Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» травня 2024 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Створення високорівневої моделі Zero Trust для IT інфраструктури»

Виконавець: студент ІІ курсу, групи КБм-21

_____ **Тарас КИРИЧУК**
(підпис) (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Микола БРАЇЛОВСЬКИЙ	
Нормоконтроль	Юрій БАБЕНКО	

Київ 2024

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» листопада 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувач КБм-21 (група) Киричука Тараса Михайловича (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Створення високорівневої моделі Zero Trust для IT інфраструктури

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 15.11.2023 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес аналізу традиційної моделі концепції Zero Trust.
Предмет досліджень	Політики традиційної моделі Zero Trust
Мета	Створення високорівневої моделі Zero Trust для IT-інфраструктури для забезпечення максимального рівня безпеки та відмови від довіри до будь-яких вузлів або користувачів, надаючи доступ лише на основі перевірених ідентифікаторів та автентифікаційних засобів, а також аналіз існуючих рішень які здатні забезпечити реалізацію високорівневої моделі Zero Trust

Вихідні дані для проведення роботи Недоліки традиційної моделі Zero Trust

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна удосконалено високорівневу модель Zero Trust, яка враховує специфіку IT інфраструктури конкретної організації, її потреби та вимоги до безпеки, що робить її унікальною в контексті конкретного бізнесу.

Практична цінність високорівнева модель Zero Trust може стати каталізатором для модернізації IT інфраструктури, спрямованої на забезпечення безпеки та ефективності в умовах постійно зростаючих загроз та вимог.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	17.11.2023 – 29.12.2023
Аналіз літературних джерел	30.12.2023 – 30.01.2024
Аналіз традиційної моделі Zero Trust	31.01.2024 – 21.02.2024
Виявлення недоліків традиційної моделі Zero Trust	22.02.2024 – 27.02.2024
Визначення кращих практик щодо впровадження високорівневої моделі Zero Trust	28.02.2024 – 06.03.2024
Визначення потенційних проблем на шляху впровадження Zero Trust	07.03.2024 – 12.03.2024
Опис концепції високорівневої моделі Zero Trust	13.03.2024 – 31.03.2024
Створення політик високорівневої моделі Zero Trust	01.04.2024 – 20.04.2024
Аналіз існуючих рішень які здатні покрити політики високорівневої моделі Zero Trust	21.04.2024 – 27.04.2024
Визначення технічного способу реалізації високорівневої моделі Zero Trust	28.04.2024 – 01.05.2024

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Оформлення пояснювальної записки згідно методичних рекомендацій	02.05.2024 – 12.05.2024
Подача пакету документів на розгляд ЕК	13.05.2024 – 17.05.2024

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Зниження збитків через цільові атаки на підприємства

Соціальний ефект Підвищення свідомості та відповідальності серед користувачів та працівників щодо безпеки інформації

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Тарас КИРИЧУК
(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 17.11.2023 р.
Термін подання кваліфікаційної роботи до ЕК 17.05.2024 р.

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Створення високорівневої моделі Zero Trust для IT інфраструктури»: 98 сторінок, 5 рисунків 11 таблиць та 53 літературних джерела.

Об’єктом дослідження є політики традиційної моделі концепції Zero Trust.

Метою роботи є створення високорівневої моделі Zero Trust для IT-інфраструктури з метою забезпечення максимального рівня безпеки та відмови від довіри до будь-яких вузлів або користувачів, надаючи доступ лише на основі перевірених ідентифікаторів та автентифікаційних засобів, а також аналіз існуючих рішень які здатні забезпечити реалізацію високорівневої моделі Zero Trust.

Методом дослідження є виявлення недоліків традиційної моделі концепції Zero Trust.

Результати роботи можуть використовуватися для покращення безпеки та впровадження високорівневої моделі Zero Trust в IT компаніях. Оцінити поточний рівень зрілості безпеки організації в контексті Zero Trust. Це дозволяє з'ясувати, наскільки ефективно організація використовує принципи Zero Trust у своїй інфраструктурі. Високорівнева модель Zero Trust допомагає визначити пріоритети для покращення безпеки на основі виявлених прогалин та можливостей.

Наукова новизна: удосконалено високорівневу модель Zero Trust, яка враховує специфіку IT інфраструктури конкретної організації, її потреби та вимоги до безпеки, що робить її унікальною в контексті конкретного бізнесу.

Актуальність роботи: високорівнева модель Zero Trust має першорядну актуальність у межах сучасного дискурсу кібербезпеки. Оскільки організації борються з ескалацією кіберзагроз і необхідністю зміцнення свого захисту, прийняття принципів «нульової довіри» стає ключовою стратегією зміцнення

безпеки. Традиційна модель Zero Trust, заснована на захисті периметра, дедалі більше застарівають перед обличчям складних кібератак. Високорівнева модель Zero Trust інкапсулює зміну парадигми до архітектури нульової довіри, виступаючи за безперервну автентифікацію та суворий контроль доступу.

Ключові слова: Створення моделі Zero Trust, IT інфраструктура, безпека мережі, автентифікація користувачів, сегментація мережі, контроль доступу, моніторинг систем, захист даних, ризик-орієнтоване управління, шифрування інформації, ідентифікація загроз, аудит безпеки, стратегія безпеки.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ZT	–	Zero Trust
ZTA	–	Zero Trust Architecture
PDP	–	Policy decision point
PEP	–	Policy enforcement point
IoT	–	Internet-of-Things
ML	–	Machine learning
TIC	–	Trusted internet connections
IT	–	Information Technology
BYOD	–	Bring your own device
NIST	–	National Institute of Standards and Technology
VPN	–	Virtual private network
Wi-fi	–	Wireless fidelity
DHCP	–	Dynamic host configuration protocol
API	–	Application programming interface
SoD	–	Segregation of duties
IAM	–	Identity and Access Management
FIDO	–	Fast IDentity Online
MFA	–	Multi-factor authentication
UBA	–	User behavior analytics
NTA	–	Network traffic analysis
WFH	–	Work from home
IT/OT	–	Information technology/Operational technology
CLI	–	Command line interface
ICAM	–	Identity, Credential, and Access Management
PIV	–	Personal identity verification
DNS	–	Domain name system

CI/CD	–	Continuous integration and continuous delivery
ST&E	–	Security test and Evaluation
SSO	–	Single Sign-On
SIEM	–	Security information and event management
SAML	–	Security assertion markup language
SSH	–	Secure shell protocol
DDoS	–	Distributed Denial-of-Service
NGFW	–	Next generation firewall
IDPS	–	Intrusion detection and prevention system
DLP	–	Data loss prevention
SOAR	–	Security orchestration, automation, and response
SDLC	–	Software development lifecycle

ЗМІСТ

РЕФЕРАТ 5
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 7
ВСТУП.....11
РОЗЖІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ZERO TRUST 14
1.1 Що таке нульова довіра та архітектура нульової довіри 14
1.2 Порівняльний аналіз між захистом периметра та нульовою довірою 18
1.3 Zero Trust в мережі..... 21
1.4 Недоліки традиційної моделі Zero Trust..... 25
Висновки до розділу 1 28
РОЗДІЛ 2 АРХІТЕКТУРА МОДЕЛІ ZERO TRUST 29
2.1 Огляд архітектури Zero Trust..... 29
2.2 Нерелевантні архітектури Zero Trust 34
2.3 Найкращі практики та кроки для успішного розгортання режиму нульової довіри 38
2.4 Потенційні проблеми на шляху впровадження до нульової довіри. 45
Висновки до розділу 2 47
3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ВИСОКОРІВНЕВОЇ МОДЕЛІ ZERO TRUST 49
3.1 Опис високорівневої моделі Zero Trust 49
3.2 Створення політик високорівневої моделі Zero Trust..... 56
Висновки до розділу 3 74
РОЗДІЛ 4 ПРАКТИЧНА РЕАЛІЗАЦІЯ МОДЕЛІ ZERO TRUST..... 75
4.1 Аналіз рішень Zero Trust 75
4.2 Комплексне впровадження розширеної моделі Zero Trust за допомогою кількох рішень.....88

Висновки до розділу 4 91
ВИСНОВКИ 92
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 93
ДОДАТОК А 99

ВСТУП

У сучасному цифровому середовищі, де загрози кібербезпеці стають все більш складними та поширеними, традиційні підходи до безпеки виявляються недостатніми для захисту конфіденційних даних і критичних активів організацій. Концепція нульової довіри з’явилася як багатообіцяюча зміна парадигми стратегії кібербезпеки, спрямована на забезпечення більш надійного захисту від загроз, що розвиваються.

Нульова довіра кидає виклик традиційному уявленню про безпеку на основі периметра, припускаючи, що жодному користувачу, пристрою чи мережевому компоненту не можна довіряти, незалежно від їхнього розташування в межах чи поза периметром мережі. Натомість Zero Trust виступає за безперервну перевірку та підтвердження довіри, вимагаючи автентифікації та авторизації кожного запиту на доступ, незалежно від передбачуваної надійності користувача чи пристрою.

Високорівнева модель Zero Trust являє собою структуровану структуру для організацій, щоб оцінити, оцінити та вдосконалити свою позицію безпеки нульової довіри. Визначаючи рівні зрілості та відповідні критерії для ключових аспектів впровадження Zero Trust, високорівнева модель Zero Trust дозволяє організаціям оцінити їх поточний стан готовності та прогрес у досягненні зрілого середовища Zero Trust.

Актуальність роботи Високорівнева модель Zero Trust має першорядну актуальність у межах сучасного дискурсу кібербезпеки. Оскільки організації борються з ескалацією кіберзагроз і необхідністю зміцнення свого захисту, прийняття принципів «нульової довіри» стає ключовою стратегією зміцнення безпеки. Традиційні моделі безпеки, засновані на захисті периметра, дедалі більше застарівають перед обличчям складних кібератак. Високорівнева модель Zero Trust інкапсулює зміну парадигми до архітектури нульової довіри, виступаючи за безперервну автентифікацію та суворий контроль доступу.

Метою роботи є створення високорівневої моделі Zero Trust для IT-інфраструктури з метою забезпечення максимального рівня безпеки та відмови від довіри до будь-яких вузлів або користувачів, надаючи доступ лише на основі перевірених ідентифікаторів та автентифікаційних засобів, а також аналіз існуючих рішень які здатні забезпечити реалізацію високорівневої моделі Zero Trust.

Завданнями кваліфікаційної роботи є:

1) Проаналізувати предметну область
2) Проаналізувати традиційну модель Zero Trust
3) Виявити недоліки традиційної моделі Zero Trust
4) Розробити розширену модель Zero Trust, де б враховувались всі недоліки традиційної моделі
5) Проаналізувати існуючі рішення які покривають високорівневу модель Zero Trust
6) На основі проаналізованих рішень надати спосіб технічної реалізації високорівневої моделі Zero Trust.

Об’єктом дослідження є політики традиційної моделі концепції Zero Trust.

Предметом дослідження є політики традиційної моделі Zero Trust.

Методом дослідження є виявлення недоліків традиційної моделі концепції Zero Trust, обширний аналіз наукової та технічної літератури щодо концепції Zero Trust, існуючих моделей та фреймворків, що використовуються для її реалізації, вивчення конкретних випадків впровадження Zero Trust у реальних організаціях або компаніях, дослідження архітектурних рішень та технічних реалізацій Zero Trust у різних організаціях.

Практичне застосування - Результати роботи можуть використовуватися для покращення безпеки та впровадження високорівневої моделі Zero Trust в IT компаніях. Оцінити поточний рівень зрілості безпеки організації в контексті Zero Trust. Це дозволяє з'ясувати, наскільки ефективно організація використовує принципи Zero Trust у своїй інфраструктурі. Високорівнева модель Zero Trust

допомагає визначити пріоритети для покращення безпеки на основі виявлених прогалин та можливостей.

Практична цінність роботи полягає в наступному:

- Створена високорівнева модель Zero Trust дозволяє організаціям створити більш ефективну систему захисту, зменшуючи вразливості та ризики, пов'язані з неавторизованим доступом до даних та ресурсів.
- Високорівнева модель Zero Trust може стати каталізатором для модернізації IT інфраструктури, спрямованої на забезпечення безпеки та ефективності в умовах постійно зростаючих загроз та вимог.
- Завдяки впровадженню моделі Zero Trust, організації можуть легше відповідати вимогам регуляторів та стандартів безпеки даних, таких як GDPR, HIPAA, а також внутрішнім політикам безпеки.
- Високорівнева модель Zero Trust дозволяє організаціям визначити конкретні стратегії та пріоритети для подальшого вдосконалення своєї моделі безпеки. Це може включати впровадження нових технологій, процесів або політик безпеки.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ZERO TRUST

1.1 Що таке нульова довіра та архітектура нульової довіри

Нульова довіра (Zero Trust) — архітектурний підхід, що передбачає, що будь-яка транзакція, сутність та особистість не є довіреними доти, доки не доведено, що їм можна довіряти, причому ця довіра має підтверджуватись знову і знову. Його мета – забезпечення мережевої безпеки. Підхід Zero Trust протилежний усталеній думці, що доки системи безпеки не виявить компрометації, мережа залишається безпечною.

Протягом останнього десятиліття цифрова трансформація підприємств дедалі більше набирає обертів. Цей процес включає використання хмарної архітектури, впровадження режиму віддаленої роботи, все ширше застосування хмарних рішень як послуг та інші зміни. Відповідно до цього фахівці з безпеки масштабували систему безпеки мережі та для посилення захисту ділили мережу на невеликі зони.

Така стратегія, на жаль, працювала на руку зловмисникам, надаючи їм більше можливостей для атак. Коли зловмисник отримує доступ до облікових даних користувача, він може розповсюджувати програми-вимагачі та додавати собі привілеї у міру просування через мережу.

Початкова увага має бути зосереджена на обмеженні ресурсів тими, хто потребує доступу та надання лише мінімальних привілеїв (наприклад, читання, запис, видалення), необхідних для виконання місії. Традиційно агентства (і корпоративні мережі загалом) зосереджені на захисті периметра, а автентифікованим суб’єктам надається авторизований доступ до великої кількості ресурсів у внутрішній мережі. У результаті несанкціоноване переміщення в навколишньому середовищі було однією з найбільших проблем для федеральних відомств. Довірені підключення до Інтернету та брандмауери периметра

агентства забезпечують надійні інтернет-шлюзи. Це допомагає блокувати зловмисників з Інтернету, але TIC і брандмауери периметра менш корисні для виявлення та блокування атак зсередини мережі та не можуть захистити суб'єктів за межами периметра підприємства (наприклад, віддалених працівників, хмарних служб, периферійних пристроїв тощо) [1].

Багатофакторна автентифікація підвищила надійність облікових даних, але додала лише один рівень автентифікації. Коли хакерам вдається увійти до мережі, вони зберігають постійний доступ до того часу, поки вийдуть із системи чи доки сама система не виведе їх. Використання особистих пристроїв на робочих місцях (BYOD), масовий перехід на віддалену роботу та розвиток хмарної архітектури призвели до появи нових вразливостей. У той же час навіть нові, посилені засоби забезпечення кібербезпеки з підвищеною видимістю зупиняються на кордоні корпоративної мережі та сліпі за межами цієї межі.

Підхід Zero Trust перевертає стару парадигму кібербезпеки з ніг на голову. Кібербезпека більше не визначається сегментами корпоративної мережі чи її кордоном. Довіра не надається за умовчанням жодному з'єднанню/активу підприємства чи приватної особи. Воно також не надається на підставі фізичного чи мережевого розташування, не має значення, чи розглядається з'єднання з Інтернетом чи всередині локальної мережі. При підході Zero Trust потрібно оцінювати ресурси, користувачів та активи окремо незалежно від того, де вони розташовані або хто ними володіє. Автентифікація виконується індивідуально для будь-якого корпоративного ресурсу і лише після перевірки користувачеві може бути наданий доступ до нього.

Кінцева мета – звести до нуля довіру до будь-якого мережного елемента, доки він не буде перевірений. Ані стандартів, ані сертифікатів для рішень, які реалізують концепцію нульової довіри, поки що немає. Перший крок у цьому напрямі зробив Національний інститут стандартів та технологій (NIST), заснований у 1901 році. На сьогоднішній день він є агентством Міністерства торгівлі США [2]. NIST надає інформацію про технології, вимірювання та

стандарти для США. Його місія – підвищення конкурентоспроможності технологій.

NIST створює стандарти в галузі комунікацій, технологій та забезпечення кібербезпеки. Як таких стандартів або сертифікації для рішень Zero Trust, він ще не створив, але випустив спеціальну публікацію NIST SP 800-207, в якій розглядаються цілі застосування архітектури нульової довіри.

“Нульова довіра” — термін, що означає набір парадигм кібербезпеки, що розвивається, і переносять захист зі статичного периметра мережі на користувачів, активи та ресурси. У світі кібербезпеки є різні думки про те, як розуміти термін «нульова довіра» [3]. Деякі вендори, скориставшись відсутністю визначеності, продають продукцію, марковану як продукти Zero Trust без жодних підстав. Тому неінформовані покупці можуть вирішити, що нульова довіра прив’язана до конкретного продукту. Насправді, це не так — і нові, і давно випущені продукти можуть стати будівельними блоками для створення архітектури нульової довіри (Zero Trust Architecture, ZTA). Zero Trust – революційний підхід до забезпечення кібербезпеки. Він враховує реальний стан справ у галузі комунікації між організацією та співробітниками, а також спосіб організації роботи [4].

«Чисту» архітектуру нульової довіри найпростіше побудувати, коли підприємство, визначивши основні робочі процеси та компоненти, створює корпоративну інфраструктуру з нуля. У довгостроковій перспективі, у міру зростання та зміни бізнесу, інфраструктуру продовжують розвивати відповідно до принципів нульової довіри.

Але на практиці більшість реалізацій Zero Trust буде тривалим процесом. Протягом деякого часу організації зберігатимуть певний баланс між забезпеченням безпеки на основі Zero Trust та на основі захисту периметра, і водночас поступово проводитиме заходи щодо модернізації. Щоб побудувати повноцінну ZTA, можливо, знадобиться кілька років. Процес, швидше за все, доведеться розбити на низку окремих проектів. Однак не можна досягти Zero Trust раз і назавжди. Оскільки бізнес та інфраструктура з часом розвиватимуться та

змінюватимуться, то відповідно і реалізація стратегії нульової довіри має продовжуватися.

Повноважені та схвалені суб’єкти (комбінація користувача, програми (або служби) і пристрою) можуть отримати доступ до даних за виключенням усіх інших суб’єктів (тобто зловмисників). Щоб зробити ще один крок далі, слово «ресурс» можна замінити на «дані», щоб ZT і ZTA стосувалися доступу до ресурсів (наприклад, принтерів, обчислювальних ресурсів, виконавчих механізмів Інтернету речей), а не лише доступу до даних.

Щоб зменшити невизначеності (оскільки їх неможливо усунути), основна увага приділяється автентифікації, авторизації та звуженню неявних зон довіри, зберігаючи при цьому доступність і мінімізуючи тимчасові затримки в механізмах автентифікації. Правила доступу створені якомога детальніше, щоб забезпечити найменші привілеї, необхідні для виконання дії в запиті як показано на рисунку 1 [5].

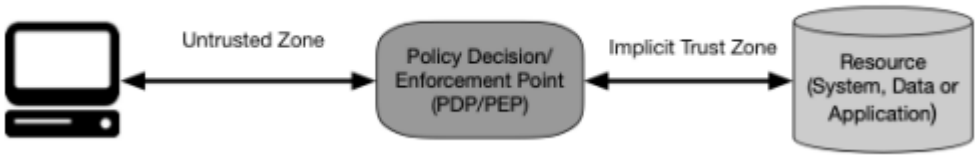

Рисунок 1.1 – Схема доступу в Zero Trust

Система повинна переконатися, що суб’єкт є автентичним, а запит дійсним. PDP/PEP приймає належне рішення, щоб дозволити суб’єкту отримати доступ до ресурсу. Це означає, що нульова довіра стосується двох основних сфер: автентифікації та авторизації. Загалом, підприємствам необхідно розробити та підтримувати динамічну політику доступу до ресурсів, що базується на оцінці ризиків, і налаштувати систему, яка гарантуватиме правильне та послідовне застосування цих політик для окремих запитів на доступ до ресурсів. Це означає, що підприємству не слід покладатися на передбачувану надійність, коли суб’єкт

відповідає базовому рівню автентифікації (наприклад, вхід в актив), усі наступні запити ресурсів вважаються однаково дійсними.

«Зона неявної довіри» представляє область, де всі об’єкти є довіреними принаймні до рівня останнього шлюзу PDP/PEP. Наприклад, розглянемо модель перевірки пасажирів в аеропорту. Усі пасажири проходять через контрольно-пропускний пункт аеропорту (PDP/PEP), щоб отримати доступ до виходу на посадку. Пасажири, співробітники аеропорту, екіпаж літака тощо перебувають у зоні терміналу, і всі особи вважаються довіреними. У цій моделі неявною зоною довіри є зона посадки. PDP/PEP застосовує набір елементів керування, щоб увесь трафік поза PEP мав загальний рівень довіри. PDP/PEP не може застосовувати додаткові політики за межами свого розташування в потоці трафіку. Щоб дозволити PDP/PEP бути максимально конкретним, неявна зона довіри має бути якомога меншою. Нульова довіра забезпечує набір принципів і концепцій щодо наближення PDP/PEP до ресурсу. Ідея полягає в тому, щоб чітко автентифікувати та авторизувати всі суб’єкти, активи та робочі процеси, які складають підприємство [6].

1.2 Порівняльний аналіз між захистом периметра та нульовою довірою

Традиційні моделі безпеки існують десятиліттями й базуються на припущенні, що всьому в мережі можна довіряти. Ці моделі спочатку були розроблені для захисту від зовнішніх загроз на початку розвитку мереж, коли більшість мереж були закриті й доступні лише для невеликої кількості людей. З розвитком Інтернету традиційні моделі безпеки розширювалися й охоплювали захист від більш складних загроз, таких як зараження зловмисним програмним забезпеченням. Основна ідея традиційних моделей безпеки — створити периметр навколо мережі та контролювати доступ до неї. Цей підхід, заснований на периметрі, часто називають моделлю «замок і рів». Мета полягає в тому, щоб не допустити зловмисників, щоб все всередині мережі було безпечним. Щоб досягти цього, традиційні моделі безпеки покладаються на технології та процеси безпеки

на основі периметра, такі як брандмауери, системи виявлення та запобігання вторгненням і антивірусне програмне забезпечення. Для захисту від кібератак.

Ці технології працюють разом, щоб контролювати та фільтрувати мережевий трафік, виявляти потенційні загрози та запобігати несанкціонованому доступу до мережі. Хоча традиційні моделі безпеки були ефективними для захисту від багатьох типів кібератак, вони мають обмеження. Наприклад, вони погано підходять для захисту від розширених постійних загроз (APT), які є дуже складними атаками, які можуть обійти захист на основі периметра. До широкого впровадження ZeroTrust існував підхід до безпеки мережі на основі периметра. Основна ідея тут полягає в тому, що будь-кому всередині корпоративної мережі можна довіряти, а будь-кому ззовні не довіряти. Це була провідна модель кібербезпеки вже понад 20 років. Однак останнє десятиліття виявило багато недоліків цього. Разом із безпекою на основі периметра часто приходить багаторівнева безпека. Рівнева безпека означала, що IT-команди встановили периметр безпеки навколо окремих активів. Ідея полягала в тому, що зловмиснику потрібно буде пройти через кілька рівнів безпеки, щоб отримати доступ до критичних активів [7].

З іншого боку, авторизовані користувачі можуть пройти повз ці рівні безпеки, оскільки вони вже перебувають у периметрі. Потім вони входили в машину, яка надавала їм доступ до IT-ресурсів. Підхід до периметра та багаторівневий підхід мав більше сенсу, коли мережа була майже повністю локальною та часто базувалася на Windows. Перше кільце безпеки зазвичай зосереджується на ідентифікації. Це означало, що користувачеві потрібен доступ до домену. Тоді наступний рівень міг бути захистом від шкідливих програм. Звідти третій рівень часто зосереджуватиметься на даних і програмах. Зовнішній рівень буде самим периметром мережі з VPN, брандмауерам, системою виявлення вторгнень та іншими функціями безпеки.

Нульова довіра та традиційні моделі безпеки — це дві різні парадигми безпеки, які відрізняються кількома ключовими аспектами. Нульова довіра — це модель безпеки, яка передбачає, що за замовчуванням ні всередині мережі, ні поза

нею не можна довіряти, а всі користувачі, пристрої та програми мають бути перевірені та автентифіковані перед доступом до будь-яких ресурсів. З іншого боку, традиційні моделі безпеки припускають, що все в мережі є надійним і покладаються на заходи безпеки на основі периметра для захисту від кібератак. Основні принципи Zero Trust включають явну перевірку, доступ з найменшими привілеями, мікросегментацію та безперервний моніторинг, тоді як традиційні моделі безпеки покладаються на засоби захисту на основі периметра, такі як брандмауери та антивірусне програмне забезпечення. Розглянемо відмінності між Zero Trust і традиційними моделями безпеки з точки зору контролю доступу, сегментації мережі, захисту даних, виявлення загроз і реагування на них, ідентифікації та керування доступом, відповідності та управління:

- Управління доступом

Традиційні моделі безпеки покладаються на єдиний рівень контролю доступу на периметрі мережі, який можуть обійти зловмисники, які отримали доступ до мережі. На відміну від цього, Zero Trust використовує багаторівневий підхід до контролю доступу, коли доступ надається на основі потреби та постійно перевіряється.

- Сегментація мережі

Традиційні моделі безпеки, як правило, покладаються на плоскі мережі з невеликою кількістю внутрішніх елементів керування, що полегшує зловмисникам пересування всередині мережі. Навпаки, Zero Trust використовує мікросегментацію для створення невеликих ізольованих сегментів у мережі та жорстко контролює доступ між ними.

- Захист даних

Традиційні моделі безпеки зосереджені на захисті даних на периметрі мережі, тоді як Zero Trust використовує наскрізне шифрування та методи запобігання втраті даних для захисту даних на всіх етапах їх життєвого циклу.

- Виявлення загроз і реагування

Традиційні моделі безпеки покладаються на методи виявлення на основі сигнатур для виявлення відомих загроз, тоді як Zero Trust використовує методи

виявлення на основі поведінки для виявлення підозрілої активності та потенційних загроз.

- Керування ідентифікацією та доступом

Традиційні моделі безпеки часто мають фрагментарний підхід до керування ідентифікацією та доступом із кількома системами та процесами для керування користувачами та доступом. На відміну від цього, Zero Trust використовує уніфікований підхід до ідентифікації та керування доступом з єдиною системою для керування всіма користувачами, пристроями та програмами.

- Відповідність та управління

Традиційні моделі безпеки часто мають проблеми з вимогами відповідності та керування, оскільки вони можуть не мати повного уявлення про всю мережеву діяльність. Навпаки, Zero Trust забезпечує цілісне уявлення про мережеву діяльність, що полегшує демонстрацію відповідності нормам і вимогам управління.

Zero Trust являє собою значну зміну традиційних моделей безпеки. У той час як традиційна безпека покладається на захист на основі периметра та передбачає, що все в мережі є довіреним, Zero Trust використовує більш цілісний підхід, зосереджуючись на постійному моніторингу та перевірці всієї мережевої активності [9]. Хоча впровадження Zero Trust може бути непростим, він пропонує надійніший і ефективніший підхід до захисту від кіберзагроз у сучасному дедалі складнішому та динамічному середовищі загроз.

1.3 Zero Trust в мережі

Є кілька основних припущень щодо підключення до мережі для будь-якої організації, яка використовує ZT під час планування та розгортання мережі. Деякі з цих припущень застосовуються до корпоративної мережевої інфраструктури, а деякі – до корпоративних ресурсів, що працюють на некорпоративній мережевій інфраструктурі (наприклад, загальнодоступні Wi-Fi або публічні хмарні постачальники). Ці припущення використовуються для спрямування формування

ZT. Мережа на підприємстві, що впроваджує ZT, повинна бути розроблена з урахуванням принципів ZT, викладених вище, і з наступними припущеннями:

- Вся корпоративна приватна мережа не вважається неявною зоною довіри.

Активи завжди повинні діяти так, ніби зловмисник присутній у корпоративній мережі, і зв’язок має здійснюватися найбезпечнішим доступним способом. Це передбачає такі дії, як автентифікація всіх з’єднань і шифрування всього трафіку.

- Пристрої в мережі можуть не належати або налаштовуватися підприємством.

Відвідувачі та/або контрактні послуги можуть включати некорпоративні активи, яким для виконання своєї ролі потрібен доступ до мережі. Це включає в себе політику використання власного пристрою, яка дозволяє суб’єктам підприємства використовувати пристрої, що не належать корпорації, для доступу до корпоративних ресурсів.

- Жодному ресурсу не можна довіряти.

Позиція безпеки кожного активу повинна бути оцінена за допомогою PEP, перш ніж буде надано запит до корпоративного ресурсу. Ця оцінка має бути постійною протягом усього сеансу. Корпоративні пристрої можуть мати артефакти, які дозволяють автентифікацію та забезпечують вищий рівень достовірності, ніж той самий запит, що надходить від некорпоративних пристроїв. Лише облікових даних суб’єкта недостатньо для автентифікації пристрою на корпоративному ресурсі.

- Не всі ресурси підприємства знаходяться в інфраструктурі підприємства.

Ресурси включають віддалені суб’єкти підприємства, а також хмарні сервіси. Активам, що належать або керуються підприємством, може знадобитися використовувати локальну (тобто некорпоративну) мережу для базового підключення та мережевих послуг (наприклад, вирішення DNS).

- Віддалені корпоративні суб’єкти та активи не можуть повністю довіряти своєму підключенню до локальної мережі.

Віддалені суб’єкти повинні вважати, що локальна (тобто некорпоративна) мережа є ворожою. Активи повинні припускати, що весь трафік відстежується та потенційно змінюється. Усі запити на з’єднання мають бути автентифіковані та авторизовані, а всі комунікації мають здійснюватися максимально безпечним способом (тобто забезпечувати конфіденційність, захист цілісності та автентифікацію джерела).

- Активи та робочі процеси, що переміщуються між корпоративною та некорпоративною інфраструктурою, повинні мати узгоджену політику та положення безпеки.

Активи та робочі навантаження повинні зберігати свою безпеку під час переміщення до корпоративної інфраструктури або з неї.

Це стосується пристроїв, які переміщуються з корпоративних мереж у некорпоративні мережі (тобто віддалених користувачів). Це також включає міграцію робочих навантажень із локальних центрів обробки даних до некорпоративних хмарних примірників.

Переваги мережі з нульовою довірою включають:

- Більша безпека. Атаки зазвичай відбуваються далеко від наміченої цілі, наприклад, корпоративної мережі. Зловмисники також часто намагаються отримати доступ схвалених користувачів, перш ніж переміщатися всередині мережі, щоб отримати доступ до цільових активів.
- Здатність керувати розосередженою інфраструктурою. Мережева інфраструктура стала більш складною та розосередженою, дані, програми та активи розкидані по багатьох хмарних і гібридних середовищах. Користувачі також працюють з багатьох місць, що ускладнює визначення захисного периметра. Насправді просто забезпечення безпеки периметра є застарілим підходом до складного завдання, яке значно відрізняється від компанії до компанії.

- Простіший підхід до безпеки. Історично організації використовували багаторівневі рішення безпеки для блокування зловмисників. Згодом це може створити прогалини в безпеці для зловмисників. Завдяки мережі з нульовою довірою безпека є бездоганною та краще інтегрованою в усі мережі.

Мережа з нульовою довірою покладається менше на спеціальне обладнання, а більше на нові підходи до безпеки. Їх можна включити в існуючу інфраструктуру за допомогою наступного процесу:

- Захищення поверхні. Поверхня захисту відноситься до будь-якого активу, який потрібно захистити.
- Шлюз сегментації. Сегментація – це термін для реорганізації більшої захисної поверхні. Прикладом є поділ усієї мережі на менші захисні поверхні, визначені цінністю, використанням, трафіком робочого процесу та іншими факторами. Шлюз сегментації фактично є брандмауером, який захищає певний сегмент у великій мережі.
- Мікросегментація. Мікросегмент — це менша захищена зона в межах великої мережі, захищена мікропериметром. Мікросегменти можна використовувати для застосування детального контролю доступу до певних робочих процесів.
- Впровадження брандмауера рівня 7. Брандмауер рівня 7 — це брандмауер нового покоління, який може перевіряти вміст пакетів, щоб використовувати більше даних у цьому вмісті для визначення критеріїв автентифікації.
- Багатофакторна автентифікація. Багатофакторна автентифікація є основним принципом мереж із нульовою довірою. Практично всі автентифікації з нульовою довірою є багатофакторними, тобто автентифікації вимагають кількох частин інформації або атрибутів, щоб дозволити доступ до мережевих ресурсів.
- Автентифікація по SMS. SMS-автентифікація є найпопулярнішим додатковим фактором, який сьогодні додається до автентифікації

користувача. Він широко використовується в службах електронної комерції та соціальних медіа. За допомогою SMS-автентифікації користувачі отримують SMS-коди, які вони надають мережі чи службі, щоб підтвердити свою особу.

- Доступ за найменшими привілеями. Доступ із найменшими привілеями стосується практики обмеження навіть довірених користувачів лише окремими програмами, послугами та даними, які їм негайно потрібні.
- Програмно-визначена мережа. У середовищі нульової довіри безпека забезпечується за замовчуванням за допомогою правил і політик, написаних і реалізованих програмним забезпеченням. Елементи середовища нульової довіри — сегменти та периметри в межах великих середовищ — самі визначаються програмним забезпеченням. Як і у випадку з програмно визначеною мережевою інфраструктурою, програмно визначені правила безпеки забезпечують більше контролю, кращу видимість і більше можливостей для автоматизації [10].

1.4 Недоліки традиційної моделі Zero Trust

Усі говорять про те, що Zero Trust є найкращою моделлю для просування безпеки. До певної міри це абсолютно правда, але те, про що не говорять, так це про проблеми та недоліки моделі Zero Trust , причому більшість розмов зосереджується на її перевагах. Як і в будь-якій моделі безпеки, Zero Trust має як плюси, так і мінуси. Зрештою, більшість організацій виявлять, що Zero Trust є найкращим рішенням для них. Але недоліки все одно потрібно буде усунути – іншими словами, щоб повністю реалізувати численні переваги моделі нульової довіри, ви повинні передбачити та вирішити проблеми моделі нульової довіри.

Впровадження Zero Trust локально забезпечує значні переваги з точки зору покращеної безпеки мережі, сегментації даних і ресурсів, а також зниження вразливості до внутрішніх загроз. Однак організації повинні ретельно розглянути

потенційні недоліки, включаючи час і зусилля, необхідні для впровадження, пов’язані витрати та вплив на продуктивність користувачів. Встановлення правильного балансу між безпекою та досвідом користувача має вирішальне значення для успішного впровадження підходу Zero Trust. Оцінюючи ці фактори, організації можуть приймати обґрунтовані рішення та розробляти надійні стратегії безпеки для захисту своїх цінних даних і систем [11].

Загалом в традиційній моделі Zero Trust можна виділити наступні недоліки:

- Нульова довіра може бути складною. Найбільша проблема Zero Trust полягає в тому, що його впровадження може бути складним. Той факт, що кожен користувач, пристрій і програма повинні бути автентифіковані та авторизовані, додає додатковий рівень складності, особливо для організацій з великою кількістю користувачів. Найкращий спосіб подолати цю проблему — співпрацювати з постачальником засобів безпеки, який спеціалізується на Zero Trust. Вони зможуть допомогти реалізувати рішення та забезпечити його ефективність.
- Нульова довіра вимагає зміни мислення. Інша проблема Zero Trust полягає в тому, що вона потребує зміни мислення як команди IT, так і служби безпеки. У традиційній моделі безпеки безпека була зосереджена на периметрі. Але з нульовою довірою безпека зосереджена на даних, а це означає, що IT-командам і командам безпеки потрібно змінити своє ставлення до безпеки. Найкращий спосіб подолати цю проблему — навчити IT-команду та команду безпеки моделі нульової довіри . Як тільки вони зрозуміють, як це працює.
- Нульова довіра вимагає більше робочої сили. Інша проблема Zero Trust полягає в тому, що для його впровадження та управління часто потрібно більше робочої сили. З традиційною моделлю безпеки на основі периметра існує лише один периметр для захисту. Але з нульовою довірою існує кілька периметрів, кожним з яких потрібно керувати та контролювати. Найкращий спосіб подолати цю проблему — знову ж таки співпрацювати з

постачальником засобів безпеки, який спеціалізується на Zero Trust. Вони зможуть допомогти реалізувати рішення та забезпечити його ефективність.

- Нульова довіра сповільнює роботу програми. Однією з найбільших скарг на Zero Trust є те, що він може сповільнити продуктивність програми. Це пояснюється тим, що кожен користувач, пристрій і програма повинні бути автентифіковані та авторизовані перед доступом до даних або програм. Найкращий спосіб подолати цю проблему — інвестувати в рішення, яке використовує адаптивну модель контролю доступу . Це дозволить динамічно контролювати доступ до даних і програм на основі профілю ризику користувача, пристрою або програми.
- Висока вартість продукту. Іншим недоліком Zero Trust є те, що його впровадження може бути дорогим. Це пояснюється тим, що для цього потрібно більше робочої сили та додаткові заходи безпеки, такі як багатофакторна автентифікація, що може збільшити загальну вартість системи. Рішенням може бути знайти рішення, які фактично заощадять гроші вашої організації, покращуючи ефективність вашої організації та безпеку IT.
- Нульова довіра може перешкодити продуктивності. Ще недоліком Zero Trust є те, що він іноді може перешкоджати продуктивності. Це пояснюється тим, що додаткові заходи безпеки, такі як багатофакторна автентифікація, можуть ускладнити роботу користувача. Користувачі можуть виявити, що вони не можуть отримати доступ до утиліт або файлів, до яких вони хочуть отримати доступ, і можуть виявити, що весь процес для них більш обмежувальний. В ідеалі цього не повинно статися, але завжди потрібно знайти баланс між наданням доступу та керуванням доступом. Найбільш релевантним рішенням може бути інвестиція в рішення Zero Trust, яке використовує адаптивну модель контролю доступу, модель без пароля або біометричну систему. Усе, що полегшує роботу користувача, швидше за все, буде дотримано та ефективніше. Слід також проводити

перевірки, щоб гарантувати, що працівники мають доступ до необхідних інструментів і утиліт [12].

Висновки до розділу 1

У цьому розділі було проведено аналіз концепції Zero Trust з точки зору історії розвитку і сучасних тенденцій в області кібербезпеки. Вивчено основні принципи, на яких ґрунтується підхід Zero Trust, такі як недовіра до всіх внутрішніх і зовнішніх мережевих джерел, необхідність автентифікації та авторизації для кожного запиту, постійний моніторинг активності користувачів та апаратних засобів, а також застосування принципу найменшого можливого доступу. Було детально проаналізовано ключові складові концепції Zero Trust, такі як мікросегментація мережі, засоби інтеграції та автоматизації процесів, централізоване керування правами доступу, захист даних у руху та спокої даних. Досліджено різноманітні методи та технології, які використовуються для реалізації підходу Zero Trust, зокрема сегментні фаєрволи, мікросервісна архітектура, технології шифрування та техніки аналізу потоків даних. На основі проведеного аналізу можна зробити висновок, що концепція Zero Trust стала однією з ключових стратегій у сучасних підходах до забезпечення кібербезпеки корпоративних мереж та інформаційних систем. Вона дозволяє зменшити ризики витоку даних, атаки з внутрішніх джерел та інші загрози, що можуть виникнути у сучасному інформаційному середовищі. Реалізація концепції Zero Trust вимагає комплексного підходу, включаючи не лише технічні засоби, але й культурні та організаційні зміни у відносинах з користувачами, персоналом та стейкхолдерами організа

РОЗДІЛ 2
АРХІТЕКТУРА МОДЕЛІ ZERO TRUST

2.1 Огляд архітектури Zero Trust

Необхідно пояснити те, називаються архітектурою нульової довіри або моделлю нульової довіри, оскільки вона повинна мати інші переваги, ніж нульова довіра. Щоб зрозуміти переваги для архітектур нульової довіри, слід пам’ятати про небезпеку виключної залежності від захисту єдиного периметра в корпоративних мережах.

Типове підприємство керує декількома внутрішніми мережами, кожна з яких є брандмауером по периметру, обчислення зловмисника автоматично стають довіреними та можуть переміщатися «збоку» по всій мережі. Останні галузеві звіти показують, що в середньому зловмиснику потрібно 1 година 24 хвилини, щоб перейти від початкової точки компрометації до інших серверів у межах зони, і що приблизно третина цих атак забезпечує «бічний» рух у нижній 30 хвилин. Як показано на рисунку 2.1 , якщо всередині зони виконується додаткова перевірка, щоб обмежити доступ до об’єктів/пристроїв, «бічний» рух супротивника може бути обмежений.

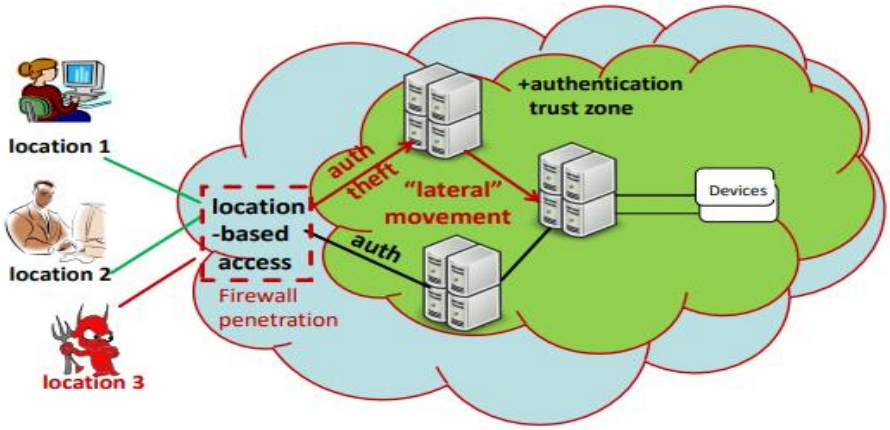

Рисунок 2.1 - Бічний рух супротивника (в місці 3) після крадіжки облікових даних [13]

Архітектури з нульовою довірою спрямовані на те, щоб усунути виняткову залежність від захисних периметрів (наприклад, на основі розташування), щоб обмежити «бокове» переміщення супротивника в скомпрометованій мережі. Це вимагає мікросегментації ресурсів зони (наприклад, мережевих пристроїв, служб і об’єктів даних) для створення менших прихованих зон довіри та надання доступу до ресурсів на основі: постійної перевірки атрибутів користувача, таких як унікальна ідентифікація, облікові дані (наприклад, ролі, дозволи, рівні доступу) і моніторинг моделей поведінки під час надання доступу. Це явно відхиляє перевірку, засновану на одноразовій перевірці довіри до кожного доступу до наступної перевірки, передбаченої захистом периметра, на користь підходу ніколи не довіряти та завжди перевіряти кожен доступ. Дотримання принципу найменших привілеїв, безвідмовність за замовчуванням та перевірка поведінки користувача після доступу. Це має на меті обмежити ефект проникнення периметра та запобігти «бічний» рух супротивника через скомпрометовану мережу. Противником завжди вважається мережа. Архітектури нульової довіри визнають, що будь-яка мікросегментація мережі та відповідна перевірка атрибутів доступу після входу створює нову, меншу неявну зону довіри.

Гіпотетично можливо припустити що всі кінцеві пристрої користувача мають унікальні ідентифікатори, розташування пристроїв відома, топологію та конфігурацію мережі, включаючи об’єкти даних високої цінності, легко визначити, і весь доступ до конфіденційних мережеві API враховуються, автентифікуються та контролюються. Коротше кажучи, можливе призначення мінімального набору дозволів кожному мікросегменту, і, в принципі, операція з найменшими привілеями може повністю підтримуватися. Однак на практиці мікросегментація мережі часто не вдається з кількох причин.

По-перше, багато підприємств страждають від розповсюдження кінцевих пристроїв, що зменшує видимість топології мережі. Більшість пристроїв користувачів не мають унікальних ідентифікаторів, що ускладнює реалізацію контролю над їхнім доступом до віддалених приватних хмар. Використання

протоколу динамічної конфігурації хоста (DHCP) для віддаленого принесення власних пристроїв ще більше підвищує незахищеність мережі. Крім того, неповне визначення розташування та переміщення цінних об’єктів даних у гібридних хмарах ще більше ускладнює їх призначення окремим мікросегментам.

По-друге, великі підприємства можуть використовувати понад десять тисяч API для створення нових програмних служб, програм і платформ у своїх мережах. Однак небагато з них можуть виявити та врахувати всі API, а коли вони це зроблять, менше автентифікують і авторизують доступ до цих API, залишаючи деяких підданими зовнішнім атакам. Мікросегментація спрямована на контроль доступу до API у неявних зонах довіри, але лише деякі підприємства впроваджують правильну автентифікацію доступу до API та керування доступом на основі суворих політик (наприклад, контроль доступу на основі ролей чи атрибутів), а не просто використовують брандмауери веб-додатків. Деякі також використовують безперервний зовнішній моніторинг для виявлення, а не запобігання за допомогою методів високої гарантії, порушень API.

По-третє, забезпечення роботи з найменшими привілеями для мікросегментів на великих підприємствах викликає значні технічні проблеми. На такому підприємстві інструменти на основі ML повинні створювати мікросегменти з найменшими привілеями на основі вивчених конфігурацій обладнання та програмного забезпечення та поведінки програм у кількох мережах. Фаза навчання цих інструментів може легко перевищити пару місяців; наприклад, поведінка всього програмного забезпечення та додатків повинна бути вивчена, перш ніж можна буде виконати мікросегментацію та призначити облікові дані/дозволи. На цьому етапі можуть виникнути принаймні дві проблеми. Оновлення конфігурації, виправлення та випуски програмного забезпечення для бізнесу в гнучких середовищах можуть мати місце, і це може призвести до безперервного виконання без завершення цієї фази. Крім того, обмежений час навчання може пропустити корпоративне програмне забезпечення, яке рідко використовується, наприклад операції наприкінці року та раз на рік тестування аварійного відновлення, і не вдасться призначити необхідні дозволи. Це може

призвести до збою цього програмного забезпечення через відсутність дозволів [14].

Відсутність інтеграції інструменту машинного навчання із розвідувальними Інтернет-каналами може призвести до виявлення зловмисних підключень мікросегментів до скомпрометованих сторонніх постачальників програмного забезпечення та навіть до іноземних серверів, контрольованих зловмисниками. Зловмисне підключення може тривати довго, перш ніж його виявляють; наприклад, у середньому більше двохсот вісімдесяти днів. Отже, мікросегментація великих корпоративних мереж для досягнення найменших привілеїв у роботі часто є грубим наближенням до реальності.

Існують випадки мінімальних неявних довірчих зон (тобто окремих пристроїв), для яких постійний моніторинг не може виявити міжзонні атаки. Наприклад, безперервний моніторинг не може виявити міжзонні атаки деякими шкідливими мікропрограмами.

Додатки в ізольованому програмному середовищі використовують функції введення-виведення, включаючи доступ до мережі та/або надійний шлях, що робить їх залежними від підсистеми вводу/виводу, що містить мільйони рядків коду в ненадійний хост-ОС. На рисунку 2.2 зображено ізольовану пісочницю 1 з ексклюзивним доступом до пристрою введення-виведення 1 та ізольовану пісочницю 2 з ексклюзивним доступом до пристрою 2. Дві програми ізольованого програмного середовища можуть містити окремі драйвери для своїх пристроїв введення-виведення [15].

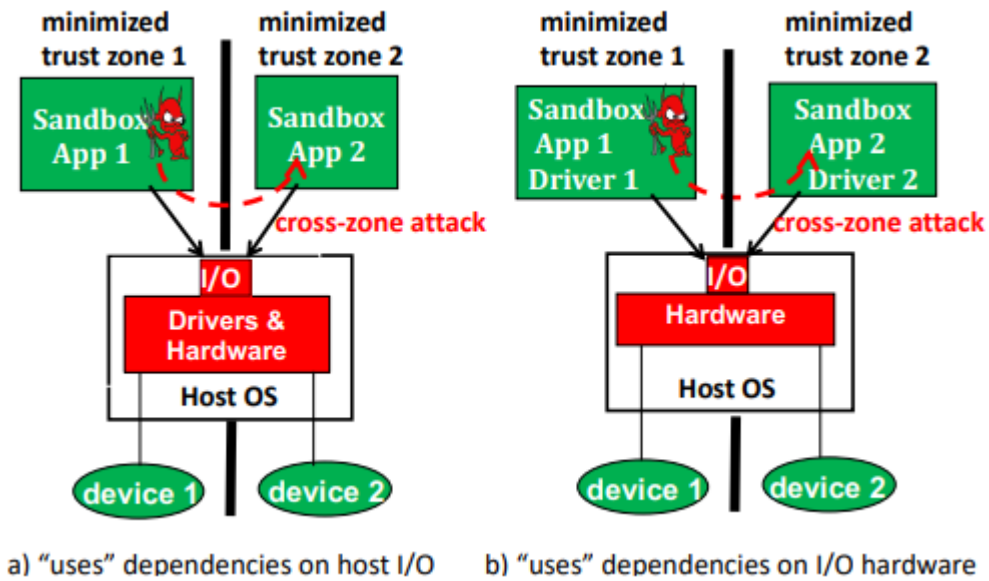

Рисунок 2.2 – Міжзональна атака ввімкнена через відсутність розділення вводу-виводу

В обох випадках зловмисне програмне забезпечення в одній зоні довіри може маніпулювати апаратним забезпеченням вводу-виводу базового хоста, щоб порушити безпеку іншої зони довіри. Загальні вразливості вводу/виводу та атаки на ізольовані програми, ілюструють цей простий випадок ненадійності. Наприклад, деяке обладнання вводу-виводу не в змозі забезпечити ексклюзивний зв'язок пристроїв вводу-виводу з їх ізольованим програмним середовищем і вибірково розділити дозволи на читання для передачі вводу-виводу. Інше обладнання вводу-виводу може вибірково пов'язувати лише контролери шини вводу-виводу з ізольованими програмами, але не окремими пристроями, а також окремі дозволи на читання й запис лише для передачі по шині. Незважаючи на те, що найсучасніше обладнання вводу-виводу (наприклад, IOMMU, PCIe та ACS)[16] може ексклюзивно пов'язувати окремі пристрої з їх ізольованими програмами та вибірково авторизувати передачу читання та запису, їх використання часто компромісне забезпечення правильності розділення передачі вводу-виводу для підвищена продуктивність, особливо в стандартних ОС. Вразливості, спричинені маніпулюванням зловмисним програмним забезпеченням апаратного забезпечення вводу-виводу в зоні довіри, що проникає,

спричиняють міжзональні атаки, які легко призводять до компрометації програм, незважаючи на силу ізольованого програмного середовища.

Усі архітектури з нульовою довірою дозволяють використовувати кінцеві точки дистанційного керування власним пристроєм у корпоративній мережі. Ці пристрої можуть представляти мінімізовані неявні зони довіри, якщо вони мають унікальні ідентифікатори, які не можуть бути пошкоджені (наприклад, шкідливим програмним забезпеченням у їх мікропрограмі чи ОС), і постійні криптографічні канали для своїх зовнішніх постачальників; наприклад, для оновлень захищеного мікропрограмного забезпечення і надання нового унікального ідентифікатора при зміні власності пристрою. Система Trusted Computing Group (TCG) може допомогти [17] з тим як забезпечити унікальну ідентифікацію пристрою і підтримувати постійні криптографічні канали для оновлення мікропрограми пристрою, включаючи сам механізм оновлення пристрою, а пізніше підтвердити завершення оновлення. Система Cider від Microsoft і її основи ілюструють, як реалізувати специфікації TCG. Наприклад, вони показують, як встановити криптографічний канал від мікропрограми BYOD до її зовнішнього постачальника, хоча це має передбачати деяку локальну ініціалізацію мікропрограми. Подібні криптографічні канали можна встановити між однозначно визначеними ОС і програмами та їхніми зовнішніми постачальниками.

2.2 Нерелевантні архітектури Zero Trust

Значною проблемою є те, що BYOD піддаються фізичним і внутрішнім атакам, які можуть пошкодити їх мікропрограму. Наприклад, деякі USB-пристрої дозволяють зловмиснику отримати прямий доступ до мікропрограми мікроконтролера пристрою. Шкідливе програмне забезпечення «evil innkeeper» може отримати доступ до користувача пристрою за відсутності користувача. Обидва можуть отримувати доступ до мікропрограми материнської плати та змінювати уніфікований розширюваний інтерфейс мікропрограми. Фізична

людина посередині може блокувати пристрій і змінювати мікропрограму його дискового контролера до того, як пристрій буде доставлено законному власнику. У всіх випадках програмне забезпечення пристрою може бути повторно налаштовано за допомогою шкідливого коду та відкритих ключів віддаленого зловмисника. Командно-контрольні сервери.

Припустимо, що повністю мінімізована неявна зона довіри містить один BYOD. Шкідливе мікропрограмне забезпечення BYOD може порушити перевірку атрибутів доступу під час входу в зону довіри, тим самим ілюструючи більш складний випадок несправності. Приклади використання зловмисного мікропрограмного забезпечення включають вдосконалені постійні загрози (APT), які дозволяють віддаленим зловмисникам використовувати відсутність цілісності мікропрограмного забезпечення пристрою, щоб обійти елементи керування доступом без використання будь-якого фізичного доступу до пристрою; напр. APT28 (Fancy Bear з атакою LoJax), APT29 (Cosy Bear викрадення результатів дослідження Covid-19), APT41 (великомасштабне шпигунство Double Dragon і нещодавня атака MoonBounce). Нешкідливі оновлення мікропрограми перевіреними постачальниками не гарантують відсутність вразливості нульового дня в оновленій мікропрограмі, якими можна скористатися віддалено [18]. Оновлення коду ядра ОС не гарантує відсутність недоліків безпеки серед мільйонів рядків коду ядра, які можуть уможливити експлойт вразливості мікропрограми та вставлення шкідливих програм у мікропрограму. Крім того, безперервний зовнішній моніторинг BYOD може не виявити наявність зловмисного програмного забезпечення і, таким чином, не може запобігти можливим між зональним атакам.

Припустимо, що кожна автономно адміністрована зовнішня (наприклад, постачальник, однорангова) мережа реалізує архітектуру нульової довіри з мінімізованими зонами довіри; перегляньте чотири (сірі) мінімізовані зони довіри на рисунку 2.3 [19]. Зламані зони постачальників можуть доставляти зловмисне програмне забезпечення до мінімізованих зон клієнтської мережі, демонструючи ненадійність без звернення клієнта. Наприклад, під час атаки ShadowHammer

(2019) зловмисник зламав сервер, на якому запущено службу живого оновлення ASUS, і отримав дійсний підпис під шкідливим оновленням мікропрограми. Атаки на ланцюги поставок можуть збільшити кількість скомпрометованих постачальників. Наприклад, нещодавній етичний хакер проти ланцюгів постачання порушив понад тридцять п’ять постачальників.

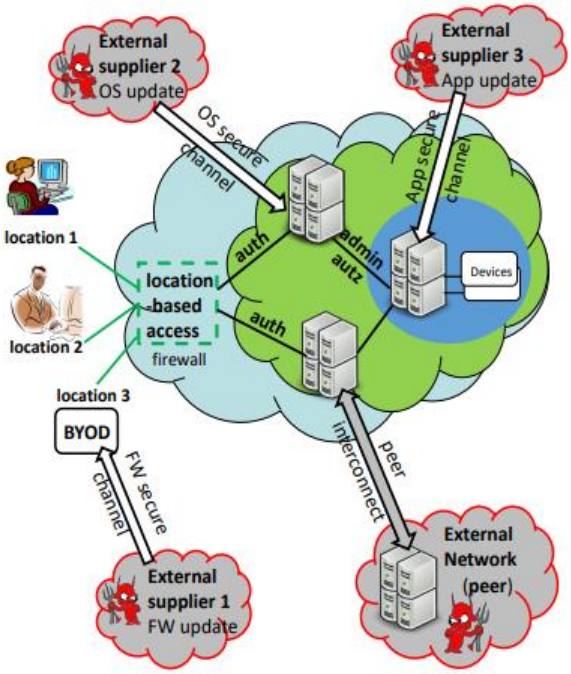

Рисунок 2.3 – Міжзонові атаки скомпрометованих зовнішніх постачальників і однорангових мереж

Архітектури з нульовою довірою також дозволяють попарно з’єднувати автономно керовані мережі. Ці мережі можуть бути підключені як однорангові мережі, як показано на рисунку 2.3, дозволяючи їхнім локальним користувачам і службам отримувати доступ до віддалених об’єктів і послуг, розташованих у їхніх однорангових мережах. Довіра автентифікації в однорангових взаємозв’язаних мережах розширює неявну зону довіри за допомогою адміністративних зон усіх її однорангових пристроїв і деяких із цих однорангових мереж. Зловмисник, який видає себе за законного користувача зовнішньої мережі шляхом зламу облікових даних користувача може розпочати міжзонову атаку на однорангову мережу. Єдиний вихід, доступний для однорангової мережі, — це завчасно знизити дозволи всіх віддалених користувачів (і, отже, зловмисників) на її локальні

об’єкти та служби, оскільки вона не може відрізнити законних від скомпрометованих віддалених користувачів. Однак це не може запобігти новим міжзональним атакам, оскільки зловмисник, який видає себе за законного користувача, отримає деякий нелегітимний доступ до об’єктів і послуг однорангової мережі, що свідчить про ненадійність.

Знижені дозволи також заборонять деяким віддаленим законним користувачам доступ до однорангової мережі, що свідчить про неповноту. Неможливість мінімізувати критичні адміністративні зони.

Поділ функцій не є мікросегментацією. Попереднє розділення адміністративних функцій на неявні зони довіри розрізняє функції адміністратора безпеки та аудитора та ставить їх у взаємозв’язок стримувань і противаг, що мінімізує довіру. Це відрізняється від мікросегментації адміністративних функцій, оскільки дотримання принципу найменших привілеїв недостатньо для реалізації відносин стримувань і противаг або інших політик розподілу обов’язків (SoD).

Хоча цей принцип допомагає мінімізувати зони довіри, він не завжди необхідний для поділу адміністративних функцій. Поділ адміністративних функцій створює залежності «використання» між функціями безпеки та політиками. Наприклад, функції системного адміністратора відокремлені від функцій центру сертифікації, які розділені на окремі функції менеджера сертифікатів і функції відновлення закритого ключа. Це розділення встановлює залежність «використання» функцій менеджера сертифікатів і відновлення закритого ключа від центру сертифікації та центру сертифікації від функцій адміністратора безпеки.

Функції відновлення закритого ключа також залежать від системи керування базами даних (СУБД) для архівації та відновлення закритого ключа, яка, у свою чергу, залежить від ядра ОС системи для встановлення своїх дозволів. Усі інші адміністративні функції залежать від функцій системного програміста. Оскільки кожна окрема адміністративна функція визначає неявну зону довіри, для

цих зон визначається функція безпеки та графік залежності політики, як показано на рисунку 2.4 [19].

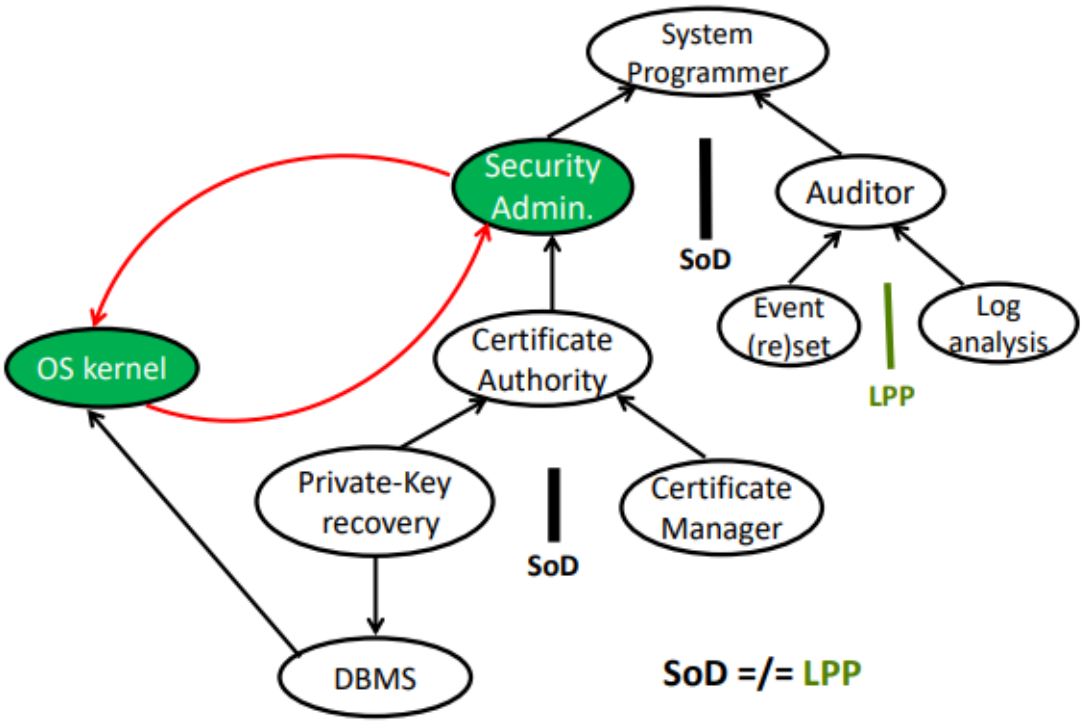

Рисунок 2.4 – Граф залежності між адміністративними зонами

На графі залежностей необхідно виконати мінімізацію адміністративної довірчої зони. Однак ані поділ зони довіри, ані мінімізація на графах залежностей не визначаються жодною архітектурою нульової довіри, включаючи NIST. Отже, передумова неявної мінімізації довірчої зони щодо архітектур нульової довіри не може виконуватися для критичних адміністративних зон.

2.3 Найкращі практики та кроки для успішного розгортання режиму нульової довіри

Zero Trust Security (ZTS) — це стратегічний підхід до кібербезпеки, який принципово усуває концепцію довіри з мережевої архітектури організації. Його основна мета — захистити цифрове середовище шляхом використання

сегментації мережі, запобігання бічному переміщенню, забезпечення запобігання загрозам рівня 7 і спрощення детального контролю доступу користувачів. Впровадження ZTS може принести значні переваги. Він покращує безпеку даних, мінімізуючи ризики витоку даних за допомогою суворого контролю доступу та постійної перевірки облікових даних користувача. Він також пропонує покращену видимість дій користувачів, уможливлюючи аналітику в реальному часі та реагування на загрози. Крім того, він забезпечує дотримання нормативних вимог, надаючи докладні журнали активності користувачів і звіти.

Однак впровадження ZTS може спричинити проблеми. Це вимагає суттєвих змін в організаційній культурі та стратегіях безпеки, які можуть бути складними та вимагати участі на всіх рівнях організації. Можуть знадобитися значні зміни в існуючій мережевій інфраструктурі, що може бути дорогим і трудомістким. Нарешті, досягнення повної видимості та контролю над усіма мережевими підключеннями може бути технічно складним, особливо в складних середовищах.

Планування успішної реалізації ZTS включає кілька ключових кроків. Спочатку потрібно визначити конфіденційні дані та їх розташування, щоб визначити необхідний рівень захисту. Потім відобразити потоки транзакцій , щоб визначити потенційні вразливості та області, які потребують додаткових заходів безпеки. Реалізація доступу з найменшими привілеями має вирішальне значення, надаючи користувачам лише той доступ, який їм потрібен, тим самим зменшуючи ризик несанкціонованого доступу та потенційних порушень даних. Перевірка та реєстрація всього трафіку має важливе значення для підтримки видимості та контролю над вашою мережею, що дозволяє швидко виявляти підозрілі дії та реагувати на них. Необхідно розглянути пов’язані ризики та можливості під час планування впровадження ZTS. Ризики включають можливі збої в роботі під час впровадження та відштовхування користувачів через уявні незручності. Однак такі можливості, як посилена безпека, зниження ризику витоку даних і покращена відповідність нормам, є значними. Розуміння основних компонентів ZTS, включаючи сегментацію мережі, перевірку особи користувача, перевірку безпеки пристрою та перевірку працездатності системи, допомагає в ефективному

плануванні. Це розуміння дає змогу розробити план впровадження, адаптований до конкретних потреб і вразливостей вашої організації, забезпечуючи комплексне й ефективне впровадження ZTS [20].

Впровадження ZTS потребує стратегічного підходу. Потрібно почати із розуміння мережі, визначення конфіденційних даних, їх потоку та вимог до доступу. Це створює основу для створення ефективної політики та контролю. Прийняти стратегію доступу з найменшими привілеями, надаючи користувачам лише мінімально необхідний доступ відповідно до їхніх ролей і обов'язків. Регулярно переглядати та коригувати ці привілеї, щоб запобігти повзучому виникненню привілеїв. Мікросегментація має вирішальне значення для обмеження бокового руху загроз. Варто розділити свою мережу на безпечні зони, ізолюючи критичні активи та дані від потенційних зломів. Підвищити безпеку за допомогою інструментів багатофакторної автентифікації (MFA) і керування ідентифікацією та доступом (IAM). MFA додає додатковий рівень перевірки, тоді як IAM забезпечує належну автентифікацію користувача та контроль доступу. Уникати поширених помилок, таких як поспішне впровадження або нехтування навчанням. ZTS не є універсальним рішенням, тому слід налаштувати його відповідно до конкретних потреб і вимог вашої організації. Ефективне планування, розуміння поточного стану безпеки, встановлення реалістичних цілей і ефективний розподіл ресурсів сприяють успішній реалізації. Регулярно відстежувати й оновлювати свою стратегію ZTS, щоб випереджати нові загрози.

Для вимірювання ефективності впровадження ZTS такі ключові показники, як зменшення кількості інцидентів безпеки , аналітика поведінки користувачів (UBA) , аналіз мережевого трафіку (NTA) , час реакції на інцидент безпеки та відповідність політикам , є вирішальними. Зменшення інцидентів безпеки означає успішне впровадження ZTS. UBA та NTA полегшують виявлення потенційних загроз шляхом моніторингу поведінки користувачів і мережевого трафіку. Коротший час реагування на інциденти безпеки вказує на ефективну модель ZTS, а регулярні аудити забезпечують дотримання політики ZTS. Ці показники відповідають найкращим практикам, таким як доступ із найменшими привілеями

, мікросегментація та постійний моніторинг. Доступ із найменшими привілеями мінімізує поверхню атаки, а мікросегментація запобігає бічному переміщенню загроз. Постійний моніторинг дозволяє виявляти загрози та реагувати на них у режимі реального часу. Регулярне відстеження та аналіз цих показників може виявити області для покращення, удосконалити стратегію ZTS і підтримувати надійну безпеку.

Впровадження ZTS часто створює такі проблеми, як складність дизайну, потенційний вплив на продуктивність, стійкість до змін і бюджетні обмеження. Поетапний підхід, починаючи з критичних активів і поступово поширюючись на менш важливі, може зменшити складність і забезпечити керований розподіл бюджету. Інвестиції в навчання та наймання кваліфікованого персоналу мають вирішальне значення для навігації зі складнощами ZTS. Розвиток культури безпеки може ще більше допомогти зменшити опір змінам. Автоматизація може спростити складну архітектуру ZTS, тим самим зменшивши навантаження на IT-команди. Перед впровадженням ZTS потрібно впевнитись в тому, що інфраструктура може витримати додаткове навантаження. Провести ретельне тестування, щоб виявити та усунути будь-які проблеми, які можуть порушити роботу. Вимірювання ефективності впровадження ZTS є життєво важливим для виявлення та подолання проблем. Регулярні перевірки та перевірки дають змогу зрозуміти продуктивність системи та області, які потрібно вдосконалити. Такі ключові показники, як кількість попереджених порушень, час безперебійної роботи системи та рівень відповідності користувачів, допомагають перевірити ефективність системи. Регулярне тестування на проникнення забезпечує надійність реалізації ZTS.

Рекомендації щодо архітектури нульової довіри [21]:

- Мікросегментація даних

Безпека перейшла від плоских мереж до багаторівневих і відокремлених мереж. Коротше кажучи, мікросегментація даних вимагає зберігання даних у різних зонах центру обробки даних. Наприклад, припустимо, що користувач або постачальник послуг має отримати доступ до даних в іншій зоні; необхідні

повторна автентифікація та повторна авторизація. Крім того, під час кібер-вторгнення мікросегментація пом’якшує бічні атаки та запобігає доступу зловмисників до критично важливих даних і програм за межами скомпрометованого сегмента (зони).

- Дотримання галузевих стандартів безпеки

Комплексні рамки та політики безпеки галузевих стандартів добре задокументовані. Таким чином, усвідомлюючи потреби підприємства та враховуючи ресурси, зусилля щодо впровадження стандартних рамок безпеки можуть знищити багатьох противників.

- Припустити порушення

Під час порушення вся робоча сила вживає всіх заходів, щоб пом’якшити атаку та обмежити шкоду. Він починається з автентифікації та авторизації користувачів, наскрізного шифрування, сегментації та інших дій протоколу, визначених політикою. Недовіра жодному користувачеві, навіть у межах цифрового периметру підприємства, формує міцну основу для досягнення повної безпеки.

- Захист особистості є фундаментальним

Надання переваги паролям перед біометричними даними та обов’язкова багатофакторна автентифікація є ключовим фактором для встановлення надійної ідентифікації користувачів. Підприємствам слід розробити альтернативні методи автентифікації та перевірки пристроїв і з’єднань сторонніх виробників. Крім того, безпека ідентифікаційної інформації має ідентифікувати джерела ефемерних об’єктів (походять із хмари), облікових записів служб та інших точок входу.

- Поверхня обмеження атаки

Наскрізне шифрування даних, захист кінцевих точок і пристроїв користувачів, керовані політикою протоколи безпеки, постійний моніторинг мережі, IDS (системи виявлення вторгнень), системи виявлення загроз, встановлення брандмауерів наступного покоління та інші протоколи та методи безпеки повинні бути де-факто практикою. Ця практика захищає поверхню атаки, допомагає виявити вразливі місця та зменшує ймовірність успішного

кібервторгнення. Крім того, допомагає регулярна оцінка ризиків і аналіз стану безпеки.

- Заміна застарілих систем

Хоча застарілі системи програмного та апаратного забезпечення можуть служити вашій меті, вони ставлять під загрозу безпеку. Впровадження сучасних протоколів безпеки на підприємстві із застарілою інфраструктурою є складним завданням. Заміна такої застарілої інфраструктури є першим кроком до покращення стану безпеки та досягнення ZTA. Крім того, застаріла інфраструктура, серед іншого, збирає вразливості нульового дня. Застаріла та погано керована інфраструктура є перешкодами для досягнення архітектури нульової довіри.

- Постійний моніторинг і виявлення загроз

Журнали загроз без контексту не приносять користі. Сучасні системи моніторингу та виявлення загроз створюють записи та звіти цілодобово. Великі дані можуть негативно вплинути на робочу силу, якщо цим записам бракує чітко визначеного контексту. Ми можемо додати контекст до даних за допомогою чітко визначеної політики щодо рівнів загроз, типів векторів загроз, реквізитів загроз, типових уразливостей та інших противників у системі. Використання можливостей машинного навчання та штучного інтелекту є вирішальним аспектом, коли справа доходить до моніторингу та виявлення.

Середовище B2B — це конгломерат бізнес-суб’єктів, що включає виробників, постачальників послуг і посередників на різних рівнях. Для безперебійного функціонування підприємства часто дозволяють іншим організаціям входити в свою мережу. Для безперебійного функціонування необхідна повна впевненість у безпеці підприємства, і ZTA забезпечує це. Нижче наведено список випадків, які допоможуть вам зрозуміти адаптацію ZTA в різних компаніях:

- Інфраструктура OT

Гарантує, що лише автентифіковані та авторизовані користувачі (робоча сила) беруть участь у роботі заводу. Допомагає контролювати офлайн- та онлайн-середовища завдяки попередньо визначеним політикам безпеки.

- WFH

Робота з дому/віддалена робота усуває потребу у великих офісних приміщеннях. Однак це також створює безліч проблем з безпекою. Архітектура нульової довіри гарантує, що співробітник (після MFA) входить лише з перевірених пристроїв, шифрування трафіку та моніторинг у реальному часі.

- Дозвіл сторонніх постачальників послуг

Багато сторонніх постачальників послуг поширюють гарантію на пристрої IoT лише в тому випадку, якщо їм дозволено входити в мережу підприємства. У таких випадках завдяки мікросегментації – основоположному компоненту архітектури нульової довіри – обмежує будь-який доступ до корпоративних та інших мереж.

- Точки введення даних (споживач)

Небагато служб працюють краще за умови постійного введення та подачі від споживача. Ці Дані обробляються в режимі реального часу для надання послуг. ZTA допомагає відокремити корпоративні та споживчі портали обслуговування та направляє дані споживачів до місця призначення, не передаючи їх через всю мережу.

- Робота з декількома хмарними провайдерами

Сучасні підприємства вибирають кілька хмарних постачальників для PaaS (платформа як послуга), IaaS (інфраструктура як послуга) і SaaS (програмне забезпечення як послуга). Безпека інфраструктури та додатків має життєво важливе значення при роботі з кількома варіантами хмари. ZTA забезпечує необхідну безпеку, дозволяючи користувачам безпечно отримувати доступ до порталу через MFA.

Після впровадження ZTS постійна оцінка та вдосконалення є життєво важливими. Це передбачає регулярні аудити, оперативне встановлення виправлень, оновлення та навчання співробітників для адаптації до нової моделі

безпеки. Дуже важливо бути в курсі нових кіберзагроз і відповідно коригувати стратегію ZTS. Пам’ятайте, ZTS — це не одноразовий проект, а довгострокове зобов’язання проактивної кібербезпеки.

По суті, успішне впровадження ZTS вимагає повного розуміння IT-інфраструктури організації, потоків даних і поведінки користувачів у поєднанні з відданістю постійному вдосконаленню та адаптації до середовища загроз, що постійно змінюється.

2.4 Потенційні проблеми на шляху впровадження до нульової довіри

Впровадження безпеки з нульовою довірою не означає розгортання однієї технології чи рішення. Натомість це переосмислення підходу підприємства до безпеки мережі. Щоб досягти середовища нульової довіри, потрібно застосувати цілісний підхід і почати з нуля. Найбільшою перешкодою тут є те, що можуть залишитися приховані прогалини у захисті, особливо якщо замінюється застарілі рішення безпеки.

Було б чудово, якби блокування мережі було таким же простим, як натискання перемикача Zero Trust Security. Але реальність така, що потрібно запровадити нову модель безпеки. Це означає ідентифікацію користувачів і пристроїв, розгортання інструментів моніторингу, налаштування контролю доступу тощо. Крім того, потрібне безпечне апаратне та програмне забезпечення, яке забезпечує безпеку зусиль щодо розгортання та керування.

Щоб подолати цю перешкоду, потрібно поступово впроваджувати нульову довіру. Це допоможе визначити ключові області, які потребують негайної уваги, а також допоможе запобігти тому, щоб прогалини залишилися непоміченими або стали серйозними вразливими місцями.

Іншою проблемою безпеки без довіри є потенційна втрата продуктивності. У певному сенсі ця перешкода виникає поряд із проблемою потреби постійного управління.

Впроваджуючи позицію нульової довіри та продовжуючи керувати нею, можна несвідомо створити проблеми з налаштуваннями безпеки. Наприклад, при впровадженні ZTS неправильно налаштувано свій брандмауер або введено помилку в CLI, що потім ненавмисно блокує цілий відділ співробітників. Вирішення цієї проблеми може потребувати швидкого вирішення або може зайняти кілька днів. Тим часом працівники відстають і не можуть працювати оптимально.

Найкращий спосіб подолати це — це, знову ж таки, поступове впровадження позиції нульової довіри та регулярне керування своїми рішеннями. Здійснюючи перехід від застарілих систем, можна вирішити подібні невдачі, коли вони з'являться до вас. Не потрібно вирішувати низку проблем одразу, а натомість можна визначити конкретні області, які викликають збої.

Часто організаціям потрібна повна інвентаризація їх активів, включаючи обладнання, програмне забезпечення та сховища даних. З чітким розумінням того, які активи існують та їх критичність, стає легше ефективно впровадити ZTA. Організації повинні ідентифікувати та класифікувати свої активи, визначити конфіденційність своїх даних і розуміти взаємодію між суб'єктами, ресурсами, програмами та службами. Ця інформація має вирішальне значення для розробки відповідних засобів контролю доступу та стратегій сегментації в рамках ZTA.

Багато організацій мають значні інвестиції в застарілі корпоративні та хмарні технології. Перехід до архітектури нульової довіри вимагає від організацій збалансувати залучення існуючих інвестицій і поступову інтеграцію нових технологій відповідно до принципів ZTA. Розуміння того, як застарілі системи вписуються в структуру ZTA, і забезпечення їх сумісності з новими рішеннями безпеки може бути складним. Це може вимагати проведення ретельної оцінки, прийняття стратегічних рішень щодо модернізації або заміни та вирішення проблем сумісності під час процесу інтеграції.

ZTA вимагає від організацій визначити та пріоритезувати свої ресурси та розробити чітку політику для надання доступу на основі конкретних умов. Ці умови можуть виходити за рамки традиційних факторів, таких як ідентичність і

роль суб’єкта, і можуть включати такі атрибути, як суб’єкт і розташування ресурсу, час доби, стан справності пристрою тощо. Розробка та управління такою політикою може бути складною для організацій, оскільки вимагає повного розуміння їхніх ресурсів, критичності даних і пов’язаних профілів ризику. Розробка політики також вимагає постійного моніторингу та оновлень для адаптації до нових загроз і мінливих вимог до бізнесу.

Незважаючи на те, що купівля продуктів по частинах може залишати прогалини, не існує універсальних, готових продуктів із нульовою довірою. Насправді нульова довіра — це не окремий продукт, а також не окремий підхід чи техніка. Це філософія та структура політик, технологій і людей, які необхідно застосовувати: безпека робочої сили, безпека пристроїв, безпека робочого навантаження, безпека мережі, безпека даних, видимість і аналітика, а також автоматизація та оркестровка.

Запровадження підходу нульової довіри може потенційно вплинути на продуктивність. Основна проблема нульової довіри полягає в тому, щоб заблокувати доступ без припинення робочих процесів. Людям потрібен доступ до конфіденційних даних для роботи, спілкування та співпраці. Якщо люди змінюють ролі та опиняться заблокованими для файлів або програм на тиждень, продуктивність може різко впасти. У гіршому випадку втрата продуктивності стає більшою проблемою, ніж сама кібербезпека. Нульова довіра вимагає спілкування між широким спектром даних, пристроїв, систем і людей. Якщо будь-яке з них не відповідає іншим, продуктивність і співпраця можуть постраждати.

Висновки до розділу 2

У цьому розділі було ретельно розглянуто ключові аспекти та компоненти моделі Zero Trust з метою розуміння їхньої ролі в забезпеченні кібербезпеки.
Аналізуючи цей розділ, можна зробити наступні висновки:
В розділі було з’ясовано, що сутність моделі Zero Trust полягає в тому, що будь-який доступ до ресурсів мережі або даних повинен бути автентифікованим,

авторизованим та налаштованим на безпеку, незалежно від того, чи знаходиться користувач в межах мережі організації чи поза її межами.

Дослідження включало в себе розгляд ключових компонентів архітектури моделі Zero Trust, таких як мікросегментація мережі, системи ідентифікації та автентифікації, централізоване керування правами доступу, а також моніторинг та аналіз активності користувачів.

В розділі були розглянуті різноманітні технологічні рішення, які можуть бути використані для реалізації архітектури Zero Trust, такі як мікро сегментовані фаєрволи, системи шифрування даних, технології моніторингу мережі та аналізу потоків даних.

Важливість інтеграції та автоматизації: Було відзначено, що успішна реалізація моделі Zero Trust вимагає інтеграції різних компонентів та автоматизації процесів, щоб забезпечити ефективне функціонування та реагування на потенційні загрози.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ ВИСОКОРІВНЕВОЇ МОДЕЛІ ZERO TRUST

3.1 Опис високорівневої моделі Zero Trust

Високорівнева модель Zero Trust є доповненням традиційної моделі нульової довіри яка застосовується для наступних ресурсів [22]:

- Облікові записи
- Пристрої
- Мережа
- Додатки
- Дані

Кожний з ресурсів містить загальні деталі та наступні можливості: видимість і аналітика, автоматизація та оркестровка.

Також в даній моделі повинні дотримуватись 7 принципів:

- Усі джерела даних і обчислювальні послуги вважаються ресурсами.

  Мережа може складатися з кількох класів пристроїв. Мережа також може мати невеликі пристрої, які надсилають дані до агрегаторів/сховищ, програмне забезпечення як послуга (SaaS), системи, що надсилають інструкції виконавчим механізмам, та інші функції. Крім того, підприємство може вирішити класифікувати особисті пристрої як ресурси, якщо вони можуть отримати доступ до корпоративних ресурсів.
- Весь зв’язок захищений незалежно від розташування мережі.

Розташування в мережі саме по собі не означає довіри. Запити на доступ від активів, розташованих у корпоративній мережевій інфраструктурі (наприклад, усередині периметра застарілої мережі), мають відповідати тим самим вимогам безпеки, що й запити на доступ і зв’язок із будь-якої іншої мережі, що не належить підприємству. Іншими словами, довіра не повинна надаватися автоматично на основі того, що пристрій знаходиться в мережевій інфраструктурі підприємства.

Усю комунікацію слід здійснювати максимально безпечним доступним способом, захищати конфіденційність і цілісність і забезпечувати автентифікацію джерела.

- Доступ до окремих ресурсів підприємства надається на основі кожного сеансу.

Довіра до запитувача оцінюється перед наданням доступу. Доступ також має бути надано з найменшими привілеями, необхідними для виконання завдання. Це може означати лише «колись нещодавно» для цієї конкретної транзакції та не може відбуватися безпосередньо перед ініціюванням сеансу або виконанням транзакції з ресурсом. Однак автентифікація та авторизація для одного ресурсу не нададуть автоматично доступ до іншого ресурсу.

- Доступ до ресурсів визначається динамічною політикою.

Організація захищає ресурси, визначаючи, які ресурси вона має, хто є її членами (або здатність автентифікувати користувачів із об'єднаної спільноти) і який доступ до ресурсів потрібен цим членам. Для нульової довіри ідентифікатор клієнта може включати обліковий запис користувача (або ідентифікатор служби) і будь-які пов'язані атрибути, призначені підприємством цьому обліковому запису або артефактам для автентифікації автоматизованих завдань. Стан активу запиту може включати такі характеристики пристрою, як встановлені версії програмного забезпечення, мережеве розташування, час/дата запиту, поведінка, що спостерігалася раніше, і встановлені облікові дані. Поведінкові атрибути включають, але не обмежуються, автоматизовану аналітику предметів, аналітику пристроїв і виміряні відхилення від спостережуваних моделей використання. Політика — це набір правил доступу на основі атрибутів, які організація призначає суб'єкту, активу даних або програмі. Атрибути середовища можуть включати такі фактори, як мережеве розташування запитувача, час, повідомлення про активні атаки тощо. Ці правила та атрибути базуються на потребах бізнес-процесу та прийнятному рівні ризику. Правила доступу до ресурсів і дозволів на дії можуть відрізнятися залежно від чутливості ресурсу/даних. Принципи найменших привілеїв застосовуються для обмеження як видимості, так і

доступності. Підприємство відстежує та оцінює цілісність і захист усіх належних і пов’язаних активів.

Жоден актив не є надійним. Підприємство оцінює стан безпеки активу під час оцінки запиту ресурсу. Підприємство, яке впроваджує ZTA, має встановити безперервну діагностику та пом’якшення або подібну систему для моніторингу стану пристроїв і додатків і за потреби застосовувати латки/виправлення. Активи, знають уразливості та/або не керовані підприємством можуть розглядатися по-іншому (включаючи відмову в усіх підключеннях до ресурсів підприємства), ніж пристрої, що належать або пов’язані з підприємством і які вважаються найбільш безпечними. Це також може стосуватися пов’язаних пристроїв (наприклад, особистих пристроїв), яким може бути дозволено доступ до деяких ресурсів, але не до інших. Це також вимагає наявності надійної системи моніторингу та звітності, щоб надавати актуальні дані про поточний стан ресурсів підприємства [23].

Уся автентифікація та авторизація ресурсів є динамічною та суворо дотримується до того, як буде дозволено доступ. Це постійний цикл отримання доступу, сканування та оцінка загроз, адаптація та постійна переоцінка довіри до поточного спілкування. Очікується, що підприємство, яке впроваджує ZTA, матиме системи управління ідентифікацією, обліковими даними та доступом (ICAM) і системи управління активами. Це включає використання багатофакторної автентифікації для доступу до деяких або всіх ресурсів підприємства.

Постійний моніторинг із можливою повторною автентифікацією та повторною авторизацією відбувається протягом усіх транзакцій користувача, як визначено та забезпечується політикою (наприклад, на основі часу, запит на новий ресурс, модифікація ресурсу, виявлена аномальна активність суб’єкта), яка прагне досягти балансу безпеки, доступності, зручності використання, і економічна ефективність. Підприємство збирає якомога більше інформації про поточний стан активів, мережевої інфраструктури та комунікацій і використовує її для покращення своєї безпеки. Підприємство має збирати дані про стан безпеки

активів, мережу запити на трафік і доступ, обробляти ці дані та використовувати будь-яку отриману інформацію для покращення створення та застосування політики. Ці дані також можна використовувати для надання контексту для запитів доступу від суб'єктів [24].

Оскільки компанії переходять до впровадження оптимальної нульової довіри, відповідні рішення все більше покладаються на автоматизовані процеси та системи, які більш повно інтегруються між основними системами та більш динамічно забезпечують виконання рішень. Кожен ресурс може прогресувати у власному темпі та може прогресувати швидше, ніж інші, доки не знадобиться координація між компонентами. Однак таку координацію можна досягти лише за допомогою можливостей і залежностей, сумісних між собою та корпоративним середовищем.

Це дозволяє та визначає поступовий розвиток до нульової довіри, розподіляючи витрати в часі, а не повністю наперед.

У відповідності до кроків NIST для переходу до нульової довіри компаніям слід оцінити свої поточні корпоративні системи, ресурси, інфраструктуру, персонал і процеси, перш ніж інвестувати в можливості нульової довіри (зокрема для ресурсів і функцій, описаних у цій моделі). Ця оцінка може допомогти компаніям визначити існуючі можливості для підтримки подальшої нульової зрілості довіри та недоліків для визначення пріоритетів. Компанії також можуть планувати можливості для координації можливостей між компонентами, щоб увімкнути детальний контроль доступу з найменшими привілеями та зменшити додаткові ризики [25].

Три етапи шляху ZTM, які просуваються від традиційної до початкової, розширеної та оптимальної, сприятимуть федеральному запровадженню ZTA. Кожен наступний етап вимагає вищих рівнів захисту, деталізації та складності для прийняття.

Компанії повинні використовувати наступні рівні для кожного етапу, щоб визначити зрілість для кожного компонента технології нульової довіри та забезпечити узгодженість у високорівневій моделі [26]:

• Традиційний — налаштовані вручну життєві цикли (тобто від встановлення до виведення з експлуатації) і призначення атрибутів (безпека та журналювання); статичні політики безпеки та рішення, які стосуються одного ресурсу від зовнішніх систем; найменші привілеї встановлюються лише при забезпеченні; закриті ресурси забезпечення виконання політики; ручне реагування та розгортання пом’якшення; і обмежена кореляція залежностей, журналів і телеметрії.

• Початковий — початок автоматизації призначення атрибутів і конфігурації життєвих циклів, рішень і примусового виконання, а також початкові багаторівневі рішення з інтеграцією зовнішніх систем;
деякі чутливі зміни до найменших привілеїв після надання; і сукупна видимість для внутрішніх систем.

• Розширений — там, де це можливо, автоматизований контроль життєвого циклу та призначення конфігурацій і політик із координацією між компонентами; централізований контроль видимості та ідентифікації; забезпечення виконання політики, інтегроване між основними принципами; відповідь на заздалегідь визначені пом’якшення; зміни до найменших привілеїв на основі оцінки ризику та положення; а також підвищення обізнаності в масштабах підприємства (включаючи зовнішні ресурси).

• Оптимальний — повністю автоматизований, своєчасний життєвий цикл і призначення атрибутів активам і ресурсам, які самостійно звітують за допомогою динамічних політик на основі автоматизованих/спостережуваних тригерів; динамічний доступ з найменшими привілеями (достатній і в межах порогів) для активів і їх відповідних залежностей на рівні підприємства; міжсистемна сумісність із постійним моніторингом; і централізована видимість із повною обізнаністю про ситуацію.

Ці рівні, пов’язані з кожним ресурсом, дозволяють компаніям оцінювати, планувати та підтримувати інвестиції, необхідні для просування до ZTA та переході до нульової довіри за п’ятьма різними ресурсами: користувачі, пристрої, мережі, програми та дані. Кожен ресурс також містить загальні відомості про

видимість і аналітику, автоматизацію та оркестровку, а також можливості керування для підтримки інтеграції з цим ресурсом і всієї моделі.

Ці три наскрізні можливості висвітлюють дії для підтримки взаємодії функцій [27]:

• Видимість і аналітика: видимість відноситься до спостережуваних артефактів, які є результатом характеристик і подій у корпоративних середовищах. Зосередженість на аналізі даних, пов'язаних з кіберпростором, може допомогти прийняти рішення, полегшити реагування та створити профіль ризику для розробки проактивних заходів безпеки до того, як станеться інцидент.

• Автоматизація та оркестровка: нульова довіра повністю використовує автоматизовані інструменти та робочі процеси, які підтримують функції реагування на безпеку в продуктах і службах, зберігаючи нагляд, безпеку та взаємодію процесу розробки для таких функцій, продуктів і послуг.

• Управління: управління стосується визначення та пов'язаного забезпечення виконання політик, процедур і процесів компанії з кібербезпеки в межах і між основними компонентами для управління підприємством агенції та пом'якшення ризиків безпеки на підтримку принципів нульової довіри та виконання вимог.

Наскрізні можливості видимості та аналітики, автоматизації та оркестровки та управління надають можливості для інтеграції просування по кожному з п'яти стовпів. У міру того, як агентства розвивають ці здібності щодо певного компонента, вони також можуть розвивати кожен потенціал незалежно від компонентів. Видимість і аналітика підтримує комплексну видимість, яка інформує про політичні рішення та полегшує реагування. Можливості автоматизації та оркестровки використовують ці знання для підтримки надійних і спрощених операцій для обробки інцидентів безпеки та реагування на події, щойно вони виникають. Управління дозволяє компаніям керувати та контролювати свої регуляторні, правові, екологічні, федеральні та операційні вимоги та політики для підтримки прийняття рішень на основі ризиків.

Можливості управління також гарантують наявність відповідних людей, процесів і технологій для підтримки місії, ризиків і дотримання цілей.

Хоча високорівнева модель охоплює багато аспектів кібербезпеки, критично важливих для підприємств, він не стосується інших аспектів кібербезпеки, таких як діяльність, пов’язана з реагуванням на інциденти, особливості журналювання, моніторинг, оповіщення, криміналістичний аналіз, прийняття ризику, відновлення. Інші аспекти та найкращі практики для управління станом кібербезпеки компанії включені до функцій високорівневої моделі. Незважаючи на те, що високорівнева має на меті бути виключною, вона стосується проблем, пов’язаних із системами технологіями, певними класами пристроїв Інтернету речей, або широкого включення нових технологій, таких як платформи обману, автентифіковані брандмауери веб-додатків, поведінкова аналітика, тощо.

Такі методології, як рекомендації щодо найкращого включення машинного навчання та можливостей штучного інтелекту в рішення з нульовою довірою, не включені в цю модель. Компанії повинні вжити заходів для моніторингу та оцінки ефективності та цілісності своїх можливостей безпеки, базової інфраструктури та політик для виявлення неавторизованого доступу та змін у міру розвитку кожного компонента. Компаніям слід бути обережними, щоб не створювати нових можливостей для використання та не послаблювати протоколи безпеки. Дослідження та розробки необхідні для ефективного забезпечення цілісності систем програмного та апаратного забезпечення в масштабах підприємств.

Плануючи впровадження даної моделі, компанії повинні приймати рішення на основі факторів, які включають ризик, місію, вимоги та операційні обмеження. Хоча ця модель, як правило, узгоджується з єдиним адміністративним доменом або межами акредитації федерального підприємства, агентства також повинні оцінити, як їхня взаємодія із зовнішніми партнерами, зацікавленими сторонами та постачальниками послуг впливає на їх.

Цю модель слід розглядати не як суворий набір вимог, а як загальний посібник, який допоможе компаніям успішно впровадити свої політики та прийняти загальну покращену позицію кібербезпеки.

3.2 Створення політик високорівневої моделі Zero Trust

Якщо говорити про користувачів, то компанії повинні забезпечувати доступ користувачів і організацій до потрібних ресурсів у потрібний час для відповідної мети, не надаючи надмірного доступу. Компанії повинні інтегрувати ідентифікаційні дані, облікові дані та рішення для керування доступом, де це можливо, на всій території підприємства, щоб забезпечити надійну автентифікацію, надати індивідуальну авторизацію на основі контексту та оцінити ризик ідентифікації для користувачів і організацій агентства. Компанії повинні інтегрувати свої сховища ідентифікаційних даних і системи керування, де це доцільно, щоб підвищити обізнаність про ідентифікаційні дані підприємства та пов’язані з ними обов’язки та повноваження.

Таблиця 3.1 Необхідні компоненти високорівневої моделі Zero Trust для облікових записів

Функція	**Традиційний**	**Початковий**	**Розширений**	**Оптимальний**
Автентифікація	Компанія автентифікує особу за допомогою паролів або багатофакторної автентифікації зі статичним доступом для ідентифікації сутності.	Компанія перевіряє автентифікацію за допомогою MFA, який може містити паролі як один із факторів і вимагає перевірки кількох атрибутів об’єкта (наприклад, мови або діяльності).	Компанія починає автентифікувати користувача за допомогою стійких до фішингу MFA та атрибутів, включаючи початкове впровадження MFA без пароля через FIDO2 або PIV.	Компанія постійно перевіряє ідентифікаційні дані за допомогою стійкого до фішингу MFA, а не лише під час початкового доступу.

Сховища ідентифікаційних даних	Компанія використовує лише самокеровані локальні (тобто сплановані, розгорнуті та підтримувані копанією) сховища ідентифікаційних даних	Компанія має поєднання самокерованих сховищ ідентифікаційної інформації та розміщеного сховища ідентифікаційної інформації (наприклад, хмара або інше агентство) з мінімальною інтеграцією між сховищем(ями) (наприклад, Single Sign-on.).	Компанія починає безпечну консолідацію та інтеграцію деяких самокерованих і розміщених сховищ.	Компанія надійно інтегрує свої сховища ідентифікаційних даних у всіх партнерів і середовищ, якщо це необхідно.
Оцінка ризиків	Компанія робить обмежені визначення щодо ризику ідентифікації (тобто ймовірності того, що особистість скомпрометована).	Компанія визначає ризик ідентичності за допомогою ручних методів і статичних правил для підтримки видимості.	Компанія визначає ризик ідентичності за допомогою певного автоматизованого аналізу та динамічних правил для інформування рішень щодо доступу та заходів реагування	Компанія визначає ризик ідентифікації в реальному часі на основі постійного аналізу та динамічних правил для забезпечення постійного захисту.
Керування доступом	Компанія надає постійний доступ із періодичним переглядом як для привілейованих, так і для непривілейованих облікових записів.	Компанія авторизує доступ, у тому числі для запитів на привілейований доступ, термін дії якого закінчується після автоматичного перегляду	Компанія авторизує доступ на основі потреб і сеансу, у тому числі для запит привілейованого доступу, адаптований до дій і ресурсів.	Компанія використовує автоматизацію для авторизації своєчасного та достатнього доступу, адаптованого до окремих дій та індивідуальних потреб у ресурсах

Таблиця 3.2 Необхідні критерії до розширеної моделі Zero Trust для облікових записів

Критерій	Традиційний	Початковий	Розширений	Оптимальний
Видимість і аналітика	Компанія збирає журнали активності користувачів і об’єктів, особливо для привілейованих облікових даних, і виконує певний рутинний ручний аналіз.	Компанія збирає журнали активності користувачів і об’єктів і виконує рутинний ручний аналіз і деякий автоматизований аналіз з обмеженою кореляцією між типами журналів.	Компанія виконує автоматичний аналіз деяких типів журналів активності користувачів і організацій і розширює збір для усунення прогалин у видимості	Компанія підтримує повну видимість і ситуаційну обізнаність у всьому підприємстві, виконуючи автоматичний аналіз типів журналів активності користувачів, включаючи аналітику на основі поведінки.
Можливість автоматизації та оркестровки	Компанія вручну організовує (підключає, виключає та вимикає) самокеровані ідентифікатори (користувачі та об’єкти) з невеликою інтеграцією та виконує регулярний перегляд	Компанія вручну керує привілейованими та зовнішніми ідентифікаторами та автоматизує оркестрування непривілейованих користувачів і самокерованих об’єктів	Компанія вручну керує привілейованими ідентифікаторами користувачів і автоматизує оркестрування всіх ідентифікаторів з інтеграцією в усі середовища	Компанія автоматизує оркестровку всіх ідентифікацій із повною інтеграцією в усі середовища на основі поведінки, реєстрації та потреб у розгортанні.
Спроможність до керування	Компанія реалізує політику ідентифікації (автентифікація, облікові дані, доступ, життєвий цикл тощо) із застосуванням технічних механізмів viastatic і перевірки вручну.	Компанія визначає та починає впроваджувати політики ідентифікації для примусового застосування в масштабах підприємства з мінімальною автоматизацією та оновленнями вручну.	Компанія реалізує політики ідентифікації для примусового застосування в масштабах підприємства з автоматизацією та періодично оновлює політики.	Компанія реалізує та повністю автоматизує загальнокорпоративну політику ідентифікації для всіх користувачів і організацій у всіх системах із безперервним контролем і динамічними оновленнями.

Таблиця 3.3 Політики розширеної моделі Zero Trust для облікових записів

Політики	**Традиційний**	**Початковий**	**Розширений**	**Оптимальний**
Identity	• Пароль або MFA • Локальні сховища ідентифікаційної інформації • Обмежені оцінки ризику ідентифікації • Постійний доступ з періодичним переглядом	• MFA з паролем • Самокеровані та розміщені сховища облікових даних • Ручна оцінка ризику ідентифікації • Закінчення доступу з автоматичним переглядом	• Стійкий до фішингу MFA • Консолідація та безпечна інтеграція сховищ облікових даних • Потреба в сеансовому доступі • Ідентифікація виключно в корпоративних додатках	• Постійна перевірка та аналіз ризиків; • Інтеграція на рівні підприємства; • Індивідуальний, за потреби автоматизований доступ

Пристрої можуть належати компанії або бути власністю співробітників, партнерів або відвідувачів. Компанії повинні захищати всі пристрої агентства, керувати ризиками авторизованих пристроїв, які не контролюються корпорацією, і запобігати доступу неавторизованих пристроїв до ресурсів. Керування пристроєм включає ведення динамічної інвентаризації всіх активів, включаючи їх апаратне забезпечення, програмне забезпечення, мікропрограми тощо, а також їхні конфігурації та пов’язані з ними вразливості, коли вони стають відомими.

Багато пристроїв представляють певні проблеми ZTA, і їх потрібно оцінювати в кожному конкретному випадку в рамках процесу, заснованого на ризиках. Наприклад, мережеве обладнання, принтери та інші можуть пропонувати обмежені можливості для автентифікації, видимості та безпеки.Підприємства, які використовують політику BYOD, ймовірно, матимуть менше можливостей для підтримки видимості та контролю таких пристроїв. Технологічний ландшафт для пристроїв продовжує змінюватися, і оскільки агентства впроваджують додаткові пристрої у свої підприємства, їм потрібно буде продовжувати керувати зростаючими ризиками, пов’язаними з цими пристроями. У деяких випадках агентства можуть бути не в змозі прийняти вказівки для певних підмножин своїх пристроїв. Корпорації також зіткнуться з труднощами в забезпеченні довірених

пристроїв і їхніх послуг, які не закінчилися, і все ще охоплені їхньою підтримкою протягом усього терміну служби, оскільки застарілі пристрої часто мають більшу кількість непомітних вразливостей, доступних неправильних конфігурацій і невідомих ризиків . Однак, незважаючи на ці проблеми, агенції все одно повинні мати змогу досягти значного прогресу на шляху до ZTA [28].

Управління локальними обчислювальними активами передбачає документування та керування фізичними активами (пристроями). Оскільки компанії переходять до хмарних середовищ, це створює нові міркування та можливості для управління та відстеження хмарних і віртуальних активів агентств. Хмарні активи включають обчислювальні ресурси (наприклад, віртуальні машини, сервери або контейнери), ресурси зберігання (наприклад, блокове сховище або сховище файлів), активи платформи (наприклад, бази даних, веб-сервери, шини/черги повідомлень) і мережеві ресурси (наприклад, , віртуальні мережі, VPN, шлюзи, служби DNS тощо) і віртуальні ресурси, пов’язані з іншими керованими хмарними службами (наприклад, моделі штучного інтелекту) [29].

Таблиця 3.4 Необхідні компоненти високорівневої моделі Zero Trust для пристроїв

Функція	**Традиційний**	**Початковий**	**Розширений**	**Оптимальний**
Застосування політик та моніторингу відповідності	Компанія має обмежений (якщо такий є) доступ (тобто можливість перевіряти поведінку пристрою) щодо відповідності пристрою за допомогою кількох методів забезпечення політики або керування програмним забезпеченням, конфігураціями чи вразливими місцями.	Організація отримує характеристики пристрою (наприклад, ключі, токени, користувачів тощо), але має обмежені механізми контролю. Організація має попередній базовий процес схвалення використання програмного забезпечення та надсилання оновлень і змін конфігурації на пристрої.	Компанія має перевірену інформацію (тобто адміністратор може перевіряти та перевіряти дані на пристрої) щодо початкового доступу до пристрою та забезпечує відповідність більшості пристроїв і віртуальних активів.	Корпорація постійно перевіряє інформацію та забезпечує відповідність протягом усього терміну служби пристроїв і віртуальних активів. Агентство інтегрує

			Агентство використовує автоматизовані методи для керування пристроями та віртуальними активами, затвердження програмного забезпечення, виявлення вразливостей і встановлення виправлень.	керування пристроєм, програмним забезпеченням, конфігурацією та вразливістю в усіх середовищах агентства, включно з віртуальними активами.
Управління ризикам и активів і ланцюгі в поставок	Компанія не відстежує фізичні чи віртуальні активи на рівні підприємства чи між постачальниками й керує власним ланцюгом постачання пристроїв і послуг у нестандартному порядку з обмеженим уявленням про ризики підприємства.	Агентство відстежує всі фізичні та деякі віртуальні активи та керує ризиками ланцюга постачання, встановлюючи політику та базові показники контролю відповідно до рекомендацій, використовуючи надійну структуру (наприклад, NIST SCRM.)	Підприємство починає розробку комплексного корпоративного уявлення про фізичні та віртуальні активи за допомогою автоматизованих процесів, які можуть функціонувати між кількома постачальниками для перевірки придбань, відстеження циклів розробки та надання оцінок третіми сторонами.	Агентство має повний або майже реальний огляд усіх активів постачальників і постачальників послуг, автоматизує управління ризиками в ланцюжку постачання, якщо це можливо, будує операції, які допускають збої в ланцюзі постачання, і використовує найкращі практики.
Доступ до ресурсів	Корпорація не вимагає видимості пристроїв або віртуальних активів, які використовуються для доступу до ресурсів.	Агентство вимагає, щоб деякі пристрої або віртуальні активи повідомляли про характеристики, а потім використовували цю інформацію для схвалення доступу до ресурсів.	Початковий доступ агентства до ресурсу враховує інформацію про перевірений пристрій або віртуальні активи.	Доступ агентства до ресурсів враховує аналіз ризиків у реальному часі на пристроях і віртуальни

				х активах.
Захист пристрою від загроз	Компанія вручну розгортає засоби захисту від загроз на деяких пристроях.	Агентство має деякі автоматизовані процеси для розгортання та оновлення можливостей захисту від загроз для пристроїв і до віртуальні активи з обмеженим застосуванням політики та інтеграцією моніторингу відповідності.	Компанія починає консолідувати можливості захисту від загроз для централізованих рішень для пристроїв і віртуальних активів і інтегрує більшість цих можливостей із застосуванням політики та моніторингом відповідності.	Компанія має централізоване рішення безпеки для захисту від загроз, розгорнуте з розширеними можливостями для всіх пристроїв і віртуальних активів і єдиним підходом до захисту пристроїв від загроз, застосування політики та моніторингу відповідності

Таблиця 3.5 Необхідні критерії до розширеної моделі Zero Trust для пристроїв

Критерій	**Традиційний**	**Початковий**	**Розширений**	Оптимальний
Видимість і аналітика	Компанія використовує фізично маркований інвентар і обмежений моніторинг програмного забезпечення, щоб регулярно перевіряти пристрої з певним ручним аналізом..	Компанія використовує цифрові ідентифікатори (наприклад, адреси інтерфейсів, цифрові теги) разом із ручною інвентаризацією та моніторингом кінцевих точок пристроїв, якщо вони доступні. Деякі пристрої та віртуальні активи агентства проходять автоматизований аналіз (наприклад, програмне	Компанія автоматизує збір інвентаризації (включно з моніторингом кінцевих точок на всіх стандартних пристроях користувача, наприклад, настільних комп’ютерів і ноутбуків, мобільних телефонів, планшетів та їхніх віртуальних активів), а також виявлення аномалій	Компанія автоматизує збір стану всіх підключених до мережі пристроїв і віртуальних активів, співвідносячи їх з ідентифікаторами, проводячи кінцеву точку моніторинг і виявлення аномалій для інформування про доступ до ресурсів. Агентство відстежує шаблони надання та/або скасування надання віртуальних активів

		сканування) для виявлення аномалій на основі ризику.	для виявлення неавторизованих пристроїв.	на наявність аномалій.
Можливість автоматизації та оркестровки	Компанія вручну забезпечує, налаштовує, та/або реєструє пристрої на підприємстві.	Компанія починає використовувати інструменти та сценарії для автоматизації процесу надання, налаштування, реєстрації та/або деініціалізації для пристроїв і віртуальних активів.	Компанія запровадила механізми моніторингу для виявлення та відключення або ізоляції невідповідних (вразливий, неперевірений сертифікат; незареєстрована mac-адреса) пристроїв і віртуальних активів.	Компанія має повністю автоматизовані процеси для надання, реєстрації, моніторингу, ізоляції, відновлення та деініціалізації пристроїв і віртуальних активів.
Спроможність до керування	Компанія встановлює деякі правила щодо життєвого циклу своїх традиційних і периферійних комп'ютерних пристроїв і покладається на ручні процеси для обслуговування (наприклад, оновлення, виправлення, очищення) цих пристроїв.	Компанія встановлює та забезпечує дотримання політики щодо закупівлі нових пристроїв, життєвого циклу нетрадиційних комп'ютерних пристроїв і віртуальних активів, а також регулярного моніторингу та сканування пристроїв.	Компанія встановлює політику для всього підприємства щодо життєвого циклу пристроїв і віртуальних активів, включаючи їх перелік і звітність, з деякими автоматизованими механізмами примусового виконання.	Компанія автоматизує політики для життєвого циклу всіх підключених до мережі пристроїв і віртуальних активів на підприємстві.

Мережа відноситься до відкритого середовища зв'язку, включаючи типові канали, такі як внутрішні мережі агентства, бездротові мережі та Інтернет, а також інші потенційні канали, такі як стільникові канали та канали на рівні програми, які використовуються для передачі повідомлень.

ZTA дозволяють відійти від традиційних підходів до безпеки, зосереджених на периметрі, і дозволяють агентствам керувати внутрішніми та зовнішніми потоками трафіку, ізолювати хости, застосовувати шифрування, сегментувати діяльність і покращувати видимість мережі в масштабах підприємства. ZTA

дозволяють реалізовувати елементи керування безпекою ближче до додатків, даних та інших ресурсів і розширюють традиційний захист на основі мережі та покращують захист. Мережа може обробляти кожну програму унікально щодо її вимог щодо доступу, пріоритету, доступності, підключень до залежних служб і шляхів підключення. Ці вимоги до мережевої програми можна зафіксувати як профіль програми, а потім повторити профілі розглядаються як клас руху [30].

Таблиця 3.6 Необхідні компоненти високорівневої моделі Zero Trust для мереж

Функція	**Традиційний**	**Початковий**	**Розширений**	**Оптимальний**
Сегментація мережі	Компанія визначає свою мережеву архітектуру, використовуючи великий периметр/макросегментацію з мінімальними обмеженнями щодо доступності в межах сегментів мережі. Агентство також може покладатися на мультисервісні взаємозв'язки (наприклад, VPN-тунелі масового трафіку). Забезпеченням, конфігураціями чи вразливими місцями.	Компанія починає розгортати мережеву архітектуру з ізоляцією критичних робочих навантажень, обмеженням підключення до принципів найменшої функції та переходом до взаємозв'язків, пов'язаних із послугами.	Компанія розширює розгортання механізмів ізоляції кінцевих точок і профілів додатків на більшу частину своєї мережевої архітектури з мікропериметрами входу/виходу та взаємозв'язкам и для певних послуг.	Мережева архітектура агентства складається з повністю розподілених вхідних/вихідних мікропериметрів і великої мікросегментації на основі профілів додатків із динамічним своєчасним і достатнім підключенням для зв'язків між послугами.

Управління мережевим трафіком	Компанія вручну впроваджує статичні мережеві правила та конфігурації для керування трафіком під час надання послуг, з обмеженими можливостями моніторингу (наприклад, моніторинг продуктивності додатків або виявлення аномалій) і ручними аудитами та переглядами змін профілю для критично важливих програм.	Компанія створює профілі додатків із різними функціями керування трафіком і починає зіставляти всі додатки з цими профілями. Агентство розширює застосування статичних правил до всіх заявок і проводить періодичні ручні перевірки оцінювання профілю програми.	Компанія впроваджує динамічні мережеві правила та конфігурації для оптимізації ресурсів, які періодично адаптуються на основі автоматизованих оцінок і моніторингу профілів додатків з урахуванням і реагування на ризики.	Компанія впроваджує динамічні мережеві правила та конфігурації, які постійно розвиваються, щоб задовольнити потреби профілю додатків і змінити пріоритети додатків на основі критичності місії, ризику тощо.
Шифрування трафіку	Корпорація шифрує мінімальний трафік і покладається на ручні або спеціальні процеси для керування та захисту ключів шифрування.	Компанія починає шифрувати весь трафік до внутрішніх додатків шифрування для трафіку до зовнішніх програм, для формалізації політик керування ключами та захисту ключів шифрування сервера/служби.	Компанія забезпечує шифрування для всіх застосовних внутрішніх і зовнішніх протоколів трафіку, керує видачею та ротацією ключів і сертифікатів, а також починає впроваджувати найкращі практики для криптографічної гнучкості.	Компанія продовжує шифрувати трафік за потреби, запроваджує принципи найменших привілеїв для безпечного керування ключами в усьому підприємстві та якомога ширше використовує найкращі практики для криптографічної гнучкості.
Стійкість мережі	Компанія налаштовує мережеві можливості в кожному конкретному випадку, щоб відповідати лише вимогам доступності окремих програм із обмеженими механізмами стійкості для робочих	Агентство починає налаштовувати мережеві можливості для керування вимогами доступності для додаткових програм і розширення механізмів стійкості для робочих навантажень, які не вважаються критично важливими.	Компанія налаштувала мережеві можливості для динамічного керування вимогами доступності та механізмами стійкості для більшості своїх програм.	Компанія об’єднує цілісне надання та обізнаність у адаптації до змін у вимогах доступності для всіх робочих навантажень і забезпечує пропорційну стійкість.

	навантажень, які не вважаються критично важливими			

Таблиця 3.7 Необхідні критерії до розширеної моделі Zero Trust для мереж

Критерій	**Традиційний**	**Початковий**	**Розширений**	**Оптимальний**
Видимість і аналітика	Компанія включає обмежені можливості моніторингу мережі, орієнтовані на межі, з мінімальним аналізом, щоб розпочати розвиток централізованої обізнаності про ситуацію.	Компанія використовує можливості моніторингу мережі на основі відомих індикаторів компрометації (включно з перерахуванням мережі), щоб розвинути ситуаційну обізнаність у кожному середовищі та починає корелювати телеметрію між типами трафіку та середовищами для аналізу та пошуку загроз.	Компанія розгортає мережеві можливості виявлення аномалій для розвитку ситуаційної обізнаності в усіх середовищах, починає корелює телеметрію з багатьох джерел для аналізу та включає автоматизовані процеси для надійного пошуку загроз.	Компанія забезпечує видимість зв’язку в усіх мережах і середовищах агентства, одночасно забезпечуючи ситуаційну обізнаність у масштабах підприємства та розширені можливості моніторингу, які автоматизують кореляцію телеметрії для всіх джерел виявлення.
Можливість автоматизації та оркестровки	Компанія використовує ручні процеси для керування конфігурацією та життєвим циклом ресурсів для мереж і середовищ агентства з періодичною інтеграцією вимог політики та обізнаності про ситуацію.	Компанія починає використовувати автоматизовані методи для керування конфігурацією та життєвим циклом ресурсів для деяких мереж або середовищ компанії та гарантує, що всі ресурси мають визначений термін служби на основі політик і телеметрії.	Компанія використовує автоматизовані методи керування змінами (наприклад, CI/CD) для керування конфігурацією та життєвим циклом ресурсів для всіх мереж і середовищ корпорації, реагуючи на політику та	Корпоративні мережі та середовища визначаються за допомогою інфраструктури як коду, керованої автоматизованими методами керування змінами, включаючи автоматичне ініціювання та завершення для узгодження з мінливими потребами.

			забезпечую чи її дотримання та захист від передбачува них ризиків.	
Спромож ність до керуванн я	Компанія впроваджує статичні мережеві політики (доступ, протоколи, сегментація, сповіщення та виправлення) з підходом, зосередженим на захисті периметра.	Компанія визначає та починає впроваджувати індивідуальну політику мережевих сегментів і ресурсів, а також успадковує загальнокорпорат ивні правила, якщо це необхідно.	Компанія використову є автоматизац ію для впроваджен ня індивідуаль них політик і полегшує перехід від захисту, орієнтовано го на периметр.	Компанія впроваджує мережеві політики для всього підприємства, які забезпечують індивідуальний локальний контроль; динамічні оновлення; і безпечні зовнішні з'єднання на основі робочих процесів програми та користувача.

Програми та робочі навантаження включають системи агентств, комп'ютерні програми та служби, які виконуються локально, на мобільних пристроях і в хмарних середовищах. Компанії повинні керувати та захищати свої розгорнуті програми, а також забезпечувати безпечну доставку програм. Детальний контроль доступу та інтегрований захист від загроз можуть запропонувати покращену обізнаність про ситуацію та пом'якшити загрози, пов'язані з програмою. Відповідно до OMB M-22-09, компанії повинні почати вивчати можливості зробити свої програми доступними через загальнодоступні мережі для авторизованих користувачів. Слід також, наскільки це можливо, застосовувати найкращі практики для процесів DevSecOps і CI/CD, включаючи використання незмінних робочих навантажень.

Компанії повинні вивчити варіанти перенесення своєї діяльності з фокусу на межі акредитації та оновлення АТО на підтримку програм, ніби вони спрямовані зовні та забезпечують відповідну безпеку [31].

Таблиця 3.8 Необхідні компоненти високорівневої моделі Zero Trust для додатків

Функція	**Традиційний**	**Початковий**	**Розширений**	**Оптимальний**
Доступ до програм	Компанія використовує доступ до програм переважно за допомогою локальної авторизації та статичних атрибутів.	Компанія починає впроваджувати можливості авторизації доступу до програм, які включають контекстну інформацію (наприклад, ідентифікаційні дані, сумісність пристрою та/або інші атрибути) за запитом із закінченням терміну дії.	Компанія автоматизує рішення щодо доступу до програми за допомогою розширеної контекстної інформації та примусових умов закінчення терміну дії, які дотримуються принципів найменших привілеїв.	Компанія постійно авторизує доступ до додатків, включаючи аналітику ризиків у реальному часі та такі фактори, як поведінка або моделі використання.
Захист програм від загроз	Корпоративні засоби захисту від загроз мають мінімальну інтеграцію з робочими процесами програми, застосовуючи засоби захисту загального призначення для відомих загроз.	Компанія інтегрує засоби захисту від загроз у робочі процеси критично важливих програм, застосовуючи захист від відомих загроз і деяких загроз, пов’язаних із програмою.	Компанія інтегрує засоби захисту від загроз у всі робочі процеси програми, захищаючи від деяких специфічних для програми та цільових загроз.	Компанія інтегрує розширений захист від загроз у всі робочі процеси додатків, пропонуючи видимість у реальному часі та захист із урахуванням вмісту від складних атак, адаптованих до додатків.
Доступність програми	Компанія робить деякі критично важливі програми доступними лише через приватні мережі та захищені загальнодоступні мережеві з’єднання (наприклад, VPN) із моніторингом.	Компанія надає доступ до деяких із своїх відповідних критично важливих додатків через відкриті загальнодоступні мережі для авторизованих користувачів, які потребують цього, за допомогою посередницьких з’єднань.	Компанія за потреби надає авторизованим користувачам доступ до більшості своїх критично важливих програм через відкриті загальнодоступні мережі.	Компанія робить усі відповідні програми доступними через відкриті загальнодоступні мережі для авторизованих користувачів і пристроїв, де це доречно, за потреби.

Безпечна розробка та розгортання програм	Компанія має спеціальні середовища розробки, тестування та виробництва з ненадійними механізмами розгортання коду.	Компанія надає інфраструктуру для розробки, тестування та виробничі середовища (включаючи автоматизацію) з формальними механізмами розгортання коду через конвеєри CI/CD і необхідні засоби контролю доступу на підтримку принципів найменших привілеїв.	Компанія використовує чіткі та скоординовані команди для розробки, безпеки та операцій, при цьому позбавляючи розробника доступу до робочого середовища для розгортання коду.	Компанія використовує незмінні робочі навантаження, де це можливо, дозволяючи змінам набути чинності лише через перерозподіл, і позбавляє адміністратора доступу до середовищ розгортання на користь автоматизованих процесів для розгортання коду.
Тестування безпеки програми	Компанія проводить тестування безпеки програми перед розгортанням, переважно за допомогою методів тестування вручну.	Компанія починає використовувати статичні та динамічні (тобто програма виконується) методи тестування для тестування безпеки, включаючи ручний експертний аналіз, перед розгортанням програми.	Компанія інтегрує тестування безпеки програми в процес розробки та розгортання програми, включаючи використання методів періодичного динамічного тестування.	Компанія об’єднує тестування безпеки додатків протягом життєвого циклу розробки програмного забезпечення на підприємстві з регулярним автоматизованим тестуванням розгорнутих додатків.

Таблиця 3.9 Необхідні критерії до розширеної моделі Zero Trust для додатків

Критерій	**Традиційний**	**Початковий**	**Розширений**	**Оптимальний**
Видимість і аналітика	Компанія виконує певний моніторинг продуктивності та безпеки критично важливих програм з обмеженим узагальненням і аналітикою.	Компанія починає автоматизувати профіль програми (наприклад, стан, працездатність і продуктивність) і моніторинг безпеки для покращення збору журналів, агрегації та аналітики.	Компанія автоматизує моніторинг профілів і безпеки для більшості додатків за допомогою евристики для виявлення тенденцій, пов’язаних із застосунком і в масштабах підприємства, і з часом удосконалює	Компанія здійснює безперервний і динамічний моніторинг усіх додатків, щоб підтримувати повну видимість у масштабах підприємства.

			процеси для усунення прогалин у видимості.	
Можливість автоматизації та оркестровки	Компанія вручну встановлює розміщення статичного додатка та доступ до нього під час надання з обмеженим обслуговуванням і переглядом.	Компанія періодично змінює конфігурації програми (в т.ч розташування та доступ), щоб досягти відповідних цілей безпеки та продуктивності.	Компанія автоматизовує конфігурації додатків, щоб реагувати на зміни в роботі та середовищі.	Компанія автоматизує налаштування додатків для постійної оптимізації безпеки та продуктивності.
Спроможність до керування	Компанія в першу чергу покладається на політику ручного застосування для доступу до додатків, розробки, розгортання, керування активами програмного забезпечення, тестування та оцінки безпеки (ST&E) під час впровадження технологій, виправлення та відстеження залежностей програмного забезпечення.	Компанія починає автоматизувати дотримання політики для розробки додатків (включно з доступом до інфраструктури розробки), розгортання, управління активами програмного забезпечення, ST&E при впровадженні технологій, виправлення та відстеження залежностей програмного забезпечення на основі відповідно до потреб місії (наприклад, за допомогою програмного забезпечення).	Компанія впроваджує багаторівневу індивідуальну політику для всього підприємства для додатків і всіх аспектів життєвих циклів розробки та розгортання додатків і, де це можливо, використовує автоматизацію для підтримки виконання.	Компанія повністю автоматизує політику розробки програм і розгортання, включаючи включення динамічних оновлень для програм через конвеєр CI/CD.

Дані включають усі структуровані та неструктуровані файли та фрагменти, які зберігаються або зберігалися у системах, пристроях, мережах, програмах, базах даних, інфраструктурі та резервних копіях (включно з локальними та віртуальними середовищами), а також пов’язані метадані.

Дані компанії повинні бути захищені на пристроях, у програмах і в мережах відповідно до вимог. Підприємства повинні інвентаризувати, класифікувати та маркувати дані; захищати дані під час передачі та передачі; і розгорнути механізми для виявлення та припинення викрадання даних. Агентства повинні ретельно розробляти та переглядати політику управління даними, щоб забезпечити належне дотримання всіх аспектів безпеки життєвого циклу даних на підприємстві [32].

Таблиця 3.10 Необхідні компоненти високорівневої моделі Zero Trust для даних

Функція	**Традиційний**	**Початковий**	**Розширений**	**Оптимальний**
Управління інвентаризацією даних	Компанія вручну визначає та інвентаризує деякі дані агентства (наприклад, критично важливі дані).	Компанія починає автоматизувати процеси інвентаризації даних як для локальних, так і для хмарних середовищ, охоплюючи більшість даних агентства, і починає включати засоби захисту від втрати даних.	Компанія автоматизує інвентаризацію та відстеження даних у масштабах підприємства, охоплюючи всі відповідні дані агентства, за допомогою стратегій запобігання втраті даних на основі статичних атрибутів і/або міток.	Компанія постійно проводить інвентаризацію всіх відповідних даних агентства та використовує надійні стратегії запобігання втраті даних, які динамічно блокують підозрювану крадіжку даних.
Категоризація даних	Компанія використовує обмежені та випадкові можливості категоризації даних.	Компанія починає впроваджувати стратегію категоризації даних із визначеними мітками та механізмами ручного контролю.	Компанія автоматизує деякі процеси категоризації та маркування даних у послідовний, багаторівневий, цілеспрямований спосіб за допомогою простих, структурованих форматів і регулярного перегляду.	Компанія автоматизує категоризацію та маркування даних у масштабах підприємства за допомогою надійних методів; структуровані формати; і механізми для адресації всіх типів даних.
Доступність даних	Компанія в основному надає доступ до даних із локальних сховищ даних із деякими резервними копіями за	Компанія надає доступ до деяких даних із надлишкових високодоступних сховищ даних (наприклад, хмара) і підтримує зовнішнє резервне копіювання	Компанія насамперед надає доступ до даних із надлишкових високодоступних сховищ даних і забезпечує доступ до архівних даних.	Компанія використовує динамічні методи для оптимізації доступності даних, у тому числі архівних, відповідно до потреб

	межами сайту.	локальних даних.		користувача та організації.
Доступ до даних	Компанія керує доступом користувачів і організацій (наприклад, дозволами на читання, запис, копіювання, надання іншим доступу тощо) до даних за допомогою статичних елементів керування доступом.	Компанія починає розгортати автоматизовані засоби контролю доступу до даних, які включають елементи найменших привілеїв на підприємстві.	Компанія автоматизує засоби контролю доступу до даних, які враховують різні атрибути, такі як ідентифікація, ризик пристрою, програма, категорія даних тощо, і обмежені часом, де це можливо.	Компанія автоматизує динамічний своєчасний і достатній контроль доступу до даних у масштабах підприємства з постійним переглядом дозволів.
Шифрування даних	Компанія шифрує мінімальну кількість даних агентства під час спокою та передачі та покладається на ручні або спеціальні процеси для керування та захисту ключів шифрування.	Компанія шифрує всі дані, що передаються, і, де це можливо, дані, що знаходяться в стані спокою (наприклад, критично важливі дані та дані, що зберігаються у зовнішньому середовищі), і починає формувати політику керування ключами та безпечні ключі шифрування.	Компанія максимально шифрує всі дані, що перебувають у стані спокою та передаються через підприємство, починає включати криптографічну гнучкість і захищає ключі шифрування (тобто секрети не закодовані жорстко й регулярно змінюються).	Компанія шифрує дані, які використовуютьс я, де це доцільно, дотримується принципів найменших привілеїв для безпечного керування ключами в усьому підприємстві та застосовує шифрування з використанням найсучасніших стандартів і криптографічної гнучкості, наскільки це можливо.

Таблиця 3.11 Необхідні критерії до розширеної моделі Zero Trust для даних

Критерій	**Традиційний**	**Початковий**	**Розширений**	**Оптимальний**
Видимість і аналітика	Компанія має обмежений доступ до даних, зокрема про місцезнаходж	Компанія отримує видимість на основі управління інвентаризацією даних, категоризації,	Компанія підтримує видимість даних у більш комплексний спосіб для всього підприємства за допомогою	Компанія має видимість упродовж усього життєвого циклу даних завдяки надійній

	ення, доступ і використання, а аналіз полягає в основному в ручних процесах.	шифрування та спроб доступу з деяким автоматизованим аналізом і кореляцією.	автоматизованого аналізу та кореляції та починає використовувати прогнозну аналітику.	аналітиці, включаючи прогнозну аналітику, яка підтримує повний перегляд даних агентства та постійну оцінку стану безпеки.
Можливість автоматизації та оркестровки	Компанія реалізує життєвий цикл даних і політики безпеки (наприклад, доступ, використання, зберігання, шифрування, конфігурації, захист, резервне копіювання, категоризація, санітарна обробка) за допомогою ручних і, можливо, спеціальних процесів.	Компанія використовує деякі автоматизовані процеси для впровадження життєвого циклу даних і політики безпеки.	Компанія реалізує життєвий цикл даних і політику безпеки в основному за допомогою автоматизованих методів для більшості даних агентства в послідовний, багаторівневий, цільовий спосіб у всьому підприємстві.	Компанія максимально автоматизує життєві цикли даних і політики безпеки для всіх даних агентства на підприємстві.
Спроможність до керування	Компанія покладається на спеціальні політики керування даними (наприклад, для захисту, категоризації, доступу, інвентаризації, зберігання, відновлення, видалення тощо) із застосуванням вручну.	Компанія визначає політику управління даними високого рівня та покладається переважно на сегментоване впровадження вручну	Компанія починає інтеграцію забезпечення виконання політики життєвого циклу даних у масштабах підприємства, забезпечуючи більш уніфіковані визначення для політик керування даними.	Політики життєвого циклу даних компанії максимально уніфіковані та динамічно застосовуються на підприємстві.

Висновки до розділу 3

Підсумовуючи, що високорівнева модель нульової довіри є ключовим прогресом у сфері кібербезпеки, пропонуючи організаціям дорожню карту до комплексної стійкості та адаптивності в умовах дедалі складнішого середовища загроз. Прийнявши його принципи та методології, організації можуть впевнено орієнтуватися в кібербезпеці, що розвивається, захищаючи критично важливі активи та зберігаючи довіру у взаємопов’язаному світі.

Значущість моделі полягає не лише в її концептуальній основі, а й у практичній застосовності. Забезпечуючи структурований підхід до впровадження, він дає змогу організаціям поступово зміцнювати свої засоби захисту, використовуючи існуючу інфраструктуру та одночасно стратегічно інтегруючи нові технології та методології.

РОЗДІЛ 4
ПРАКТИЧНА РЕАЛІЗАЦІЯ МОДЕЛІ ZERO TRUST

4.1 Аналіз рішень Zero Trust

Рішення безпеки Zero Trust, включають низку різних технологій і процесів, які автентифікують доступ користувачів, сегментують і керують доступом до даних, а також постійно відстежують мережу на наявність шкідливих мережевих дій; три найважливіші функції будь-якої моделі безпеки Zero Trust. Враховуючи ключові функції, включаючи методи автентифікації, політики, моніторинг і звіти є рішення які здатні це забезпечити:

Twingate — це рішення Zero Trust Network Access (ZTNA), яке забезпечує хмарний віддалений доступ, альтернативу традиційним рішенням VPN. Їхнє рішення дозволяє IT-командам легко контролювати мережевий периметр і централізовано керувати доступом користувачів до будь-яких внутрішніх програм, як локальних, так і хмарних. Рішення ZTNA від Twingate забезпечує кілька переваг порівняно з традиційними рішеннями VPN, дозволяючи організаціям використовувати підхід Zero Trust до віддаленого доступу. Платформа покращує адміністративний контроль і безпеку, дозволяючи адміністраторам надавати доступ до програм для кожного користувача, гарантуючи, що користувачі можуть отримувати доступ лише до програм, необхідних для ефективного виконання своєї роботи (принцип найменших привілеїв), і допомагаючи обмежити обсяг даних порушення у разі атаки компрометації облікового запису [33].

Адміністратори можуть призначати ролі користувачам, які керують доступом до програм на основі кількох джерел даних. До них належать місцезнаходження користувача, час доби, контекстна інформація, наприклад оцінка ризику співробітника на основі минулої поведінки, а також інтеграція зі сторонніми інструментами керування ідентифікацією, включаючи рішення SSO

або MFA. Twingate надає просту в управлінні консоль адміністратора, яка забезпечує централізований контроль і видимість усього мережевого середовища. З консолі адміністратори можуть отримати доступ до детальних журналів і звітів, а також інтегрувати платформу з іншими інструментами звітності або рішеннями SIEM.

Платформа зменшує затримку, пов’язану з традиційними рішеннями VPN, і працює добре, зменшуючи використання корпоративної смуги пропускання та покращуючи досвід роботи для кінцевих користувачів, які підключаються до застарілих VPN. Рішення можна встановити на пристроях MacOS, Windows, Linux, iOS, Android і Chrome. Конфігурація проста з чіткою документацією для першого налаштування на веб-сайті Twingate [34].

NordLayer — це рішення Zero Trust Network Access — альтернатива застарілій VPN, — яке дозволяє користувачам легко підключатися до корпоративної мережі, а потім захищає кожне з’єднання за допомогою автентифікації користувача, сегментації мережі та шифрування трафіку. NordLayer, що надається як послуга, дозволяє IT-адміністраторам централізовано та віддалено керувати та захищати доступ користувачів до будь-яких областей їхнього хмарного або багатохмарного середовища. NordLayer дозволяє адміністраторам сегментувати доступ користувачів до своєї мережі. Відповідно до принципів нульової довіри та найменших привілеїв, це означає, що користувачі можуть отримувати доступ лише до певних програм і даних, необхідних для виконання своєї роботи, на основі дозволів, налаштованих адміністратором. Цей підхід означає, що якщо зловмисник зламатиме мережу, він зможе отримати доступ лише до невеликої її частини, а не до всієї мережі, як це було б із застарілою VPN. Платформа автентифікує користувачів за допомогою інтеграції зі сторонніми постачальниками MFA та SSO, включаючи Azure AD, Google Workspace, Okta та OneLogin. Після автентифікації користувачі можуть розпочати віддалене з’єднання одним клацанням миші. Вони також можуть увімкнути автоматичне підключення для постійного, негайного підключення до мережі через власний протокол NordLynx NordLayer.

NordLayer захищає всі з’єднання за допомогою 256-бітного шифрування AES, а також пропонує функцію Kill Switch, яка автоматично відключає весь трафік до пристрою, якщо його з’єднання з сервером взагалі розривається, допомагаючи пом’якшити атаки Man-in-the-Middle. З центральної консолі керування адміністратори можуть керувати обліковими записами користувачів і шлюзами; налаштовувати дозволи та політики безпеки для користувачів, пристроїв і програм; і отримати підтримку від свого менеджера облікового запису. NordLayer пропонує комплексні функції безпеки мережі як частину свого рішення безпеки Zero Trust. Це включає комплексний хмарний брандмауер, який поєднує в собі перевірку мережевого трафіку з перевіркою пакетів, запобігання вторгненням і розвідку про загрози. Іншою ключовою функцією є модуль безпеки положення пристрою, який відстежує всі пристрої, підключені до вашої мережі, дозволяючи адміністраторам налаштовувати політики та сповіщення, щоб запобігти доступу невідповідних пристроїв. NordLayer надається як послуга. Він має високу масштабованість і легко інтегрується з іншими інструментами безпеки сторонніх виробників. Платформа швидко розгортається, забезпечуючи захист протягом кількох годин після покупки, а Nord Security також пропонує спеціального менеджера облікових записів і високоефективні варіанти підтримки клієнтів для допомоги під час розгортання та після нього.

JumpCloud — це комплексна платформа Open Directory Platform, яка допомагає організаціям централізовано керувати ідентифікацією, доступом і пристроями для створення середовища нульової довіри. Платформа відкритих каталогів JumpCloud дозволяє адміністраторам і командам безпеки безпечно надавати ідентифікаційні дані та керувати ними; легко налаштовувати політики, щоб дозволити користувачам доступ лише до тих пристроїв, програм і мереж, які необхідні для їх роботи; а також забезпечити комплексні можливості моніторингу та журналювання, щоб забезпечити широку видимість організації для всіх її користувачів та IT-ресурсів.

JumpCloud дозволяє організаціям побудувати міцну основу Zero Trust у всіх аспектах життєвого циклу співробітників. Це включає в себе надання нових

ідентифікацій, їх скасування, коли працівник змінює роль або залишає організацію, налаштування політик умовного доступу на основі бізнес-потреб, надання привілейованого доступу до облікових записів для певних груп, доступ до програми єдиного входу, своєчасний доступ забезпечення доступу тощо [35].

Щоб переконатися, що доступ надається за принципом найменших привілеїв, адміністратори можуть установити детальні політики, щоб визначити, які користувачі мають які рівні доступу та за яких умов. Наприклад, адміністратори можуть запровадити контроль доступу на основі груп, щоб гарантувати, що користувачі мають доступ лише до тих ресурсів, які їм потрібні для виконання їхніх ролей. Адміністратори також можуть запроваджувати правила, які вказують, що користувачам потрібно входити за допомогою багатофакторної автентифікації або що користувачі можуть входити лише на надійних пристроях або в мережах. Платформа JumpCloud Open Directory забезпечує повну видимість їхніх користувачів, пристроїв та IT-ресурсів і має вбудовані потужні функції моніторингу та журналювання подій, щоб надати адміністраторам детальний перегляд усього свого IT-середовища [36]. Це включає в себе можливість переглядати запити на автентифікацію, які користувачі отримують доступ до яких служб і коли, дії, які вони виконують, зміни ідентифікаційних даних тощо. Це не лише допомагає адміністраторам виявляти підозрілу поведінку та потенційні вразливості, а й допомагає організаціям дотримуватися правил аудиту та відповідності.

Prove є провідним на ринку постачальником рішень для автентифікації користувачів і перевірки особи, які дозволяють організаціям забезпечити доступ користувачів до програм і послуг із нульовою довірою. Pinnacle — це платформа ідентифікації Prove, яка використовує методи машинного навчання та механізми криптографічної автентифікації для забезпечення точної автентифікації споживача, яка зберігає конфіденційність [37].

Prove Pinnacle використовує криптографічну модель автентифікації для забезпечення легкої та високоточної автентифікації кінцевого користувача. Підхід платформи «Phone-Centric Identity» перевіряє осіб на основі даних,

отриманих із мобільного телефону особи. Коли користувач вперше «прив'язує» до себе криптографічний ключ (тобто SIM-карту або ключ FIDO на смартфоні), йому видається ProveID. Потім Pinnacle використовує 128-бітове шифрування, пов'язане з телефоном, щоб перевірити користувача на основі його фізичного володіння телефоном у реальному часі в поєднанні з профілем репутації на основі поведінки, пов'язаним з його ProveID. Це дає змогу Pinnacle точно й швидко оцінювати ризик користувача, що значно покращує безпеку, не ускладнюючи команди безпеки. Платформа Pinnacle містить чотири ключові рішення, які зосереджені на підході перевірки особи Prove, орієнтованому на телефон. Prove Pre-Fill автоматично попередньо заповнює форми заявок підтвердженою ідентифікаційною інформацією, зменшуючи тертя під час реєстрації споживача та підвищуючи безпеку. Prove Identity перевіряє особистість користувачів на основі мільярдів сигналів у реальному часі з їхніх телефонів, а Prove Auth забезпечує автентифікацію без пароля за допомогою біометричних даних або push-повідомлень. Обидва ці рішення допомагають зменшити тертя та шахрайство. Нарешті, Prove Identity Manager надає організаціям реєстр маркерів ідентифікації телефону в реальному часі, що полегшує їм керування атрибутами ідентифікації споживачів протягом усього життєвого циклу [36].

GoodAccess пропонує хмарне рішення Zero Trust Network Access, створене для забезпечення безпечного доступу до бізнес-ресурсів незалежно від місця розташування. Ця платформа забезпечує набір функцій безпеки, включаючи правила доступу на основі ідентичності, шифрування трафіку, багатофакторну автентифікацію, єдиний вхід (SSO) і сегментацію мережі [38].

Завдяки зручному веб-інтерфейсу підприємства можуть налаштувати свою віртуальну інфраструктуру, досягнувши високошвидкісного з'єднання в багатьох місцях. Розраховане на малий і середній бізнес, це 100% хмарне рішення спрямоване на оптимізацію операцій безпеки мережі, дозволяючи швидке налаштування без спеціальних навичок. Функції платформи включають ряд заходів безпеки. Хмарні з'єднувачі та роз'єми гілок допомагають інтегрувати різні точки даних в інфраструктуру GoodAccess, дозволяючи користувачам

вибирати між протоколами IPsec, IKEv2 або OpenVPN відповідно до своїх потреб. Єдиний вхід полегшується завдяки інтеграції з такими платформами, як Microsoft Azure, Google Workspace та іншими службами, сумісними з SAML. Функція Threat Blocker спрямована на захист користувачів від доступу до зловмисних веб-сайтів, тоді як фільтрація DNS пропонує контроль над доступом до сайтів і програм. Платформа також наголошує на відповідності, з журналюванням активності користувачів і багатофакторною автентифікацією як для адміністраторів, так і для користувачів. Нарешті, централізоване керування доступом здійснюється за допомогою віртуальних карт доступу, які призначають дозволи на основі певних критеріїв, гарантуючи, що кожен користувач може отримати доступ лише до тих ресурсів, до яких йому дозволено [39].

Duo Beyond — це рішення безпеки Zero Trust, яке забезпечує детальну перевірку користувачів, автентифікацію, єдиний вхід і багатофакторну автентифікацію, розроблене з урахуванням принципів Zero Trust. Duo Beyond дозволяє безпечно автентифікувати доступ до будь-якого користувача з будь-яким пристроєм, щоб забезпечити захист даних. Duo Beyond поєднує багатофакторну автентифікацію користувача з перевіркою пристрою та безпечним єдиним входом для захисту всіх довірених активів вашої організації. Duo Beyond містить усі функції, які пропонують Duo Access і продукт MFA, із системою єдиного входу, політиками та елементами керування, статистикою пристрою та синхронізацією каталогів. Duo був придбаний компанією Cisco у 2018 році і зараз є одним із основних стовпів їхнього пакету безпеки Zero Trust, повністю інтегрованого в портфоліо рішень Cisco Zero Trust.

Duo Beyond пропонує дві основні функції: надійні кінцеві точки та мережевий шлюз Duo. За допомогою довірених кінцевих точок ви можете визначати та керувати пристроями, які підключаються до облікових записів вашої компанії, і надавати безпечний доступ за допомогою політик перевірки сертифікатів пристроїв. Довірені керовані пристрої можна класифікувати як безпечні за допомогою сертифіката Duo, а потім отримати доступ до конфіденційних облікових записів. Некерованим кінцевим точкам без

сертифіката можна заблокувати доступ до програм відповідно до політик адміністратора. Їх можна налаштувати на рівні групи або користувача [40].

Мережевий шлюз Duo дозволяє користувачам безпечно отримувати доступ до внутрішніх веб-додатків за допомогою будь-якого пристрою чи браузера з будь-якої мережі в світі без використання програмного забезпечення віддаленого доступу або VPN. Duo використовує MFA для автентифікації доступу користувачів і забезпечує детальний контроль доступу до програми, SSH-серверів і груп користувачів, щоб ви могли точно налаштувати процеси безпеки для кожної програми [41].

Поряд із довіреними кінцевими точками та мережевим шлюзом Duo забезпечує моніторинг довіри, єдиний вхід, синхронізацію каталогів тощо. Нещодавно Cisco оголосила, що можливості автентифікації Duo без пароля будуть додані до її платформи Zero Trust.

Google BeyondCorp — це власна реалізація системи безпеки Zero Trust від Google, яка дає змогу перемістити елементи керування доступом із периметра вашої мережі до окремих користувачів. BeyondCorp дозволяє користувачам безпечно підключатися до корпоративних програм практично з будь-якого місця в будь-який час без використання VPN. BeyondCorp є результатом десятиліття процесів безпеки, створених у Google, і спочатку був розроблений як внутрішня ініціатива, щоб дозволити співробітникам Google отримати доступ до внутрішніх програм. Відтоді BeyondCorp розроблявся як корпоративне рішення Zero Trust, що постачається через глобальну мережу Google і забезпечує безпечний доступ до програм і хмарних ресурсів.

BeyondCorp надає низку функцій для безпечного доступу до корпоративних додатків із вбудованим захистом даних і загроз. Адміністратори можуть налаштовувати політики доступу на основі оцінки ризиків на основі ідентифікації користувача, стану пристрою та інших контекстних факторів, щоб гарантувати, що лише авторизовані користувачі можуть отримати доступ до корпоративних програм, віртуальних машин і API Google. Google також забезпечує захист від втрати даних із захистом від зловмисного програмного забезпечення та фішингу,

вбудованим у веб-переглядач Chrome, і автоматичними сповіщеннями для IT-адміністраторів. BeyondCorp пропонує ряд інтеграцій від провідних постачальників кібербезпеки для кращого контролю та видимості вашої мережі. Рішення Google мають високу масштабованість, а BeyondCorp також забезпечує інтегрований захист від DDoS-атак [42].

BeyondCorp enterprise повністю працює через хмару та не потребує жодних агентів для розгортання. BeyondCorp використовує глобальну мережеву інфраструктуру Google для підтримки з'єднань із низькою затримкою та еластичного масштабування. BeyondCorp дозволяє користувачам підключатися до будь-яких програм SaaS, веб-додатків і хмарних ресурсів з будь-якої точки світу. BeyondCorp надається як послуга передплати з оплатою за кожного користувача за місяць [43].

Корпорація Майкрософт, розробник провідних у світі платформ електронної пошти Exchange і Office 365, пропонує стек безпеки Zero Trust через Azure, своє хмарне рішення для ідентифікації та керування доступом. Microsoft Azure Active Directory дає змогу керувати всіма вашими користувачами Office 365, синхронізуючи облікові записи користувачів і паролі в корпоративних програмах і вмикаючи багатофакторну автентифікацію та єдиний вхід для користувачів. Це означає, що ви можете отримати більший контроль і видимість над своїми користувачами та їхнім рівнем доступу, гарантуючи, що користувачі можуть легко отримати доступ до всіх облікових записів і служб, які їм потрібні, через Microsoft і за її межами. Azure також має масштабований VPN-шлюз як альтернативу використанню сторонніх VPN, а також низку інших програм, які допомагають виконувати Zero Trust [44].

Використовуючи Azure, ви можете перевірити та захистити кожного користувача за допомогою суворих стандартів автентифікації у своїх програмах Microsoft. Корпорація Майкрософт безкоштовно надає простий у використанні додаток для смартфона, який дозволяє користувачам легко сканувати відбитки пальців або генерувати одноразовий пароль. Корпорація Майкрософт також надає

ряд звітів про доступ користувачів, покращуючи видимість того, хто отримує доступ до програм [45].

Використовуючи Azure, адміністратори мають більший контроль над дозволами в програмі для різних груп користувачів і можуть контролювати дозволи користувачів і за потреби обмежувати доступ до конфіденційних даних. Корпорація Майкрософт також використовує моніторинг у реальному часі для виявлення потенційно зловмисної поведінки користувачів, щоб запобігти витоку даних. Статус Microsoft як провідного постачальника на ринку означає, що Azure широко підтримується програмами сторонніх розробників, що дозволяє використовувати єдиний вхід для користувачів.

Azure AD входить до складу всіх платних підписок на Microsoft 365. Службою Azure Active Directory можна керувати з консолі адміністратора Microsoft 365. Тут ви можете створювати групи користувачів і керувати ними. Ціноутворення для Microsoft 365 залежить від розміру організації та необхідного рівня функціональності [46].

OKTA є провідним на ринку постачальником ідентифікаційних даних і керування доступом, який пропонує ряд різних продуктів і рішень, спрямованих на допомогу організаціям в управлінні доступом до систем і досягненні безпеки без довіри. OKTA обслуговує дві різні аудиторії: організації, які шукають рішення для автентифікації доступу для своїх співробітників за допомогою OKTA Workforce Identity, і розробників, яким потрібно реалізувати безпечний доступ для входу для своїх програм за допомогою OKTA Customer Identity. OKTA забезпечує безпеку Zero Trust для програм, серверів і API, а також забезпечує безпечний доступ як для хмарних, так і для локальних програм. OKTA також відома своєю інтеграційною мережею OKTA, яка забезпечує понад 7000 інтеграцій для керування ідентифікацією в різних програмах.

OKTA надає низку різних продуктів і наборів функцій, щоб допомогти організаціям досягти нульової довіри. OKTA Workforce Identity дозволяє організаціям підтримувати віддалених працівників і захищати доступ за допомогою системи єдиного входу, універсального каталогу користувачів,

засобів керування доступом до сервера, адаптивної багатофакторної автентифікації, детального керування наданням і керування API. OKTA Customer Identity дозволяє розробникам впроваджувати MFA, безпечну автентифікацію, керування користувачами тощо, усіма якими можна керувати за допомогою однієї масштабованої платформи. OKTA також надає різноманітні сервіси платформи для підтримки Zero Trust, включаючи низку інтеграцій, звітів і аналітичних даних, настроювані робочі процеси ідентифікації та керування пристроями.

OKTA можна розгорнути в хмарних або локальних програмах. Етапи розгортання відрізняються для різних рішень і програм; OKTA пропонує вичерпні посібники у своїй базі знань. OKTA допомагає керувати спрощеним розгортанням за допомогою майстра інтеграції в рамках мережі інтеграції OKTA[47]. OKTA надає 7000 готових інтеграцій із хмарними та локальними системами, що дозволяє легко надавати SSO та MFA для сторонніх облікових записів і програм. Це дозволяє централізувати керування користувачами та автоматизувати доступ до робочих процесів і політик [48].

Ping Identity — це постачальник ідентифікаційних даних і керування доступом, який пропонує рішення, що забезпечують максимальну безпеку доступу до облікових записів і програм у вашій організації. PingOne for Workforce, який використовується 60% компаній зі списку Fortune 100, — це хмарне рішення ідентифікації, яке забезпечує надійну адаптивну автентифікацію користувачів із вбудованим єдиним входом і уніфікованим порталом адміністратора для створення безперебійного безпечного процесу входу як для співробітників, так і для адміністраторів.

PingOne пропонує адаптивну автентифікацію для користувачів і пристроїв у широкому діапазоні SaaS, локальних і хмарних додатків. Платформа надає можливість виявляти поведінку з високим ступенем ризику, наприклад неавторизований вхід або зловмисні атаки. Якщо така поведінка виявлена, PingOne може вимагати від користувача повторної автентифікації або відхилити його спробу входу відповідно до попередньо визначених політик. Якщо аномальної поведінки не виявлено, користувачеві надається доступ без . Це дає

адміністраторам більше впевненості в тому, що користувачі є легітимними, не додаючи непотрібного тертя до входу всіх користувачів. Платформа PingOne також забезпечує вбудовану систему єдиного входу для всіх програм, постачальників послуг і постачальників ідентифікаційної інформації, що означає, що користувачі можуть входити в кожен із цих облікових записів лише з одним набором облікових даних, незалежно від того, чи облікові записи налаштовано. SSO PingOne також працює в мобільних додатках, забезпечуючи плавний вхід незалежно від того, з якого пристрою підключається користувач. За допомогою універсальної консолі керування, створеної з урахуванням простоти, адміністратори можуть генерувати корисну інформацію про стан автентифікації у своєму бізнесі та налаштовувати детальні адаптивні політики автентифікації відповідно до своїх принципів нульової довіри. Вони також можуть автоматизувати та делегувати певні адміністративні завдання, що спрощує контроль над запитами служби підтримки. Окрім можливостей MFA та SSO, PingOne пропонує низку технологічних інтеграцій з іншими сторонніми постачальниками, включаючи постачальників пристроїв і мережевої безпеки, щоб допомогти вам створити повну архітектуру нульової довіри. PingOne — це хмарна платформа, яка надається як послуга, і тому її відносно легко розгорнути. Рішення пропонує інтеграцію Active Directory, яка полегшує початкову адаптацію користувачів, але також дозволяє автоматично видаляти користувачів із платформи Ping, якщо вони залишають компанію. PingOne також пропонує інтеграцію з широким спектром SaaS, застарілих, локальних і спеціальних додатків, щоб організації могли легко створити безперебійний, універсальний досвід входу в усі свої робочі програми [49].

Платформа SentinelOne допомагає оптимізувати та реалізувати багато рекомендацій розширеної моделі Zero Trust, розширюючи можливості видимості, аналітики та реагування на кінцевих точках, ідентифікаційних даних, хмарних і мережевих поверхнях.

SentinelOne надає комплексні можливості захисту ідентифікаційної інформації , включаючи зниження ризику ідентифікаційної інформації, виявлення

загроз і реагування на них, а також обман ідентифікаційних даних. Йдучи на крок далі, ніж традиційний IAM, рішення для захисту ідентифікаційної інформації SentinelOne проактивно зменшує поверхню атаки на інфраструктуру ідентифікаційної інформації, закриваючи прогалини в середовищах Active Directory і Azure AD, які зазвичай експлуатуються, і перешкоджаючи прогресу атаки через тактику неправильного спрямування.

Можливості EDR SentinelOne забезпечують видимість активності кінцевої точки в реальному часі, дозволяючи організаціям швидко виявляти загрози та реагувати на них. Оскільки кінцеві точки залишаються ключовим вектором атаки для суб'єктів загрози, SentinelOne поєднує статичні та поведінкові виявлення для нейтралізації відомих і невідомих загроз.

Відсутність видимості через застарілі засоби керування мережею породжує прогалини та невідповідності, якими можуть скористатися зловмисники. Платформа SentinelOne надає підприємствам повну видимість і контроль своєї мережі, дозволяючи командам безпеки відстежувати та ізолювати скомпрометовані пристрої та зупиняти бічний рух. Агенти SentinelOne також створюють детальну топологію мережі для підтримки судових розслідувань, процесів прийняття рішень і створення політики мікросегментації.

Хмарні обчислення та гібридні робочі простори зараз є звичним явищем для світового бізнесу. Оскільки кількість і складність хмарних атак зростає, SentinelOne бореться із загрозами на цій поверхні атаки, забезпечуючи контроль доступу на рівні додатків і використовуючи методи безпечного кодування для запобігання вразливостям. Компанії можуть керувати та захищати гібридні, приватні та багатохмарні робочі навантаження з єдиної консолі за допомогою одного агента.

У минулому підприємства зберігали конфіденційні дані у своїх корпоративних мережах. Оскільки все більше переходять на хмарні програми, просто захистити периметр від зовнішніх загроз недостатньо. Платформа SentinelOne забезпечує шифрування та контроль доступу для запобігання несанкціонованому доступу до конфіденційних даних ізсередини [50].

Але Sentinel One не зможе забезпечити наступні політики:

Сегментація та мікросегментація мережі. Хоча SentinelOne захищає кінцеві точки від зловмисних дій, вона безпосередньо не надає можливості сегментації мережі чи мікросегментації [51].

Zero Trust Network Access: SentinelOne фокусується на безпеці кінцевої точки, а не на контролі доступу до мережі. Рішення ZTNA забезпечують безпечний доступ до програм і ресурсів на основі ідентичності користувача, положення пристрою та інших контекстних факторів, незалежно від місця розташування користувача чи периметра мережі.

Контроль доступу до рівня додатків: Хоча SentinelOne захищає кінцеві точки від шкідливих програм і файлів, він не надає детального контролю доступу до рівня додатків для мережевого трафіку [52]. Розширені політики нульової довіри можуть включати засоби контролю доступу на рівні програми для обмеження доступу до певних програм або служб на основі ролей користувачів, бізнес-потреб або політик безпеки.

Контроль доступу на основі ідентифікаційних даних: хоча SentinelOne інтегрується з постачальниками ідентифікаційних даних для автентифікації користувачів і керування доступом, він може не надавати розширені засоби контролю доступу на основі ідентифікаційних даних, окрім основних механізмів автентифікації. Розширені політики нульової довіри можуть передбачати динамічний контроль доступу на основі ідентичності користувача, атрибутів пристрою та аналітики поведінки. Для досягнення цих можливостей організаціям може знадобитися інтегрувати SentinelOne з рішеннями керування ідентифікацією та доступом (IAM) або іншими механізмами контролю доступу [53].

4.2 Комплексне впровадження розширеної моделі Zero Trust за допомогою кількох рішень

Для розширеної моделі організаціям може знадобитися поєднання постачальників, які спеціалізуються на різних аспектах кібербезпеки, мережевої інфраструктури, керування ідентифікацією та хмарної безпеки.

Ось деякі постачальники, які надають рішення та послуги для підтримки розширених політик:

- Рішення ZTNA забезпечують контроль доступу на основі ідентичності користувача, стану пристрою та інших контекстних факторів, забезпечуючи безпечний доступ до програм і ресурсів.

Постачальники: Akamai Enterprise Application Access, Zscaler Private Access, Cisco Zero Trust Access (раніше Duo Beyond), AppGate SDP.

- Рішення IAM автентифікують і авторизують користувачів і пристрої перед наданням доступу до ресурсів, включаючи принципи найменших привілеїв і постійної автентифікації.

Постачальники: Okta, Microsoft Azure Active Directory, Ping Identity, OneLogin.

- Endpoint security solutions protect devices from malware, ransomware, and other threats, often incorporating features like endpoint detection and response (EDR) and device encryption.

Постачальники: CrowdStrike Falcon, Carbon Black (Vmware), Microsoft Defender for Endpoint, Symantec Endpoint Protection.

- Рішення для безпеки мережі включають брандмауери наступного покоління (NGFW), системи виявлення/запобігання вторгненням (IDPS) і методи сегментації мережі для зменшення ризиків і контролю трафіку.

Постачальники: Palo Alto Networks (NGFWs), Cisco (Firepower NGFW), Fortinet (FortiGate), Check Point (мережевий екран наступного покоління).

- Хмарні рішення безпеки захищають дані та програми, розміщені в хмарних середовищах, забезпечуючи відповідність вимогам, захист даних і виявлення/реагування на загрози.

Постачальники: AWS Security Hub, Microsoft Azure Security Center, Google Cloud Security Command Center, Netskope.

- Рішення для захисту даних включають шифрування, запобігання втраті даних (DLP) і механізми класифікації даних для захисту конфіденційної інформації.

Постачальники: Symantec Data Loss Prevention, Microsoft BitLocker, McAfee Total Protection, VeraCrypt.

- Платформи SOAR автоматизують робочі процеси реагування на інциденти, включаючи виявлення, аналіз і усунення загроз, щоб покращити операції безпеки.

Постачальники: Palo Alto Networks Cortex XSOAR, Splunk Phantom, IBM Resilient, Demisto (придбано Palo Alto Networks).

- Рішення UBA аналізують поведінку користувачів, щоб виявляти аномалії та потенційні загрози безпеці, допомагаючи організаціям виявляти внутрішні загрози та реагувати на них.

Постачальники: Exabeam, Splunk UBA, Rapid7 InsightIDR, Securonix.

- Рішення для керування вразливістю оцінюють і визначають пріоритетність вразливостей безпеки в IT-активах, забезпечуючи проактивне зниження ризиків і керування виправленнями.

Постачальники: Qualys, Tenable.io, Rapid7 InsightVM, Nessus Professional.

- DevSecOps інтегрує методи безпеки в життєвий цикл розробки програмного забезпечення (SDLC), включаючи автоматизоване тестування безпеки, аналіз коду та сканування вразливостей.

Постачальники: GitLab Secure, GitHub Advanced Security, Snyk, Aqua Security.

Як ми бачимо з постачальників немає єдиного постачальника за допомогою якого можна забезпечити впровадження розширених політик Zero Trust. Мінімальна кількість постачальників яка потрібна для забезпечення розширеної моделі Zero Trust сягає восьми. Але такий спосіб впровадження не є релевантним через вартість та складність впровадження. Тому у вендору потрібно

покращувати рішення Zero Trust таким чином, щоб покрити розширені політики розширеної моделі Zero Trust.

Якщо говорити за рішення Sentinel One, слід удосконалити рішення безпеки розширеної моделі Zero Trust включаючи постійну оцінку, уточнення та оптимізацію існуючих заходів безпеки для покращення захисту від нових загроз і ризиків. Першим кроком для покращення це використання новітніх технології та інноваційні рішення безпеки, які доповнюють принципи ZTMM, такі як штучний інтелект (AI), машинне навчання (ML), аналітика поведінки та платформи аналізу загроз. Інтегрувати інструменти автоматизації та оркестровки для оптимізації операцій безпеки, покращення часу реагування на інциденти та зменшення кількості помилок, що виникають вручну. Розширити впровадження ZTNA, щоб охопити ширший діапазон програм, послуг і груп користувачів, включаючи сторонніх постачальників, партнерів і віддалених працівників. Використовувати технології програмно-визначеного периметра (SDP) і платформи безпечного доступу (SASE), щоб забезпечити плавний і безпечний доступ до ресурсів незалежно від місцезнаходження користувача чи периметра мережі. Інтегрувати канали аналізу загроз і платформи аналізу загроз (TIP) у рішення розширеної моделі Zero Trust, щоб розширити аналітику безпеки, покращити можливості виявлення загроз і визначити пріоритетність дій у відповідь на основі серйозності та актуальності загроз. Покращити механізми автентифікації користувачів, реалізувавши багатофакторну автентифікацію, адаптивну автентифікацію та методи постійної автентифікації на основі поведінки користувача та контексту. Застосувати елементи керування доступом із найменшими привілеями, щоб обмежити доступ користувачів і пристроїв лише до ресурсів і даних, необхідних для виконання їхніх ролей і обов’язків. Інтегрувати безпеку в життєвий цикл розробки програмного забезпечення (SDLC), запровадивши методи DevSecOps, включивши засоби контролю безпеки та тестування на кожному етапі процесу розробки.

Висновки до розділу 4

Практична реалізація розширеної моделі Zero Trust дозволяє підвищити рівень безпеки та захищеності інформаційних ресурсів та інфраструктури підприємства. Цей підхід ґрунтується на принципі відсутності довіри до будь-яких користувачів, пристроїв або мереж, що надає більш глибокий та гнучкий підхід до забезпечення безпеки порівняно з традиційними периметровими моделями захисту.

У рамках дослідження було проаналізовано та визначено основні складові реалізації розширеної моделі Zero Trust, включаючи ідентифікацію та автентифікацію користувачів, мікро- та макросегментацію мережі, застосування заходів захисту на рівні кінцевих точок, розвиток політик управління доступом, та імплементацію засобів моніторингу та аналізу безпекових подій.

Завершеною реалізацією розширеної моделі Zero Trust можна забезпечити лише високий рівень безпеки, але й покращити реакцію на інциденти, оптимізувати витрати на забезпечення безпеки та забезпечити відповідність різноманітним нормативно-правовим вимогам.

Рішення які були проаналізовані, а саме Twingate, NordLayer, GoodAccess можна використовувати для безпечного доступу до корпоративних ресурсів з будь-якого місця, а JumpCloud Open Directory Platform, OKTA Identity Cloud, Ping Identity PingOne допоможуть у керуванні ідентичністю і контролі доступу, Prove Pinnacle, Duo Beyond забезпечують багаторівневу аутентифікацію та безпечний доступ.

ВИСНОВКИ

В результаті виконання дипломної роботи було створено високорівневу модель Zero Trust. Було проаналізовано концепцію "нульової довіри" та порівнюючи її з традиційним захистом периметру, було виявлено, що нульова довіра надає більш глибокий та гнучкий підхід до кібербезпеки, уникаючи довіри до будь-якого внутрішнього або зовнішнього джерела.

В другому розділі дипломної роботи був зроблений огляд архітектури "нульової довіри" який дозволив виявити нерелевантні аспекти та визначити найкращі практики для успішного розгортання цього підходу. Однак, було визначено й потенційні проблеми на шляху впровадження, такі як складність розгортання та відсутність єдиної стандартної моделі.

Третій розділ дипломної роботи був присвячений створенні та опису концепції високорівневої моделі Zero Trust. Були створені політики всіх рівнів високорівневої моделі Zero Trust для облікових записів, пристроїв, мережі, додатків та даних.

У четвертому розділі дипломної роботи були проаналізовані рішення для комплексного впровадження політик високорівневої моделі Zero Trust це показує те, що високорівневу модель Zero Trust технічно можливо реалізувати за умови детального планування та врахування конкретних потреб організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cam-Winget N (ed.), Appala S, Pope S, Saint-Andre P (2019) Using Extensible Messaging and Presence Protocol (XMPP) for Security Information Exchange. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 8600. [Електронний ресурс]. – Режим доступу: https://doi.org/10.17487/RFC8600

2. Software Defined Perimeter Working Group “SDP Specification 1.0” Cloud Security Alliance. April 2014. – pp. 91-97

3. Stanton B, Theofanos MF, Spickard Prettyman S, Furman S (2016) Security Fatigue. IT Professional 18(5): pp. 26-32. [Електронний ресурс].– Режим доступу: https://ieeexplore.ieee.org/document/7579112

4. Strouble D, Shechtman GM, Alsop AS (2009) Productivity and Usability Effects of Using a Two-Factor Security System. SAIS 2009 Proceedings (AIS, Charleston, SC), p. 37. [Електронний ресурс] – Режим доступу: http://aisel.aisnet.org/sais2009/37

5. Weidman J, Grossklags J (2017) I Like It but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication. Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017) (ACM, Orlando, FL), C. 212-224. [Електронний ресурс] – Режим доступу: https://doi.org/10.1145/3134600.3134629.

6. G. Evan and D. Barth, Zero Trust Networks: Building Secure Systems in Untrusted Networks, Beijing, Boston, Frnham, Sebastopol, Tokyo: O'Reilly, 2017.

7. P. Ferrill, "What Is Zero Trust Architecture?," The New Stack, 17 June 2022. [Електронний ресурс]. – Режим доступу: https://thenewstack.io/what-is-zero-trust-architecture/.

8. M. James, "A 2022 Guide to Zero Trust for Data Protection," Smart Data Collective, 2022. [Електронний ресурс]. – Режим доступу: https://www.smartdatacollective.com/guide-to-zero-trust-for-data-protection/.

9. C. Winckless and S. Olyaei, "How to Decipher Zero Trust for Your Business," 22 May 2022. [Електронний ресурс]. – Режим доступу: www.gartner.com.

10. CISA, "Zero Trust Maturity Model," June 2021. [Електронний ресурс]. – Режим доступу: https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Mod el_Draft.pdf.

11. Microsoft Docs, "What is Conditional Access?," Microsoft, 22 April 2022. [Електронний ресурс]. – Режим доступу: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview.

12. C. Buck, C. Olenberger, A. Schweizer, F. Völter, T. Eymann. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zerotrust. Computers & Security, vol.112, Article number 102436, 2022. [Електронний ресурс]. – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S1084804520301168?via%3Dihub.

13. L. Cittadini, B. Spear, B. Beyer, M. Saltonstall. BeyondCorp: The access proxy. Security, 2016. – vol.41, no.4, pp. 28–33.

14. C. Cunningham. The Zero Trust Extended (ZTX) Ecosystem, Combridge, UK: Forrester Research, Inc., 2018. – 188 с.

15. Zero Trust основні принципи роботи [Електронний ресурс] – Режим доступу: https://www.microsoft.com/en-us/security/business/zero-trust.

16. J. Garbis, J. W. Chapman. Zero Trust Security: An Enterprise Guide, Berkeley, USA: Apress, 2021. – p. 35.

17. X. R. Wang, J. Yang, Q. Y. Wang, C. X. Su. Threat intelligence relationship extraction based on distant supervision and reinforcement learning.

In Proceedings of the 32nd International Conference on Software Engineering and Knowledge Engineering, pp.572–576, 2020.

18. S. A. Siddiqui, A. Mahmood, W. E. Zhang, Q. Z. Sheng. Machine learning based trust model for misbehaviour detection in internet-of-vehicles. In Proceedings of the 26th International Conference on Neural Information Processing, Sydney, Australia, 2019. – pp.512–520 [Електронний ресурс] – Режим доступу: https://link.springer.com/chapter/10.1007/978-3-030-36808-1_56.

19. Fortinet Multi-Cloud security challenges. [Електронний ресурс] – Режим доступу: https://www.fortinet.com/blog/industry-trends/multi-cloud-securitychallenges-key-tips.

20. Palo Alto Network Zero Trust. [Електронний ресурс] – Режим доступу: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture.

21. Liu Q. Data center security protection in the industry based on zero-trust architecture // Security & Informatization. 2018. – 12 par., pp. 107–109.

22. Yang Z., Jin M., Zhang X. Research on Security Technology of Zero Trust in Cloud Business // Information Security and Communications Privacy. 2020. – 3 par., pp. 91–98.

23. Zuo Y. Zero-trust architecture: a new paradigm for network security // Financial Computerizing. 2018. – 11 par., pp. 50–51.

24. Zeng H. Discussion on Network Security Model and Zerotrust Practice // Computer Products and Circulation. 2020. – 7 par., p. 48.

25. Zhong X., Guo W., Ma Y., Wang M. Airport Network Security Protection Scheme Based on Zero Trust Security Architecture // Journal of Civil Aviation, 2019. – 3(03). pp. 114–117.

26. Stafford, V.(2020). Zero trust architecture.NIST special publication, 800, 207. [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

27. Ward, R., & Beyer, B. (2014). Beyondcorp: A new approach to enterprise security. [Електронний ресурс] – Режим доступу: https://www.usenix.org/system/files/login/articles/login_dec14_02_ward.pdf.

28. Bavendiek,S.(2022).A zero trust security approach with FIDO2, preprint (Version 1) available at Research Square. [Електронний ресурс] – Режим доступу: https://doi.org/10.21203/rs.3.rs-2022891/.

29. Implementing a Zero Trust security model at Microsoft. Microsoft Insider Talk. [Електронний ресурс] – Режим доступу: https://www.microsoft.com/insidetrack/blog/implementing-a-zero-trust-security-model-at-microsoft/.

30. Zero trust: What it is, why you need it, and how to get started. Quest Blog. [Електронний ресурс] – Режим доступу: https://blog.quest.com/zero-trust-what-it-is-why-you-need-it-and-how-to-get-started/.

31. Security rapid modernization plan. Microsoft Learn. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/security/privileged-access-workstations/security-rapid-modernization-plan.

W. B. Daoud, M. S. Obaidat, A. Meddeb-Makhlouf, F. Zarai, and K.-F. Hsiao, ‘‘TACRM: Trust access control and resource management mechanism in fog computing,’’ Hum.-Centric Comput. Inf. Sci.,2019. – vol. 9, no. 1, p. 28.

32. Z. Zaheer, H. Chang, S. Mukherjee, and J. Van der Merwe, ‘‘eztrust: Network-independent zero-trust perimeterization for microservices,’’ in Proc. ACM Symp. SDN Res., 2019. – pp. 49–61.

33. C. DeCusatis, P. Liengtiraphan, A. Sager, and M. Pinelli, ‘‘Implementing zero trust cloud networks with transport access control and first packet authentication,’’ in Proc. IEEE Int. Conf. Smart Cloud (SmartCloud), Nov. 2016. – pp. 5–10.

34. S. W. Shah and S. S. Kanhere, ‘‘Smart user identification using cardiopulmonary activity,’’ Pervas. Mobile Comput., vol. 58, Aug. 2019,

35. A. Mosenia, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, ‘‘CABA: Continuous authentication based on bioaura,’’ IEEE Trans. Comput, 2017. – vol. 66, no. 5, pp. 759–772.

36. O. W. Group. The Oauth 2.1 Authorization Framework. Accessed: Mar. 6, 2022. [Електронний ресурс] – Режим доступу: https://datatracker.ietf.org/doc/html/ draft-ietf-oauth-v2-1-00.

37. S. Teerakanok, T. Uehara, A. Inomata. Migrating to zero trust architecture: Reviews and challenges. Security and Communication Networks, vol.2021, Article number 9947347, 2021. [Електронний ресурс] – Режим доступу: https://www.hindawi.com/journals/scn/2021/9947347/

38. Department of Defense. DoD Zero Trust Strategy, 2022 [Електронний ресурс] – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0167404821002601?via%3Dihub.

39. J. M. Pittman, S. Alaee, C. Crosby, T. Honey, G. M. Schaefer. Towards a model for zero trust data. American Journal of Science & Engineering, vol.3, no. 1, 2022. – pp. 18–24. [Електронний ресурс] – Режим доступу: https://www.ingentaconnect.com/content/smart/ajse/2022/00000003/00000001/art00003;jsessionid=beiq061de9jph.x-ic-live-02.

40. E. Gilman, D. Barth. Zero Trust Networks: Building Secure Systems in Untrusted Networks, O’Reilly Media, Inc., 2017. – pp. 134–143.

41. L. F. Huang. The firewall technology study of network perimeter security. In Proceedings of IEEE Asia-Pacific Services Computing Conference, Guilin, China, 2020. – pp. 410–413. [Електронний ресурс] – Режим доступу: https://ieeexplore.ieee.org/document/6478255

42. Jericho Forum Commandments, Version 1.2. [Електронний ресурс] – Режим доступу:https://static.spiceworks.com/attachments/post/0016/4842/commandments_v1.2.pdf

43. Escobedo, V.; Beyer, B.; Saltonstall, M.; Zyzniewski, F. BeyondCorp: The user experience. Login, 2017. – 42 par, pp. 38–43.

44. Govindan, K.; Mohapatra, P. Trust computations and trust dynamics in mobile adhoc networks: A survey. IEEE Commun. Surv. Tutorials, 2011. – 14 par, pp. 279–298.

45. Moubayed, A.; Refaey, A.; Shami, A. Software-Defined Perimeter (SDP): State of the Art Secure Solution for Modern Networks. Netwrk. Mag. Glob. Internetwkg, 2019. – 33 par, pp. 226–233.

46. Zolotukhin, M.; Hämäläinen, T.; Kotilainen, P. Intelligent Solutions for Attack Mitigation in Zero-Trust Environments. In Cyber Security; Lehto, M., Neittaanmäki, P., Eds.; Springer: Cham, Switzerland, 2022. – pp. 403–417.

47. SentinelOne, Sentinelone website, 2023. [Електронний ресурс] – Режим доступу: https://www.sentinelone.com/.

48. M. Compastié, S. Sisinni, S. Gurung, C. Fernández, L. Jacquin, I. Mlakar, V. Šafran, A. Lioy, I. Pedone, PALANTIR: Zero-Trust Architecture for Managed Security Service Provider, in 2022, pp. 83–98.

49. W. Steingartner, D. Galinec and A. Kozina, "Threat defense: Cyber deception approach and education for resilience in hybrid threats model," Symmetry, 2021. – p. 597.

50. S. O. Olabanji, O. O. Olaniyi, C. S. Adigwe, O. J. Okunleye and T. O. Oladoyinbo, "AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems," Asian Journal of Research in Computer Science, 2018. – pp. 38-56.

51. S. Stalla-Bourdillon, G. Thuermer, J. Walker, L. Carmichael and E. Simperl, "Data protection by design: Building the foundations of trustworthy data sharing," Data & Policy, 2020. – p. 4.

52. L. Alevizos, V. T. Ta and M. Hashem Eiza, "Augmenting zero trust architecture to endpoints using blockchain: A state- of- the- art review," Security and Privacy, 2022. – p. 191.

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Тези наукових доповідей

- Taras Kyrychuk, Mykola Brailovskyi – Improving the protection system of the zero trust model – Information Technology and Implementation (Satellite), 21 November, 2023. – pp. 90-92
- Brailovskyi Nikolay, Khoroshko Volodymyr, Serhii Toluipa, Taras Kyrychuk – Model of implementation of management of access to information assets in the concept of zero trust – Kyiv, Taras Shevchenko National University of Kyiv, 2023. – p. 10-18.