройти через «хмару», перед тим як остаточно потрапити до кінцевого ресурсу. Загалом, варіант є дуже поширеним через легкість налаштування та зменшення витрат при такому підході до безпеки організації. Також у такому випадку спеціалісти із введення моделі в експлуатацію іноді одразу додають послугу використання безпечного веб-шлюзу (Secure Web Gateway, SWG). Проте цей метод має і досить вагомі мінуси, наприклад [6]:

- Затримка трафіку.

- Неможливе використання для локальних користувачів чи ресурсів, які зберігаються лише у локальній мережі.
- Архітектура легко вводиться у робочу систему, через що можливі неякісні перевірки мережі чи здійснення неповного контролю безпеки для швидшого завершення налаштувань

1.3.2. Реалізовані приклади моделі нульової довіри

Окрім загалом описаної моделі, NIST пропонує також і реальні моделі з імплементацією нульової довіри, які доступні для встановлення [6]. Такі моделі повністю або частково застосовують керівні принципи нульової довіри для роботи із даними та їх переміщення. Наприклад, до існуючих моделей розгортання відносять:

- Модель розгортання на основі агента пристрою/шлюзу (рис. 1.2). На кожному пристрої в моделі встановлюється спеціальний програмний агент. Такий агент займається координацією з’єднань до ресурсів, які мають такий самий програмний шлюз. Після отримання запиту на доступ до ресурсу, такі агенти скеровують його до адміністратора. Після цього адміністратор передає ресурс у механізм реалізації політик на оцінку. Якщо відповідь буде позитивною, агент конфігурує з’єднання з відповідним шлюзом.

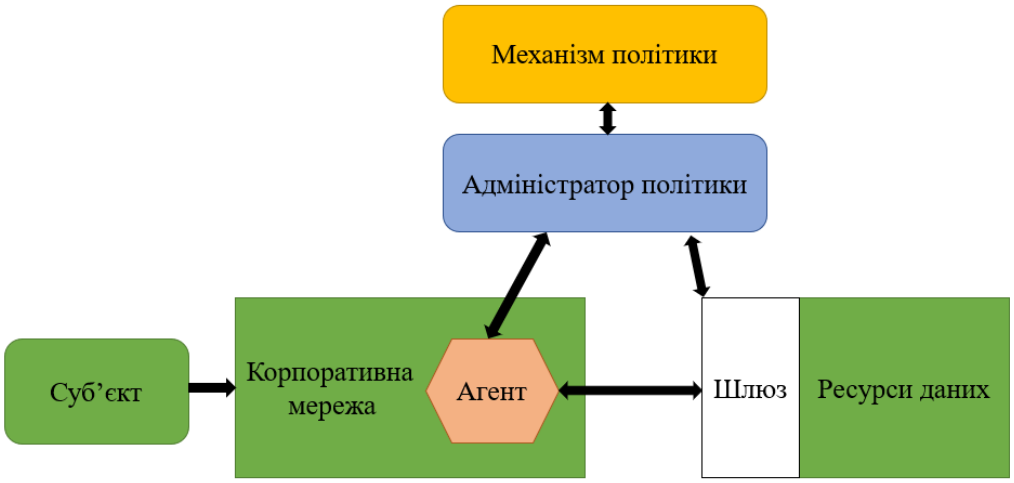

Рисунок 1.2 – Модель нульової довіри на основі агента пристрою/шлюзу

- Модель розгортання на основі анклаву (рис. 1.3). В моделі шлюз розташовується перед групою схожих ресурсів. Використовується організаціях з власним дата-центром або застарілими ресурсами.

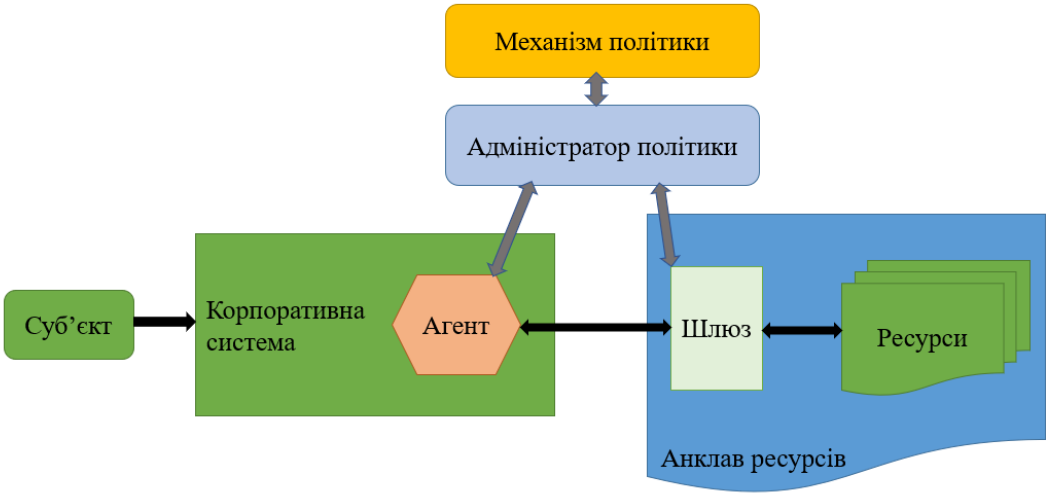

Рисунок 1.3 – Модель нульової довіри на основі анклаву

- Модель розгортання на основі порталу (рис. 1.4). У моделі використовується шлюз, який слугує порталом до якоїсь групи ресурсів

або індивідуального ресурсу. В такому варіанті не потрібно встановлювати спеціальний програмний агент на кожен пристрій, що є зручним для BYOD і співпраці між компаніями. Натомість, система може зберігати лише обмежену інформацію на пристроях в системі.

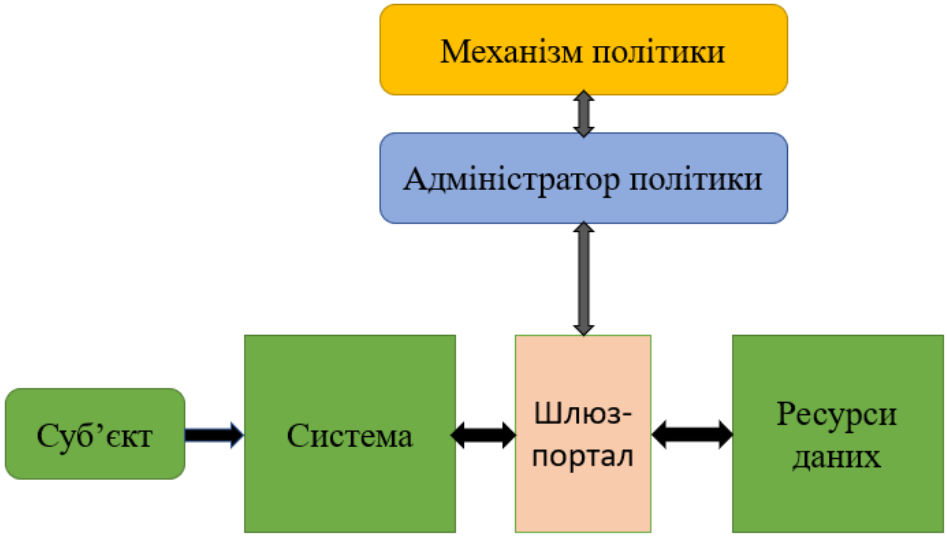

Рисунок 1.4 – Модель нульової довіри на основі порталу

- Модель розгортання на основі використання «пісочниці» (рис. 1.5). Цей варіант пропонує запуск на користувацьких пристроях дозволених програм або процесів лише на захищених ізольованих каналах. Основною перевагою таких моделей є захист системних пристроїв від потенційної компрометації. У таких моделях лише дозволені програми можуть надсилати запити на ресурси і отримувати позитивний відгук, але усі інші застосунки отримуватимуть відмову. Цей метод використовують через гарантію безпеки системних пристроїв у будь-яких ситуаціях, навіть коли сканування на вразливості недоступні. Для роботи системи компанія повинна забезпечити роботу пісочниць на всіх системних пристроях.

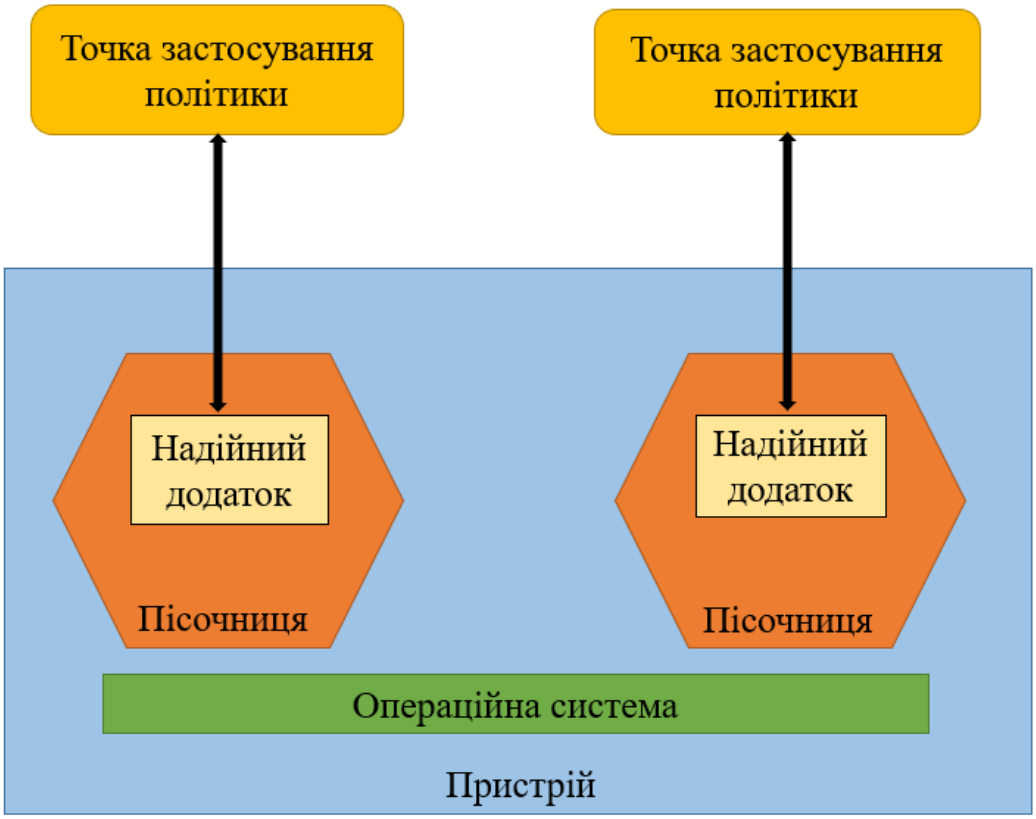

Рисунок 1.5 – Модель нульової довіри на основі «пісочниці»

У сучасному світі моделі нульової довіри на основі систем NIST поширені на усіх материках Землі. У своїх звітах «Zero Trust eXtended Ecosystem Platform Providers» Forrester [5] навіть наводить рейтинг таких виробників за трьома критеріями:

- поточна пропозиція,
- стратегія,
- присутність на ринку.

У звітах до сімки лідерів віднесені компанії [5]:

- Palo Alto Networks;
- MobileIron;
- Illumio;
- Appgate;
- Cisco;

- Microsoft;
- Google.

Абсолютним лідером варто вважати компанію Palo Alto. Вона має повний набір послуг і продуктів для забезпечення нульової довіри в локальних системах, дата-центрі або хмарах. Компанія займається створенням і купівлею інструментів з приводу захисту з нульовою довірою.

Архітектура Zero Trust, яка побудована на рішеннях Palo Alto забезпечує професійний захист інформації в системі і гарантує валідність передачі доступу до ресурсів без передачі даних зловмисникам. Прикладом таких рішень є платформа захисту для хмар Prisma Cloud і, зокрема, модуль Enterprise Infrastructure Entitlement Management (EIAM). Ця технологія виконує функції контролера: визначає доступ до хмарних ресурсів, виконує пошук ризикованих дозволів, забезпечує доступ із найменшими привілеями. Компанія також займається встановленням мережевих екранів наступного покоління і платформ виявлення та реагування на загрози кінцевих точок Cortex XDR.

У свою чергу компанія Cisco придбала компанію Duo Security в 2018 році. Компанія спеціалізувалася на мультифакторній автентифікації. З цього моменту продукти Duo були повністю інтегровані у портфель Cisco. Як результат була створена нова архітектура для захисту «трьох W»:

- персоналу (Workforce) за допомогою Duo;
- робочого місця (Workplace) через SDWAN;
- робочого трафіка (Workload), де рішення Tetration забезпечує сегментацію для програм у багатохмарних середовищах.

Технологія пропонує сучасні методі рішення проблем в питаннях захисту вищевказаних областей і гарантує безпечність використання такої архітектури. Додатково компанія Cisco пропонує послугу Zero Trust Strategy Service, що пропонує класифікований і професіональний перехід до моделі нульової довіри за особливостями замовника.

Окрім лідерів з розробок рішення проблем безпеки питанням нульової довіри та прогресом по таким системам цікавляться і звичайні українські виробники. Прикладом може бути компанія Fortinet [7] із рішеннями FortiToken, FortiNAC. В основі архітектури такої системи лежить FortiAuthentificator. Цей компонент виконує роль керівного центру і відповідає за монофакторну та багатофакторну автентифікацію і авторизацію, управляє дозволами і надає доступи. Рішення FortiToken використовується для двофакторної автентифікації і реалізується у вигляді апаратного токена або мобільного застосунку.

Другою метою архітектури Fortinet є безперервний моніторинг пристроїв у мережі та контроль доступу цих пристроїв. Для цього використовується рішення FortiNAC. Суть рішення полягає у виявлявленні усіх підключених до мережі пристроїв, визначення пристроїв на момент компрометації, класифікування пристроїв за фактором компрометації, ролі та призначенням. Для забезпечення безпечного віддаленого доступу Fortinet розробила рішення FortiClient, яке створює VPN-тунелі.

Також гарним прикладом архітектури на основі нульової довіри є архітектура Check Point. Така архітектура носить ім’я Infinity та об’єднує існуючі рішення за кількома напрямками захисту [8]:

- мереж (шлюзи);
- робочого трафіка (CloudGuard);
- персоналу (Identity Awareness і CloudGuard SaaS);
- даних (рішення для шифрування та запобігання витокам);
- пристроїв (зокрема, пісочниця SandBlast).

Загалом архітектура нульової довіри Infinity використовує 64 різних засоби безпеки для захисту від відомих і невідомих загроз.

2. ВІДМІННІСТЬ ПІДХОДУ НУЛЬОВОЇ ДОВІРИ ВІД КЛАСИЧНИХ РІШЕНЬ БЕЗПЕКИ

2.1. Переваги архітектури нульової довіри

Головною розглянутою властивістю архітектури нульової довіри є незалежність захисту та комунікації від місцезнаходження пристрою. Перевага цього рішення полягає у простому посиленні захисту – зловмисник не може сподіватися на автоматичний доступ до даних, навіть якщо знаходиться на території компанії, офісу, робочому місці працівника тощо. Посилення захисту в моделі нульової довіри означає і сегментацію мережі разом із захистом кінцевих точок, що дозволяє швидше реагувати на спроби шахраїв дістатися до даних або модифікувати їх. Відповідно, втрати даних та несакціоновані втручання значно зменшуються саме при застосуванні такої архітектури.

Другою поверхнево описаною перевагою був доступ на основі кожного сеансу – постійна перевірка особистості користувача перед наданням дозволу на перегляд чи обробку файлів. Ця перевага особлива тим, що потенційний зловмисник не зможе отримати доступ до нещодавно оброблених файлів без попередньої перевірки особи та її прав доступу. Також подібний сеансовий доступ гарантує доступ до однієї конкретної (необхідної в даний момент) інформації, проте не гарантує автоматичного доступу до інших ресурсів. При налаштуванні доступу за стратегією «найменших привілеїв» користувач взагалі не буде мати змоги отримати доступ до будь-яких даних, що не стосуються його поточної роботи. Подібні обмеження підвищують стійкість системи до атак, так як поверхня атаки фактично зменшується від усієї мережі до конкретного окремого ресурсу.

Третьою і однією з основних переваг є постійний моніторинг та аналіз системи, яка використовує модель нульової довіри. Такий підхід дозволяє швидко виявляти аномалії трафіку, помилкові запити, втручання до журналу доступу тощо. При використанні постійного моніторингу додаються політики

керування доступом, що регулюють необхідні правила доступу до конкретного ресурсу та його доступність. Це допомагає легко виявити втручання чи порушення робочого процесу та оперативно заблокувати доступ чи «відрізати» конкретний пристрій від загальної мережі, створивши ізоляцію можливої злочинної програми чи захист від подальших дій шахраїв. За допомогою використання постійного моніторингу компанія може також поступово покращувати та створювати нові політики безпеки, так як має змогу аналізувати можливі ризики, поточний стан активів, вразливості мережевої інфраструктури чи комунікацій. Постійний аналіз включає у себе і докуметування запитів для створення контекстної уяви запитів на доступ у подальшій роботі системи. Як продемонстрував звіт IBM 2021-го року [9], підприємтсва, що застосовували модель нульової довіри, змогли скоротити витрати на виправлення змінених чи втрачених даних більше ніж на півтора мільйона доларів.

Четвертою дуже важливою перевагою архітектури нульової довіри є можливість її застосування для віддалених підключень та хмарних середовищ, що гарантує відслідковування сеансів та підвищення надійності за рахунок можливості введення політик безпеки для цих робочих ланок підприємства. Окрім цього, можливості архітектури дозволяють застосовувати принцип надання найменших привілеїв і для таких типів з’єднань, що, навідміну від VPN, блокує вільне пересування користувачів по усій інформаційній системі. Оскільки хмарні середовища та віддалені підключення частіше за все знаходяться за межами периметру організації, така перевага zero-trust буде найвигіднішою для забезбечення надійності та безпеки цих з’єднань. Необхідність такої можливості полягає у сучасних умовах роботи: згідно із нещодавніми дослідженнями, 55% компаній використовують гібридний метод роботи, поєднуючи віддалену роботу із роботою в офісі [10].

П’ятою перевагою, що частково пов’язана із попередньою, є можливість налаштування автоматичного впливу на доступ користувачів, тобто використання попередньо сформованої оцінки ризику, на основі якої рішення на доступ надавалося б без необхідності втручання адміністратора безпеки. Такий

вплив може включати у себе додаткові перевірки, проте основна його мета полягає у закріпленні обов'язкової ідентифікації для усіх девайсів, програм та користувачів з будь-якої локації. Так як глобальне дослідження KuppingerCole і HP показало, що майже половина офісних працівників використовує свої робочі пристрої для особистого користування, ця перевага zero-trust є дуже актуальною для сучасного робочого ритму.

Шоста перевага здебільшого є зручною саме для працівників у мережі: налаштування політик доступу та постійний моніторинг з'єднання технічно дозволяє виключити з сеансу необхідність повторної автентифікації до його фактичного завершення. Таким чином, користувачі системи можуть отримати зручний доступ без використання багатосимвольних паролів, наприклад, використовуючи для роботи систему єдиного входу (SSO).

Відповідно до сформованих переваг можна порівняти підхід нульової довіри із класичними рішеннями безпеки, визначивши відмінності у захисті та забезпеченні доступу (табл. 2.1):

Таблиця 2.1 – Переваги нульової довіри у порівнянні з класичними рішеннями безпеки

	Нульова довіра	Класичні рішення
Захист фізичних ресурсів підприємства та мережі	Захист не залежить від місцезнаходження пристрою, мережа сегментується.	Довіра надається на основі знаходження пристрою у периметрі підприємства, мережа може бути не сегментованою.
Доступ до ресурсів	Перевірка користувача на підозрілу активність відбувається перед наданням доступу до кожного ресурсу, а також впродовж сеансу. Застосовується принцип найменших привілеїв.	Доступ забезпечується після проходження ідентифікації та авторизації.
Перевірка системи	Постійний аналіз та моніторинг подій, ведення журналів доступу. Створення політик доступу.	Забезпечується докуметування початку та закінчення сеансу, створюються журнали доступу

Продовження таблиці 2.1

	Нульова довіра	Класичні рішення
Захист віддалених підключень та взаємодії із хмарним середовищем	Застосовується як для віддалених підключень, так і для хмарних середовищ. Надає можливість відслідковування сеансів у цих ланках підприємства, дозволяє застосовувати до них визначені політики доступу. Надає можливість віддаленого впливу на доступ користувачів.	Зв'язок забезпечується за допомогою VPN, можливість введення політик доступу та принципу найменших привілеїв не надається.
Ідентифікація та авторизація	Забезпечує з'єднання без необхідності повторної автентифікації до завершення сеансу, виключає необхідність використання складних багатосимвольних паролів.	Налаштована для кожного з'єднання, також може вимагатися повторна авторизація при роботі через певний проміжок часу. Може використовувати автоматично згенеровані паролі та вимагати їх постійного оновлення.

2.2. Мінуси і вразливості архітектури нульової довіри

З іншого боку, архітектура нульової довіри містить низку дуже істотних недоліків та вразливостей.

Однією з найбільших вразливостей, як і у будь-якої неавтономної системи, завжди залишається людина. Компоненти в системі, які відповідають за прийняття рішень про доступ до ресурсів за запитами, потребують належного налаштування і обслуговування, тому багато дій залежить від персоналу. В свою чергу, персонал може вносити зловмисні зміни, допускати помилки, виконувати дії з пристроями, не дотримуючись правил користування ними тощо. Таким чином скомпрометовані контролери надаватимуть доступ до ресурсів несхваленим пристроям, видавати помилки в ситуаціях, коли безпечному користувачу необхідно надати дозвіл до ресурсу або взагалі не працювати. Рішенням такої проблеми може слугувати запис кожної зміни конфігурації

пристроїв до спеціального журналу конфігурацій і подальша перевірка змін на наявність слабких місць автоматичним або ручним методом.

За допомогою засобів соціальної інженерії зловмисники можуть отримати доступ до валідних облікових записів. Таким чином зловмисник, який заволодіє легітимним записом, може отримувати доступ до ресурсів, що є дозволеними для такого запису, ознайомитись із конфіденційною інформацією, виконати її редагування і надіслати запит на оновлення або просто видалити дані. Архітектура нульової довіри не дозволить йому рухатися далі і відмовлятиме в доступі до ресурсів, де він не авторизований. Якщо хакер буде намагатися отримати доступ до заблокованих ресурсів агресивно, алгоритм визначення довіри зрештою помітить незвичну поведінку і заблокує скомпрометований обліковий запис.

Небезпеку для архітектур нульової довіри становлять також і DDoS-атаки, які спрямовані на окремі компоненти архітектури нульової довіри. Така проблема може призвести до аномальної поведінки пристроїв, які будуть відповідати на запити повільно, або просто перестануть працювати. Загрозу можна зменшити за рахунок розташування відповідних компонентів в спеціальних захищених хмарах та/або рівноцінним розподіленням компонентів серед інфраструктури. Проте, це створює нові ризики у вигляді атак на хмарні провайдери.

Існує і можливість проведення атак на ресурси замість компонентів архітектури нульової довіри. У такому разі компоненти не зможуть сконфігурувати маршрут, тому що ресурси будуть недоступні через перезавантаження. Також DDoS-атака може зламати брокер в системі, через що стане необхідним негайно переключитися на резервного брокера або просто відключитись від Інтернету.

Також мінусом архітектур нульової довіри є питання бюджету. Більшості невеликих фірм бракує грошей, досвіду та можливостей для запровадження передових концепцій кібербезпеки як в загальних сферах, так і у сфері моделей

нульової довіри. Наприклад, Markets&Markets зазначає, що вимоги до кібербезпеки зростають швидше, ніж заплановані бюджети [10].

2.3. Порівняльна характеристика неявної та нульової довіри

Зрозуміло, що до появи моделі нульової довіри усі підприємтсва, навчальні заклади, товариства тощо користувалися іншими способами забезпечення безпеки. Якщо узагальнювати, усі методи захисту та архітектури минулих років були варіантами «неявної» довіри або окремими системами доступу. Проте чому цих методів недостатньо для попередження сучасних загроз?

Деякі підприємства використовують систему перепусток, яка дозволяє працівникам отримувати доступ до інформації всередині будівлі лише через факт наявності в них корпоративної картки. Ця модель доступу ілюструє неявну довіру за місцезнаходженням людини та пристрою, проте такий спосіб вже давно став застарілим: звичайні матеріальні перепустки легко втратити або викрасти, через що будь-яка інша людина зможе потрапити на територію підприємства, маючи при собі таку магнітну карту. Окрім цього, не варто виключати недоброчесність і справжніх працівників – за особистих обставин вони також можуть мати наміри пошкодити, викрасти чи знищити якісь активи підприємства.

Якщо розглядати масштабні підприємства, вони також мають широку мережеву інфраструктуру. Частіше за все, для захисту мережі у таких випадках використовується спеціальний приватний DNS-сервер (Domain name system server), що визначає імена внутрішніх серверів, та звичайні міжмережеві екрани. Проте, враховуючи нинішні умови, ці засоби стають недостатніми. При збільшенні навантажень на систему (та збільшенні віддалених підключень) такий спосіб сегментації мережі та контролю доступу надає занадто широкий доступ до мережі, так як є націленим на класичну однозначно визначену IT-інфраструктуру. Така сформована специфікація не дає системі належним чином розрізняти цільові навантаження та якісно аналізувати сеанси користувачів. Цей недолік може призвести не лише до невеликих помилок в обслуговуванні

сеансів, але й до повної відмови системи у випадку атаки – надання широкого доступу надає і можливість поширити зловмисне програмне забезбечення по усьому периметру мережі. Архітектура нульової довіри, навідміну від «класичного» методу захисту, пропонує більш якісну сегментацію та керування доступом, що дає можливість обмежити розповсюдження зловмисних програм та відділити критично важливі дані від робочих даних необхідних для конкретного працівника.

Для захисту мережі можливе рішення NAC (Network Access Control), яке є частиною загальної мережевої інфраструктури. Цей контроль доступу до мережі передбачає застосування сертифікатів, які б підтверджували та ідентифікували пристрій, що запитує дозвіл. Проблема такого підходу полягає у тому, що операції перевірки NAC є недостатньо швидкими для мінливої мережі, через що працівники можуть отримати більший обсяг даних, ніж дозволений за їхнім сертифікатом. Іншою проблемою рішення NAC є його коштовність – більшість компаній в результаті розгортають декілька різних систем контролю доступу для зменшення ціни, що в результаті може призводити до порушень з’єднань між відділами чи конфліктів всередині самої мережі. Важливим мінусом цього способу контролю доступу є і неможливість його використання для хмарних середовищ чи віддалених підключень, які, проте, є цілком можливими у випадку використання архітектури нульової довіри. Незважаючи на те, що підхід zero-trust також не є дешевим, його застосування визначено дешевшим та більш окупним за використання NAC.

Більшість підприємств використовують мережеву систему виявлення вторгнень/систему запобігання вторгненням (Intrusion Detection System/Intrusion Prevention System, IDS/IPS), що вводиться в експлуатацію за допомогою мережевих екранів наступного покоління (NGFW). Системи, як зрозуміло з назви, необхідні для виявлення аномалій трафіку та реагування на вже зчинене вторгнення до мережі. IDS/IPS використовують у якості реакції на можливі вторгнення комбінацію з команд від центру безпеки (адміністратор безпеки чи інша уповноважена особа мають вручну надати системі команди для подальших

дій) та автоматичних дій, заздалегідь заданих для таких випадків. Така система є досить гарним рівнем захисту, проте система із застосуванням моделі нульової довіри здатна зменшити кількість помилкових спрацьовувань за допомогою впровадження журналів доступу та аналізу трафіку, що спрощують процес реагування на потенційно небезпечний сеанс. Ще однією проблемою, яку здатна вирішити архітектура нульової довіри, є незручність і неможливість застосування системи IDS/IPS у хмарних середовищах.

Найрозповсюдженішим рішенням для віддалених підключень на сьогоднішній день є VPN, що є досить дешевим та легким для введення у робочий процес. Проте, використання корпоративної віртуальної приватної мережі не надає жодного контексту щодо підключень: частіше за все, у якості ідентифікації мережа не потребує нічого, окрім пароля, що значно зменшує надійність з'єднання. При цьому рішенні користувачі не лише мають легкий доступ до мережі, але вони також отримують і можливість доступу до усіх ресурсів, що зберігаються у цій мережі. Також, віртуальна приватна мережа не здатна відслідковувати робочий процес, через що велика кількість підприємств зтикаються із падінням продуктивності працівників при застосуванні такого методу контролю. Як вже було вказано раніше, модель нульової довіри зможе не лише аналізувати робочий трафік та увесь сеанс, а й забезпечити у системі віддалений вплив на користувачів та надання чи заборони на доступ без необхідності верифікації безпосередньо адміністратором безпеки. Модель нульової довіри, зокрема, дозволяє внести у систему примусове виконання деяких рішень, що стосуються доступу, для запобігання зловмисних дій з боку користувача.

Популярне рішення для відслідковування подій щодо безпеки - система управління інформаційною безпекою та подіями безпеки (Security information and event management, SIEM). Така система управління може бути хмарною – вона забезпечує гарне масштабування і продуктивність, надаючи і можливість ведення журналу подій з подальшим аналізом сеансів. Цей варіант системи є досить оптимальним рішенням, його відмінність від нульової довіри полягає

лише у недостатньому впливу: SIEM не має інструментів для автоматичного впливу на віддалені підключення. Технічно можливою є не повна заміна рішення, а поєднання нульової довіри із покращеним варіантом SIEM – SOAR (Security orchestration, automation and response), тобто системою оркестрації, автоматизації й реагування.

Головною проблемою сучасних систем є відсутність зручних та довершених поєднань локальної мережі із хмарною інфраструктурою. Зазвичай проблема з'єднання полягає у неможливості застосування однакових моделей безпеки для обох систем та явній різниці мережевих компонентів. Навіть у випадку застосування додаткових інструментів моніторингу, які може надати обраний постачальник хмарних послуг (Cloud Solution Provider, CSP), інфраструктура локальної мережі частіше за все не має відповідних компонентів, що можуть поєднуватися із додатково запропонаваними та працювати у хмарному середовищі. Архітетура нульової довіри здатна не лише забезпечити моніторинг і захист в обох середовищах (як хмарному, так і локальному), але й надати системі динамічну безпеку, що зможе аналізувати контекст запитів на доступ.

Враховуючи розглянуті рішення безпеки та проаналізувавши відмінності класичних систем від систем із застосуванням нульової довіри, можна виділити наступні застарілі чи не достатньо ефективні рішення, які було б вигідно замінити компонентами архітектури нульової довіри (табл. 2.2):

Таблиця 2.2 – Популярні рішення безпеки, які можуть бути замінені рішенням нульової довіри

Розповсюджене рішення безпеки	Його недоліки
Перепустки	Втрата носія чи його викрадення
Сегментація за допомогою DNS-сервера	Занадто широкий доступ до мережі
NAC	Коштовність та недостатня швидкість, відсутність можливості використання для хмарних середовищ

Продовження таблиці 2.2

Розповсюджене рішення безпеки	Його недоліки
IDS/IPS	Відсутність можливості застосування у хмарному середовищі, наявні помилкові спрацьовування при перевірці доступу
VPN	Занадто проста процедура отримання доступу, надає широкий доступ до мережі
SIEM	Відсутність можливості керування віддаленим доступом

Якщо розглядати усе вищевказане, використання моделі нульової довіри для захисту підприємства є найактуальнішим на сьогоднішній день. Однак, статистика демонструє, що наразі використання ZTA не досягло навіть 1% розповсюдження [11]. Бізнес-фірма Gartner прогнозує, що навіть за умови якісного фінансування відділів безпеки підприємств, лише 10% організацій зможуть досягнути повної, комплексної та належно функціонуючої архітектури нульової довіри до 2026-го року.

Щоб зрозуміти, що спричиняє таку серйозну проблему із розповсюдженням архітектури zero-trust, компанія Fortinet [7] провела масштабне опитування: питання щодо розгортання нульової довіри було підняте у 31 країні та більше 570 провідних IT-спеціалістів дали свій огляд на ситуацію. У порівнянні з 2021 роком було виявлено, що використання доступу до мережі за допомогою нульової довіри збільшилося майже на 10% у 2023 році, а відсоток підприємств, що взагалі не планували використовувати це рішення для своїх систем, знизився на 8 позицій (рис. 2.1):

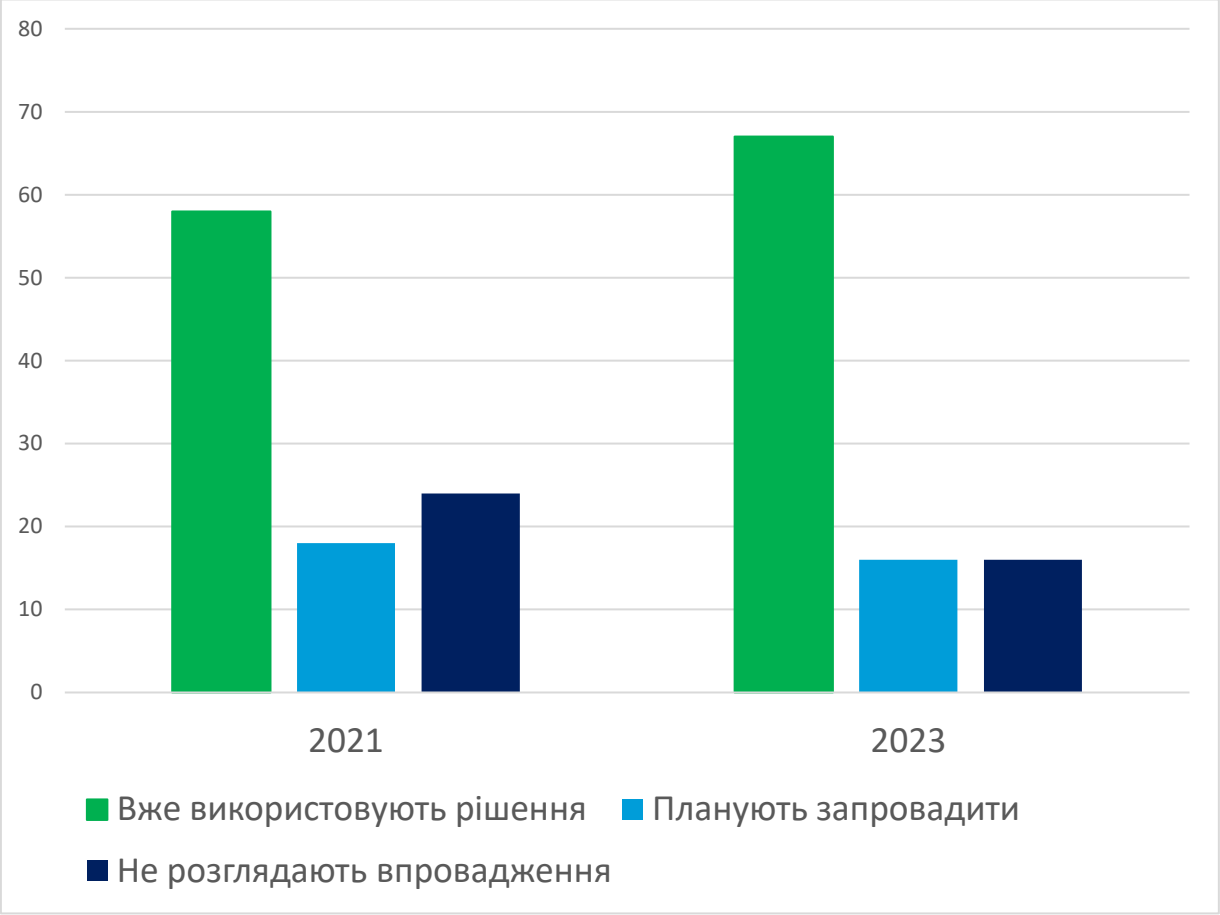

Рисунок 2.1 – Використання компаніями доступу до мережі за допомогою ZTA

Проте, опитування показало, що незважаючи на популяризацію підходу нульової довіри, у більшості підприємств виникли проблеми із його впровадженням – робота з архітектурою виявилася значно складнішою, ніж передбачалося (рис. 2.2). В результаті спроб впровадження, 33% підприємств стикнулися з серйозними проблемами затримки при використанні ZTA, 24% компаній стикнулися із проблемами недостатньої кількості інформації щодо моделі нульової довіри, 24% підприємств зазначили відсутність якісних кваліфікованих постачальників такої архітектури, а також проблеми недостатності ресурсів (4%) та занадто великої коштовності моделі (17%) [10].

Рисунок 2.2 – Проблеми впровадження архітектури нульової довіри

Розгляд проблеми з боку Fortinet показав, що основними проблемами, що заважають заміні усіх систем із неявною довірою на системи з архітектурою нульової довіри, є недостатність фінансів та інформації щодо введення моделі в експлуатацію. Проте, за прогнозами компанії, використання концепції zero-trust буде постійно зростати через дедалі ширшу популяризацію хмарних середовищ та можливості віддаленої роботи.

Водночас, інша компанія – Gartner, на основі власних досліджень зазначає, що кількість систем із нульовою довірою зросте до 10% найближчими роками: її впровадження допоможе забезпечити постійну оцінку, чіткий розрахунок та адаптивну довіру між користувачами, пристроями та ресурсами [12].

3. ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО УСПІШНОГО ВПРОВАДЖЕННЯ КОНЦЕПЦІЇ НУЛЬОВОЇ ДОВІРИ

Для розв’язання проблеми недостатньої кількості інформації щодо впровадження моделі, у цьому розділі будуть надані практичні рекомендації щодо її розгортання та огляд необхідних дій перед її початком.

3.1. Визначення вимог та необхідних умов можливості реалізації моделі нульової довіри на підприємстві

Для успішного впровадження архітектури нульової довіри до робочої системи необхідно визначити можливі проблеми на підприємстві (рис. 3.1). Вони можуть стосуватися обладнання, працівників, розробників, постачальників чи фізичного периметра загалом.

Починати необхідно з розгляду фізичних активів підприємства. Треба точно визначити їх кількість, розташування, поточну захищеність та критичність для роботи. Після створення чіткого списку ресурсів, необхідно визначити їх стан: чи потребують вони заміни на більш нові провідні девайси та чи мають користувачі проблеми із доступом до них на сьогоднішній день. Хоч і не обов’язковим, але важливим для архітектури нульової довіри, буде розподілення або сегментація ресурсів – у такому випадку ZTA буде найбільш продуктивною при роботі. Використання моделі нульової довіри буде дуже доречним при наявності у підприємстві динамічних ресурсів. Також перед початком роботи необхідно точно знати топологію мережі підприємства, розташування її точок входу і способу надання доступу до сегментованих даних. Це завдання може виявитися складним у випадку великих розмірів підприємства чи його динамічної структури. У такому випадку методом контролю може бути поступовий аналіз окремих частин інфраструктури без залучення на перевірку нового сегменту до завершення повної перевірки та взяття під контроль попереднього.

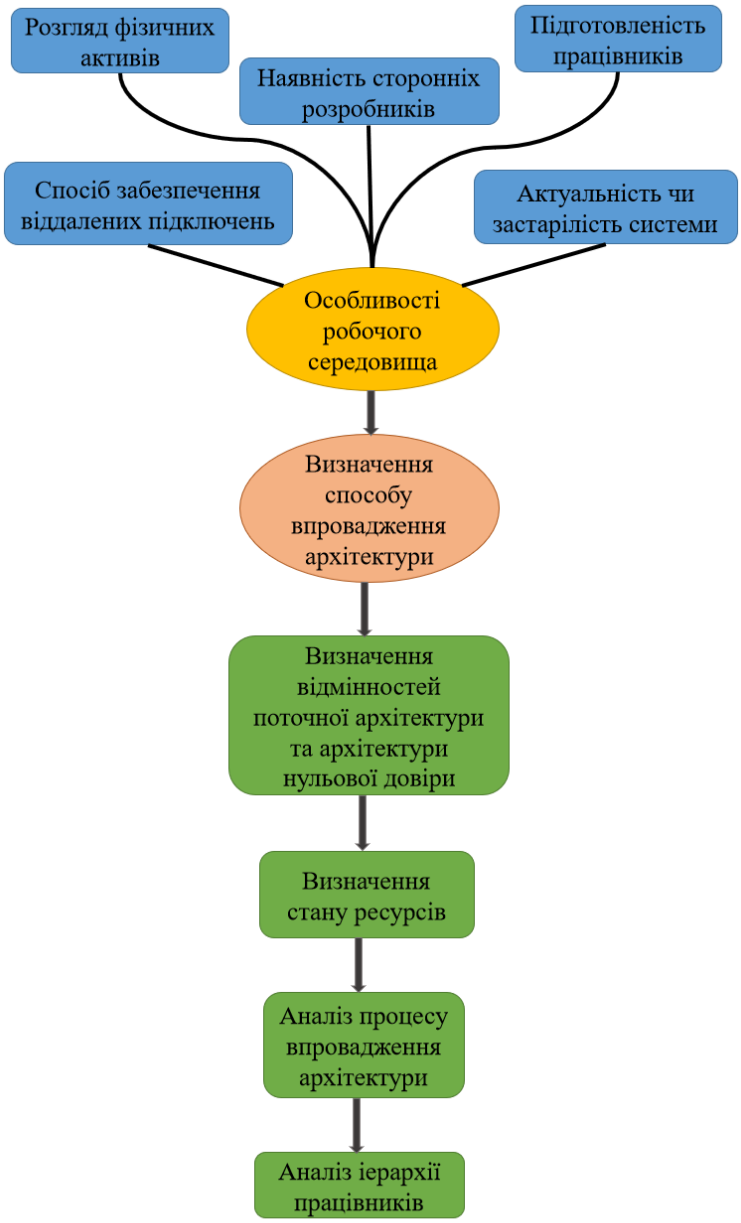

Рисунок 3.1 – Визначення особливостей підприємства та способу впровадження архітектури нульової довіри

При розгляді підходу zero-trust треба обов’язково визначити можливість присутності сторонніх розробників на підприємстві. Зазвичай їх присутність зумовлена спільними із компанією проектами, через що їх доступ заздалегідь вже обмежений конкретними даними і задачами. Визначити наявність таких користувачів у системі є важливим з іншої причини: сторонні розробники

зазвичай отримують доступ до інформації та ресурсів підприємства, використовуючи для цього власні пристрої, що може становити ризик для безпеки мережі. Для архітектури нульової довіри варто визначити, яким чином забезпечується з'єднання цих користувачів із корпоративною мережею та шлях їх мережевого трафіку при роботі із даними. Це надасть можливість змінити процедуру зв'язку у випадку того, якщо трафік охоплює велику частину мережевих ресурсів, що не потрібні для виконання завдання та зрозуміти, у яких місцях повинні розташовуватися захисні шлюзи із реалізацією політик доступу. Для таких з'єднань правильним буде застосування принципу найменших привілеїв, так як сторонні розробники, по факту, є користувачами з некорпоративної території. Важливо, що ці рекомендації щодо доступу є корисними не лише для користувачів мережі, які використовують власні девайси чи віддалене підключення, але й для незадокументованих осіб: захисні шлюзи і принцип найменших привілеїв значно зменшать їх шанси на проникнення та отримання доступу до важливих даних чи ресурсів підприємства. Зручною ZTA робить і налаштування одночасного доступу через захищені підключення, так як за правильних параметрів користувачі зможуть отримувати доступ до декількох даних одночасно, при цьому зберігаючи свій рівень доступу, який був заздалегідь визначений політиками підприємства.

Важливо визначити, яким чином підприємство забезпечує віддалені підключення та/чи взаємодію із хмарним середовищем на теперішній час. До 2019 року такий спосіб роботи був не дуже розповсюджений, проте через швидку появу світової пандемії більшість організацій мала забезпечити його наявність. Це призвело до того, що рішення щодо з'єднання були прийняті у найкоротші строки, і зазвичай цим рішенням було введення корпоративних VPN. Проблема швидких рішень полягає у тому, що, частіше за все, віртуальна приватна мережа була розгорнута у якості окремої системи, налаштованої лише для умов віддаленого підключення, через що така мережа може мати конфлікти взаємодії із загальною локальною мережею підприємства. Другою проблемою є те, що швидкі і дешеві рішення VPN забезпечують надто широкий доступ до даних,

часто охоплюючи не лише ту інформацію, яка необхідна працівнику для роботи. У такому випадку розгортання zero-trust рішення буде найбільш зручним для забезпечення доступу в усіх мережах без конфліктів між собою та захисту даних під час сеансу користувача.

Проблемою, яка може бути виявлена на підприємстві, також є використання застарілих систем, які поступово були оснащені необхідними додатками для підтримки належного рівня відповідності вимогам. Якщо така проблема дійсно буде присутня на підприємстві, ZTA здатна надати рішення із підтримкою різних типів ідентифікаційних даних, щоб захистити систему відповідно до сучасних протоколів автентифікації та ідентифікації користувачів.

Іншою можливою проблемою може бути непідготовленість працівників до рішення нульової довіри. Ця проблема може здаватися незначною у порівнянні з фінансовими та апаратними складовими, проте звичайна людська непідготовленість може викликати серйозні проблеми із впровадженням [4]. Люди можуть відмовлятися від моделі нульової довіри, небажати змінювати робочу рутину, розглядати зміни документації та загалом не сприймати подібне нововведення. Важливо детально підійти до питання освіти майбутніх користувачів системи з архітектурою нульової довіри.

Розглядаючи підхід нульової довіри, варто чітко усвідомлювати, які переваги він може надати, якою є ціль такого рішення, а також знати методи, якими реалізується рішення zero-trust (табл. 3.1) [13]:

Таблиця 3.1 – Принципи, цілі та методи zero-trust

Принципи нульової довіри	Цілі нульової довіри	Методи реалізації нульової довіри
• Вся комунікація захищена незалежно від місця розташування мережі. • Доступ до ресурсів надається на основі аналізу з'єднання.	• Ідентифікація та класифікація ресурсів. • Забезпечення однакової політики безпеки для внутрішніх та зовнішніх запитів на доступ.	• Управління ідентифікацією користувачів та пристроїв. • Аутентифікація сеансів, контроль доступу на рівні ресурсів.

Продовження таблиці 3.1

Принципи нульової довіри	Цілі нульової довіри	Методи реалізації нульової довіри
• Доступ до ресурсів надається на основі динамічних політик, які враховують стан ідентифікації користувача/пристрою та можуть включати інші поведінкові атрибути. Таким чином, усі власні ресурси та/чи пристрої знаходяться у максимально захищеному стані. • Автентифікація та авторизація всіх ресурсів є динамічною та суворо дотримується. • Регулярно проводиться збір інформації для коригування та покращення стану безпеки.	• Забезпечення того, щоб попередні права доступу до з'єднання або сеансу не впливали на наступні права сеансу, а доступ до запитуваного ресурсу був суворо обмежений. • Впровадження динамічних політик доступу, які враховують стан користувача, стан пристрою користувача та його поведінкові атрибути. • Безперервна діагностика та пом'якшення наслідків для оцінки стану пристрою, швидкого блокування доступу скомпрометованого пристрою • Забезпечення аутентифікації та авторизації як безперервних та автоматичних процесів, переоцінка та адаптація довіри до нових та поточних комунікацій.	• Сегментація мережі та додатків для впровадження політик ближче до даних або ресурсів, автентифікація та авторизація всіх запитів, як внутрішніх, так і зовнішніх, шифрування всієї комунікації, як внутрішньої, так і зовнішньої. • Контекстна автентифікація та авторизація, заснована на ризиках (розрахунок оцінки ризику на основі контексту та історії), адаптивні та динамічні методи контролю доступу. • Безперервна автентифікація та авторизація, адаптивні політики доступу, повторна автентифікація та повторна авторизація, автоматизація автентифікації та авторизації.

Продовження таблиці 3.1

Принципи нульової довіри	Цілі нульової довіри	Методи реалізації нульової довіри
	• Безперервний збір даних для виявлення загроз у системі з автоматичним застосуванням необхідних заходів безпеки	• Моніторинг зв'язку, аутентифікація на основі поведінки для заборони доступу до скомпрометованих пристроїв. • Журналювання активності, моніторинг мережі, виявлення та аналіз загроз

Враховуючи усі отримані дані, можна сформувати власне чітке уявлення про архітектуру нульової довіри для підприємства.

Після визначення усіх особливостей роботи підприємства та повного ознайомлення із усіма методами забезпечення безпеки за допомогою рішення нульової довіри наступним завданням є визначення способу впровадження архітектури нульової довіри. Потрібно розглянути готовність переходу системи на рішення zero-trust та можливі затримки чи проблеми під час розгортання, визначивши також стан ресурсів і стан користувачів (рис. 3.1).

По-перше, необхідно буде визначити теоретичні відмінності поточної мережі від її вигляду при застосуванні ZTA. Ці теоретичні роздуми допоможуть визначити, які зміни мають відбутися у розташуванні точок доступу та що може змінитися у процедурі взаємодії компонентів системи між собою. Розгляд відмінностей надасть розуміння, як наразі розташовані ресурси компанії та чи існує у її роботі неявна зона довіри, а також нинішний стан обміну потоками даних між визначеними зонами.

По-друге, треба з’ясувати стан ресурсів та доступу до них. У цьому пункті основним є розуміння способу захисту ресурсів на сьогоднішній день та ступінь необхідності доступу працівників до них. Це допоможе сформувати правильну схему взаємодії та визначити найбільш критично важливі дані для роботи.

Третім етапом роботи є аналіз процесу заміни вже існуючої архітектури на архітектуру нульвої довіри (або введення архітектури з нуля, повністю перебудовуючи систему). Треба зрозуміти, чи можна об’єднати існуючу архітектуру з ахітектурою zero-trust, чи є ресурси, які потребують повної заміни для застосування в архітектурі та чи є необхідним забезпечення тимчасового співіснування системи без підходу нульової довіри та системи із її застосуванням. У такому випадку буде необхідним застосування гнучкої моделі zero-trust, яка дозволяє асиметричну взаємодію: користувачі зможуть отримувати доступ до ресурсів, що не є частиною системи із нульовою довірою, так як мережевий трафік буде проходити через шлюз із PEP. Така взаємодія буде зручною і для забезпечення зв’язку із хмарним середовищем, так як надасть додатковий контроль з’єднань. Окрім забезпечення взаємодії двох систем, реалізація нульової довіри може повністю замінити собою WAN (Wide Area Network) на підприємстві: послідовна реалізація ZTA здатна усунути конфлікт між корпоративними мережами та об’єднати їх у чітко визначену систему з власними політиками взаємодії.

По-четверте, необхідно отримати дані про нинішню ієрархію працівників у системі та яким чином вони отримують інформацію і доступ до ресурсів, що потребуються їм для роботи. Існування журналу доступу чи документації про ідентифікацію користувачів у системі може значно полегшити відслідковування підозрілих з’єднань чи дій у мережі. Якщо ж будь-який спосіб запису та аналізу ідентифікації відсутній, підхід нульової довіри надає можливість легкого автоматичного відслідковування та документування сеансу. Важливо, що наявність журналів доступу збільшує відповідність системи нормативним вимогам безпеки.

Загалом, з огляду на всі проблеми і труднощі введення архітектури нульової довіри, найоптимальнішим процесом розгортання буде поступове впровадження окремих процесів та політик доступу у систему, так як це надасть можливість відслідковування можливих проблем і взаємодії користувачів при нововведеннях, що полегшить вирішення виникаючих труднощів при зміні

архітектури. Такий поступовий підхід зменшить ризик відмов і незрозумілих помилок у системі, а також надасть розуміння щодо наступних процесів розгортання архітектури, так як роздуми зможуть базуватися на практичному досвіді. Поступове введення нових політик доступу та правил взаємодії полегшить і перехід персоналу на нову архітектуру, так як у процесі він буде отримувати нові знання щодо підходу нульової довіри, через що буде готовим до наступних нововведень в подальшому.

3.2. Рекомендації щодо розгортання моделі нульової довіри

Як вже було вказано вище, найкращим способом розгортання моделі нульової довіри буде поетапність (рис. 3.2) – такий поступовий підхід підготує усе підприємство до повного переходу на архітектуру zero-trust, а також зробить її впровадження легшим і більш впорядкованим, що в кінцевому результаті зробить модель більш надійною. Важливо зазначити, що навіть поступове впровадження вимагає завершення – ZTA необхідна взаємодія з усіма компонентами безпеки мережі підприємства для гарантії повної захищеності.

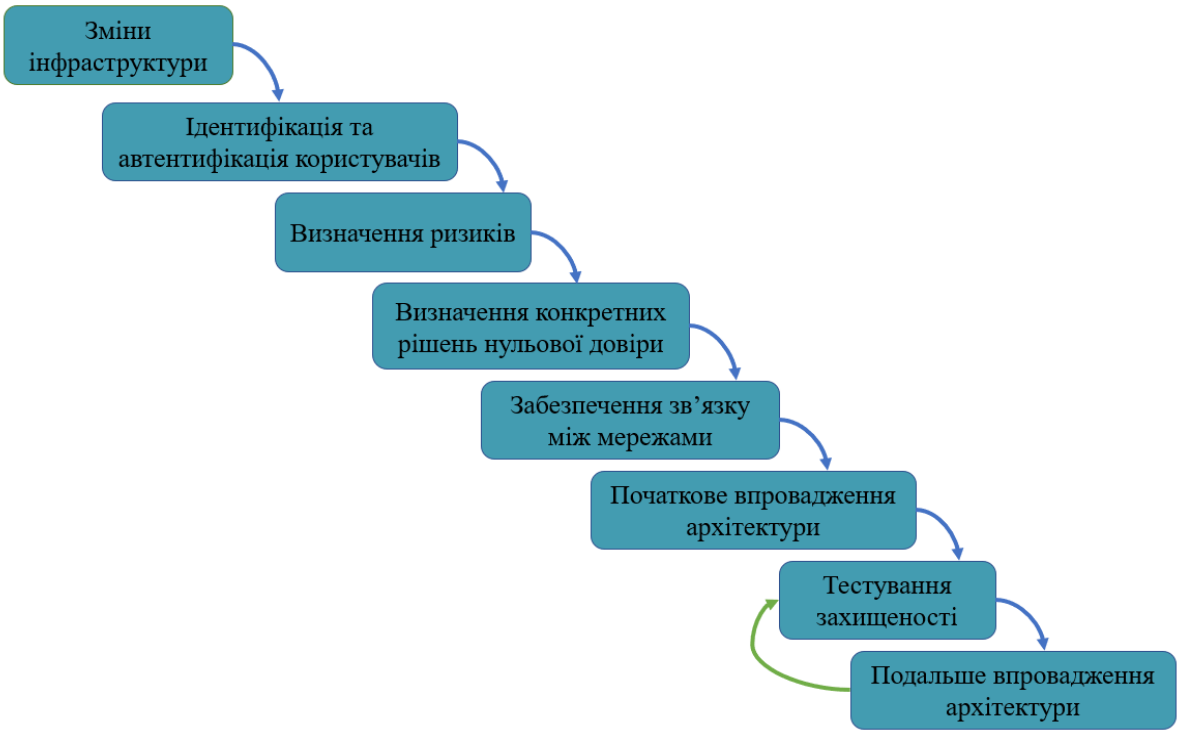

Рисунок 3.2 – Поетапне впровадження архітектури нульової довіри

Почати варто зі змін інфраструктури підприємства: важливо виключити застарілі та не відповідні вимогам ресурси. Під час такої оптимізації активів треба визначити усі пристрої, що будуть мати доступ до мережі [14]. Такими пристроями можуть бути:

- комп’ютери та ноутбуки;
- мобільні пристрої;
- сенсори;
- принтери та факси;
- окремі компоненти девайсів;
- програми сертифікації;
- власні пристрої працівників або девайси з неявної зони довіри;
- інші ресурси.

На цьому етапі обробляється можливість швидкої ідентифікації пристрою та визначаються політики доступу до мережі, щоб забезпечити підприємство методом швидкого реагування на усі запити. При цьому розробляється можливість моніторингу системи для постійного спостереження за сеансом і блокуванні його у разі порушень політик. Важливим є створення унікальних ідентифікаційних номерів для усіх ресурсів системи, за якими будуть відслідковуватися їх дії при функціонуванні у мережі: так як підключення можуть здійснюватися між середовищами (локальним і хмарним), між окремими частинами мережі, програмами, операційними системами і т.д., спосіб ідентифікації за IP-адресою стає застарілим та нерелевантним рішенням [15]. Окрім цього, нині існуючою проблемою є вичерпання існуючих адрес, що також ускладнює ідентифікацію за цим параметром, а також демонструє його невідповідність до провідних методів забезпечення безпеки.

Наступним оптимальним кроком буде ідентифікація та автентифікація користувачів: необхідно забезпечити якісну перевірку доступу та контроль користувачів, які зможуть переглядати будь-які дані підприємства та оперувати ними. У цьому випадку треба застосувати підхід найменших привілеїв, щоб

абсолютно усі користувачі мали лише необхідні для їх роботи дані, незважаючи на визначений для них рівень доступу. Доречно визначити користувачів, які мають ширші привілеї, наприклад таких, як адміністратор безпеки, щоб призначити для них додатковий контроль від системи. Загалом, усі користувачі, так само як і девайси, теж мають отримати власні атрибути для їх ідентифікації у мережі. Це не обов'язково мають бути номери, проте кожен ідентифікатор має належати лише одній особі та бути за нею закріпленим. На цьому кроці також створюються журнали доступу для відстеження сеансів, дій у них та їх тривалості. Під час формування правил ідентифікації формуються і умови використання, з якими мають ознайомитися усі користувачі. Можливою реалізацією автентифікації та ідентифікації буде вбудовування облікового запису до пристрою чи введення до вже існуючої процедури підтвердження особи додаткових параметрів, наприклад, відбитків пальців. Авторизація зазвичай також забезпечується на основі визначеного рівня доступу користувача – це забезпечує відслідковування того, яким чином відбувається взаємодія із мережею і до яких даних особа отримує доступ упродовж сеансу. На цьому кроці реалізації нульової довіри необхідно забезпечити повну автентифікацію та авторизацію. За допомогою керування політиками та інструментами доступу можливим є здійснення детального контролю незалежно від привілейованості користувача та важливості запиту у черзі мережевого стеку.

Третім етапом реалізації ZTA є визначення ризиків: для успішного захисту підприємства треба визначити ризики та надати їм рівні. Рівень небезпечності ризику визначається за допомогою розуміння ймовірності його появи та збитків, які принесе підприємству його реалізація. Після документування ризиків буде зрозуміло, які ресурси є найбільш критично важливими для роботи компанії та які вразливості вони мають. Керуючись отриманими даними, необхідно забезпечити роботу із впровадження нульової довіри таким чином, щоб вона відбувалася для найбільш вразливих до атак ресурсів у першу чергу. Визначивши такі ресурси, необхідно запровадити для них політики нульової довіри та принцип найменших привілеїв, щоб майже негайно знизити чи уникнути

небезпечність робочого процесу. Оцінку ризику за правильних налаштувань можна здійснити і для кожного запиту на доступ: політики доступу на основі вже існуючих даних зможуть прогнозувати рівень небезпеки від ініціатора зв'язку, наприклад, аналізуючи місце з'єднання користувача із мережею, рівень його доступу до ресурсів та посаду в організації.

Четвертим важливим кроком розгортання моделі є визначення конкретних рішень, які відповідали б принципам нульвої довіри. Як було вказано у Розділі 1, наразі вже існує декілька функціональних моделей нульової довіри, які є доступними для встановлення на підприємстві. Тому важливо зрозуміти конкретні потреби організації для визначення найоптимальнішого варіанту архітектури. Важливими параметрами, що впливають на вибір моделі, є:

- необхідність нульової довіри як у хмарних, так і у локальних середовищах;
- необхідність встановлення додатків із нульовою довіру на пристроях користувачів;
- необхідність шифрування даних на усіх етапах їх передачі (та наявності процедур шифрування за замовчуванням або за запитом користувача);
- необхідність створення журналів доступу та реєстрації мережевих взаємодій;
- необхідність відстеження процесів скидання пароля, оновлення профіля та інших дій в контексті одного користувача чи групи користувачів;
- необхідність підтримки великої кількості протоколів на різних рівнях мережевого стеку (наприклад, підтримку як протоколів прикладного рівня для взаємодії мережі і користувача, так і протоколів транспортного рівня для безпечної передачі даних у мережі);
- необхідність наявності сертифікованих документів;
- необхідність змін поточної інфраструктури підприємства.

Рішення, яке є грунтовним при розгортанні нульової довіри – це забезпечення зв'язку між серверами. При застосуванні міжмережевих екранів із

точкою прийняття рішень про політику необхідно забезпечити екран для взаємодії між трафіком, що потрапляє до хмарної чи віддаленої мережі та тим, що надходить із локальної мережі підприємства. NIST визначає чотири варіанти шлюзів для забезпечення надійного зв'язку [16]:

- Вхідний. Цей шлюз відповідає за прийняття даних у мережу, відслідковуючи їх подальший шлях та взаємодію у системі.
- Вихідний шлюз. Ця точка виходу з мережі відповідає за взаємодію поза мережею, аналізуючи та документуючи обмін даними між середовищами.
- Граничний. Як зрозуміло з назви, цей шлюз знаходиться на кордоні між мережею та вхідним шлюзом, відповідаючи за припинення надходження зовнішнього трафіку та полегшення подальної маршрутизації даних.
- Sidecar. Особливість цього шлюзу полягає у його розташуванні разом із кожною програмою, що має обмін мережевого трафіку, для його перехоплення і зв'язку між іншими додатками чи службами мережевої інфраструктури.

Хоча це не є обов'язковим для розгортання моделі нульової довіри, правильним рішенням буде забезпечення сегментації мережі: розбиття інфраструктури на групи значно полегшить виявлення несправностей у майбутньому, а також сприяє розподіленню навантаження на систему. У такому випадку підприємство може стикнутися із додатковими етапами роботи: окрім загальних політик доступу до ресурсів, мають бути впроваджені і політики доступу та взаємодії між сегментами інфраструктури. Для кожного сегменту має бути забезпечений шлюз, який буде здатний відслідковувати трафік та буде оснащений точкою прийняття рішень про політику, щоб забезпечити захист від загроз та динамічні рішення щодо доступу без необхідності втручання адміністратора безпеки. Втім, кожне підприємство має самостійно визначити критерії сегментації своїх мереж.

Після визначення усіх необхідних рішень можна переходити до наступного масштабного кроку: початкового розготання нульової довіри. Важливим є поступове розгортання архітектури для забезпечення правильного функціонування усіх впроваджених політик доступу та процесів обміну даними. Покрокове розгортання також дозволяє швидко виявити проблеми чи несправності у системі, щоб поступово усувати їх без ризику перевантаження чи значних помилок в обслуговуванні системи. Архітектура нульової довіри здатна до самостійного ведення журналу доступу та аналізу трафіку за визначеними для неї політиками, проте доречним буде і створення реєстру послуг для полегшення відслідковування усіх ресурсів, що є наявними у мережі.

Окремим пунктом впровадження нульової довіри буде проведення тестів захищеності: наприклад, атак на проникнення та атак викрадення інформації. Безумовно необхідним є не лише проведення тестових запусків розгорнутих рішень, але й тестування їх стійкості. Тестову роботу у режимі нульової довіри варто перевірити і на персоналі системи: проведення спроб атак за допомогою фішингу чи діпфейків здатне показати і рівень захищеності з боку «людського ресурсу».

Нарешті, коли усі дії із впровадження виконані та початкові нововведення у системі стають частиною робочого процесу, можна переходити до впровадження наступних політик. Таким чином, забезпечуючи постійне оновлення архітектури нульової довіри, можна дійти до повного переходу підприємства на функціонування за моделлю zero-trust. Важливо створити можливість регулярної перевірки стану системи та план майбутніх впроваджень, щоб мати змогу дотримуватись узгодженності між усіма компонентами.

Навіть після повноцінного розгортання архітектури нульової довіри із дотриманням усіх вимог і принципів такого підходу робота не має зупинятися. Важливо постійно відслідковувати можливі оновлення рішень нульової довіри та бути відкритими для обміну досвідом: консультація із більш досвідченими користувачами моделі нульової довіри може бути корисною інвестицією у покращення вже розгорнутої архітектури. Іншою постійно відслідковуваною

роботою є забезпечення якісного навчання працівників підприємства для повної їх інформованості про методи забезпечення безпеки і коректні шляхи роботи із ними у мережевому середовищі, протидії атакам та розпізнаванню підозрілої активності власноруч. Також потрібно регулярно перевіряти систему на відповідність нормативним вимогам [17].

Цілком природньо, що навіть із застосуванням детальних рекомендацій та наявністю проаналізованого функціонування підприємства у впровадженні чи підтримці архітектури нульової довіри час від часу будуть виникати проблеми: ніколи неможливо виключити ризики програмних збоїв, відмов обладнання чи інших технічних проблем. Проте важливо пам’ятати, що помилки трапляються у багатьох системах, а враховуючи зміни в багаторічній архітектурі підприємства не варто розраховувати на ідеальне безпроблемне впровадження нульової довіри, через що необхідно підготуватися до змін і кропіткої роботи для досягнення цілей і найкращих рішень безпеки.

ВИСНОВКИ

Архітектура нульової довіри є складним підходом захисту персональних даних та активів підприємства, що грунтується на трьох вагомих принципах:

- нікому не довіряти;
- завжди перевіряти;
- безпека вже порушена.

Ці основоположні принципи забезпечують новий спосіб забезпечення захищеності мереж: дотримання методів нульової довіри забезпечує найбільш чітку, змістовну та якісну перевірку усіх з'єднань як локальної, так і хмарної мережі. Підхід забезпечує прозору поетапну автентифікацію та ідентифікацію з'єднань, застосовуючи для цього політики керування доступом, принцип найменших привілеїв і захищені шлюзи в комплекті із документуванням та аналізом ініційованих сеансів.

Zero-trust архітектура не є конкретним додатком або чітко визначеною структурою робочого процесу: вона може різнитися залежно від необхідностей підприємств та організацій.

У роботі були висвітлені можливі для розробки і встановлення архітектури, а також був наданий деталізований аналіз усіх особливостей роботи моделі нульової довіри, вимогах до її застосування, переваги і недоліки такого підходу.

Важливою частиною роботи було формування практичних рекомендацій: в результаті був створений окремий розділ для визначення найоптимальніших рішень, які підвищать можливість успішного розгортання архітектури нульової довіри на підприємстві. Було визначено, що найкращим підходом введення моделі нульової довіри в експлуатацію є поступовість – поступове введення нових політик доступу та компонентів до мережі полегшить відслідковування

з’єднань чи можливих конфліктів при впровадженні, а також підготує і працівників підприємства до змін робочого процесу. Це рішення забезпечує:

- детальний аналіз та ідентифікацію фізичних ресурсів підприємства;
- ідентифікацію та автентифікацію користувачів;
- оцінку ризиків та способів зниження їх рівня чи повноцінного усунення небезпеки;
- визначаються найважливіші рішення нульової безпеки для потреб конкретного підприємства;
- тестування системи із нововведеними політиками;
- постійне вдосконалення впровадженої архітектури нульової довіри.

У цій роботі вдалося підсумувати наявні дані про підхід нульової довіри, а також розглянути можливі сценарії введення його в експлуатацію системи.

В результаті роботи було доведено, що підхід нульової довіри є одним з оптимальних рішень для забезпечення безпеки на сьогоднішній день, і хоча його розгортка має деякі труднощі, його переваги значно перекривають його недоліки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. H-X Довідник з рішень кібербезпеки. Дата оновлення: 22.04.2024. Режим доступу: https://www.h-x.technology/ua/security-solutions-full-review-ua (дата звернення: 12.05.2024)
2. Wikipedia Jericho Forum. 2023. Режим доступу: https://en.wikipedia.org/wiki/Jericho_Forum (дата звернення: 20.05.2024)
3. National Security Agency Embracing a Zero Trust Security Model. 2021. 7 с. Режим доступу: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF (дата звернення: 09.05.2024)
4. Jason Garbis, Jerry W. Chapman Zero Trust Security – An Enterprise Guide. 2021. 306 с.
5. В. Ткаченко Zero Trust, або Керована параноя. 2021. 6 с. Режим доступу: https://sib.com.ua/sib-05-120-2021/zero-trast.html (дата звернення 09.05.2024)
6. NIST Special Publication 800-207 Zero Trust Architecture. 2020. 59 с. Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (дата звернення: 10.05.2024)
7. Fortinet Document Library. Режим доступу: https://docs.fortinet.com/ztna (дата звернення 18.05.2024)
8. National Technology Security Coalition Check point infinity architecture. 2020. 19 с. Режим доступу: https://www.ntsc.org/assets/pdfs/cp-infinity-whitepaper.pdf (дата звернення: 06.05.2024)

9. IBM Cost of a Data Breach Report. 2023. Режим доступу: https://www.ibm.com/reports/data-breach?_ga=2.3019568.1436252282.1637663307-1392706600.1635762999 (дата звернення 15.05.2024)
10. Софтліст Еволюція безпеки: впровадження Zero Trust у корпоративному середовищі. 2023. Режим доступу: https://ua.softlist.com.ua/articles/evolyutsiya-bezopasnosti-vnedrenie-zero-trust-v-korporativnoy-srede/ (дата звернення 10.05.2024)
11. Packetlabs Only 1% of Companies Meet the Definition of Zero Trust. 2023. Режим доступу: https://www.packetlabs.net/posts/1-percent-meet-the-definition-of-zero-trust/#:~:text=While%20many%20organizations%20have%20implemented,and%20activities%20on%20the%20network (дата звернення: 13.05.2024)
12. Gather Gartner Predicts 10% of Large Enterprises Will Have a Mature and Measurable Zero-Trust Program in Place by 2026. 2023. Режим доступу: https://www.gartner.com/en/newsroom/press-releases/2023-01-23-gartner-predicts-10-percent-of-large-enterprises-will-have-a-mature-and-measurable-zero-trust-program-in-place-by-2026 (дата звернення: 08.05.2024)
13. IEEE Zero Trust Architecture (ZTA): A Comprehensive Survey. 2022. Режим доступу: https://ieeexplore.ieee.org/abstract/document/9773102 (дата звернення: 22.05.2024)
14. Keeper «What is Zero Trust?». 2024. Режим доступу: https://www.keepersecurity.com/resources/glossary/what-is-zero-trust/ (дата звернення: 16.05.2024)

15. Paul Toal, Krithiga Gopalan Approaching Zero Trust Security with Oracle Cloud Infrastructure. 2022. 35 с. Режим доступу: https://www.oracle.com/a/ocom/docs/whitepaper-zero-trust-security-oci.pdf (дата звернення: 14.05.2024)
16. NIST Special Publication 800-207A A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments. 2023. 31 с. Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207A.pdf (дата звернення: 11.05.2024)
17. ETSI TR 103 866 V1.1.1 Cyber Security (CYBER) Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls. 2023. 26 с. Режим доступу: https://www.etsi.org/deliver/etsi_tr/103800_103899/103866/01.01.01_60/tr_103866v010101p.pdf (дата звернення: 10.05.2024)
18. H-X Директива кібербезпеки NIS 2. 2023. Режим доступу: https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua (дата звернення: 06.05.2024)