Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Шаповалова Євгенія Вікторовича*

академічної групи *125-20-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Аналіз розвитку та розробка методики використання мереж з нульовою довірою*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., проф. Котух Є.В.			
розділів:				
спеціальний	ас. Рибальченко Ю.П.			
економічний	к. е. н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	Мєшков В.І.			

Дніпро 2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту ***Шаповалов Є.В.*** **академічної групи** ***125-20-3***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Аналіз розвитку та розробка методики використання мереж з нульовою довірою***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № _____

Розділ	Зміст	Термін виконання
1	Аналіз розвитку мереж з нульовою довірою, дослідження існуючих підходів та методологій.	26.05.2024
2	Розробка методики використання мереж з нульовою довірою, визначеннння ключових компонентів та етапів впровадження	19.06.2024
3	Розрахунок річних витрат на розробку комплексу технічного захисту інформації, оцінка величини збитку. Розрахунок ефективності запропонованого комплексу.	26.06.2024

Завдання видано _____ Рибальченко Ю.П.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 06.05.2024

Дата подання до екзаменаційної комісії: 01.07.2024

Прийнято до виконання _____ Шаповалов Є.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить 66 с., 9 табл., 6 додатків, 43 джерел.

Об`єкт дослідження: процес впровадження мереж з нульовою довірою в інформаційних системах.

Мета роботи: забезпечення безпеки інформаційних активів шляхом впровадження методики використання мереж з нульовою довірою.

У першому розділі кваліфікаційної роботи проведено аналіз теоретичних основ мереж з нульовою довірою, досліджено еволюцію цієї концепції, проаналізовані сучасні підходи до забезпечення кібербезпеки, а також сформульовані основні задачі даної кваліфікаційної роботи.

У спеціальній частині проведено аналіз розвитку мереж з нульовою довірою, в рамках розробки методики їх використання запропоновані організаційні, технічні та програмні заходи щодо впровадження принципів нульової довіри в мережеву інфраструктуру підприємств.

В економічному розділі визначені витрати на розробку і впровадження мережі з нульовою довірою та проведено аналіз її економічної ефективності.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні рівня кібербезпеки підприємств шляхом впровадження розробленої методики використання мереж з нульовою довірою.

ІНФОРМАЦІЙНА БЕЗПЕКА, МЕРЕЖІ З НУЛЬОВОЮ ДОВІРОЮ, КІБЕРБЕЗПЕКА, УПРАВЛІННЯ ДОСТУПОМ, ТЕХНОЛОГІЇ НУЛЬОВОЇ ДОВІРИ.

ABSTRACT

The explanatory note contains 66 pages, 9 tables, 6 appendices, 43 sources.

Object of study: The process of implementing zero trust networks in information systems.

Purpose of the work: To ensure the security of information assets through the implementation of a methodology for using zero trust networks.

In the first section of the qualification work, an analysis of the theoretical foundations of zero trust networks was conducted, the evolution of this concept was studied, modern approaches to ensuring cybersecurity were analyzed, and the main tasks of this qualification work were formulated.

In the special section, an analysis of the development of zero trust networks was conducted. As part of developing a methodology for their use, organizational, technical, and software measures were proposed for implementing zero trust principles in the network infrastructure of enterprises.

In the economic section, the costs for developing and implementing a zero trust network were determined, and an analysis of its economic efficiency was conducted.

The practical significance of the qualification work results lies in increasing the level of cybersecurity for enterprises through the implementation of the developed methodology for using zero trust networks.

INFORMATION SECURITY, ZERO TRUST NETWORKS, CYBERSECURITY, ACCESS MANAGEMENT, ZERO TRUST TECHNOLOGIES.

ЗМІСТ

ВСТУП

Обґрунтування актуальності обраної теми. У сучасному цифровому світі питання кібербезпеки стають дедалі актуальнішими, оскільки зростає кількість та складність кібератак. Традиційні методи захисту, які базуються на ідеї периметрової безпеки, більше не є достатніми для захисту інформаційних активів організацій. Мережі з нульовою довірою (Zero Trust Networks) представляють новий підхід до безпеки, де жоден користувач або пристрій не є автоматично довіреним, незалежно від його розташування у мережі. Це робить тему дослідження розвитку та впровадження мереж з нульовою довірою надзвичайно актуальною.

Актуальність теми "Аналіз розвитку та розробка методики використання мереж з нульовою довірою" полягає в постійному зростанні кіберзагроз та необхідності забезпечення надійного захисту даних в умовах сучасного цифрового світу. З розвитком технологій і збільшенням кількості підключених пристроїв ризики безпеки також зростають, що вимагає нових підходів до захисту інформації. Традиційні методи захисту, що базуються на периметровій безпеці, виявляються недостатньо ефективними, оскільки зловмисники знаходять нові способи обходу захисних бар'єрів.

Мережі з нульовою довірою (Zero Trust Networks) пропонують інноваційний підхід до кібербезпеки, що передбачає постійну верифікацію кожного користувача та пристрою, незалежно від їхнього місцезнаходження. Такий підхід дозволяє мінімізувати ризики несанкціонованого доступу та витоку даних, що є критично важливим для сучасних організацій. Використання мереж з нульовою довірою також сприяє підвищенню ефективності управління безпекою, дозволяючи краще контролювати доступ до ресурсів і вчасно виявляти потенційні загрози.

Важливість розробки методики використання мереж з нульовою довірою полягає у створенні системного підходу до впровадження цього підходу в організаціях різного масштабу. Методика дозволяє структурувати

процеси забезпечення безпеки, визначити основні етапи та кроки, необхідні для успішного впровадження, а також розробити рекомендації щодо адаптації під конкретні потреби організації. Такий підхід сприятиме підвищенню рівня кібербезпеки та забезпечить більш надійний захист критичних даних.

Зв'язок проблеми, що вирішується, з об'єктом діяльності фахівця спеціальності. Проблема забезпечення кібербезпеки є ключовою для фахівців у сфері інформаційних технологій та кібербезпеки. Спеціалісти, що працюють у цій галузі, стикаються з необхідністю захисту інформаційних систем від внутрішніх та зовнішніх загроз. Впровадження мереж з нульовою довірою дозволяє забезпечити високий рівень безпеки, контролюючи доступ до інформаційних ресурсів на всіх рівнях. Це робить дану тему надзвичайно важливою для фахівців, що займаються кібербезпекою.

Сучасний стан проблеми. Незважаючи на активний розвиток технологій кібербезпеки, багато організацій все ще використовують застарілі методи захисту, що базуються на периметровій безпеці. Водночас, зростає кількість досліджень та розробок у сфері мереж з нульовою довірою, які демонструють їхню ефективність у захисті інформаційних систем. Однак, існує низка протиріч та прогалин у знаннях, які стосуються впровадження та використання цієї технології. Зокрема, багато організацій стикаються з труднощами у інтеграції мереж з нульовою довірою зі своїми існуючими системами та процесами.

ПОСТАНОВКА ЗАДАЧІ

Мета роботи

Метою даної кваліфікаційної роботи є аналіз розвитку мереж з нульовою довірою та розробка методики їх використання для забезпечення кібербезпеки організацій. Для досягнення цієї мети було поставлено такі задачі:

Дослідити сучасний стан та розвиток технології мереж з нульовою довірою.

Визначити основні принципи та вимоги до впровадження мереж з нульовою довірою.

Розробити методику впровадження мереж з нульовою довірою в інформаційні системи організацій.

Оцінити економічну доцільність впровадження даної технології.

Надати рекомендації щодо інтеграції мереж з нульовою довірою з існуючими системами кібербезпеки.

Теоретична значущість та прикладна цінність отриманих результатів

Теоретична значущість роботи полягає у систематизації знань про мережі з нульовою довірою, визначенні їх основних характеристик та вимог до впровадження. Прикладна цінність результатів дослідження полягає у розробці практичних рекомендацій щодо впровадження та використання мереж з нульовою довірою, що дозволить організаціям підвищити рівень безпеки своїх інформаційних систем, знизити ризики кібер-атак та оптимізувати процес управління доступом до інформаційних ресурсів.

ТЕОРЕТИЧНІ ОСНОВИ МЕРЕЖ З НУЛЬОВОЮ ДОВІРОЮ

1.1. Визначення та принципи нульової довіри

У зв'язку з тим, що зловмисники стають дедалі хитрішими, підприємствам необхідно постійно вдосконалювати свої політики безпеки та засоби контролю, щоб відповідати новим загрозам. Через ускладнення технологічного ландшафту збільшується поверхня атак, що створює більше можливостей для хакерів здійснювати масштабні атаки.

Таблиця 1.1. – Принципи нульової довіри

Номер	Пункт	Опис
1.1.1	Визначення нульової довіри	Нульова довіра - це концепція кібербезпеки, яка передбачає перевірку кожного доступу, незалежно від того, звідки він походить, будь то з мережі організації чи ззовні. Це підхід, який не довіряє жодному пристрою чи користувачу за замовчуванням, навіть якщо вони знаходяться всередині мережі.
1.1.2	Принцип 1: Перевірка завжди	Кожен доступ до системи або ресурсу повинен бути автентифікований і авторизований перед тим, як дозволити користувачу або пристрою отримати доступ. Це включає багатофакторну автентифікацію (MFA) і постійну перевірку привілеїв.
1.1.3	Принцип 2: Мінімальні права	Користувачі та пристрої повинні мати мінімальні необхідні права доступу для виконання своїх завдань. Це обмежує потенційні наслідки компрометації облікових записів або пристроїв.

1.1.4	Принцип 3: Сегментація мережі	Розподіл мережі на сегменти допомагає ізолювати окремі ресурси і обмежити рух даних між різними частинами мережі. Це зменшує площу потенційної атаки і допомагає запобігти поширенню загроз.
1.1.5	Принцип 4: Моніторинг та аналіз	Постійний моніторинг діяльності в мережі для виявлення аномалій і загроз. Використання інструментів для аналізу поведінки дозволяє швидко виявляти і реагувати на підозрілу активність.
1.1.6	Принцип 5: Динамічне застосування політик	Використання політик доступу, що автоматично адаптуються до змін в середовищі, таких як нові загрози або зміни в конфігурації мережі. Це забезпечує гнучкість і ефективність у підтримці безпеки.

Таблицю розроблено на основі джерела [1].

Модель нульової довіри стала потужною стратегією у боротьбі з цими викликами. Вона базується на принципі "ніколи не довіряй, завжди перевіряй", змінюючи підхід організацій до управління доступом та видимістю мережі. Проте, як і будь-яка модель безпеки, нульова довіра має свої переваги та виклики.

Основною перевагою нульової довіри є підвищений рівень безпеки мережі, захист як від зовнішніх атак, так і від внутрішніх загроз. Вона також ефективно масштабується для гібридних і віддалених робочих середовищ.

Забезпечуючи доступ виключно за принципом службової необхідності, нульова довіра зменшує поверхню атаки та ускладнює зловмисникам завдання отримати несанкціонований доступ. Це підвищений рівень безпеки, який особливо корисний у сучасному технологічному середовищі, де кіберзагрози стають все більш поширеними та складними.

Модель нульової довіри забезпечує організаціям детальну видимість їхньої мережевої діяльності. Це дозволяє контролювати, хто, коли і звідки отримує доступ до ресурсів, що має вирішальне значення для швидкого виявлення незвичайної активності та запобігання потенційним зламам та іншим інцидентам безпеки.

Покращена видимість також дає змогу організаціям краще розуміти свої мережеві операції, виявляти потенційні вразливості та приймати обґрунтовані рішення щодо розподілу ресурсів та управління ризиками.

Інсайдерські загрози, будь то зловмисні або випадкові, становлять значний ризик для організацій. Модель нульової довіри зменшує цей ризик, застосовуючи однаково суворий контроль доступу для всіх користувачів, незалежно від їхньої ролі в організації. Це гарантує, що навіть у разі компрометації облікових даних інсайдера, потенційну шкоду можна мінімізувати [2].

Розглядаючи кожен запит на доступ як потенційно небезпечний, модель нульової довіри значно знижує ймовірність внутрішніх загроз, що можуть призвести до витоку даних. Хоча зменшення поверхні атаки та обмеження доступу до даних через сегментацію допомагають захиститися від витоків, зламів та перехоплень, вони не є ефективними, якщо дані не захищені під час передачі та зберігання [3].

Модель нульової довіри забезпечує надійний захист даних, гарантуючи, що доступ надається лише тим, кому це дійсно необхідно для виконання конкретних завдань. Такий підхід не лише запобігає несанкціонованому доступу, але й зменшує ризик переміщення або копіювання даних без дозволу.

Завдяки нульовій довірі організації можуть забезпечити безпеку своїх конфіденційних даних під час зберігання та передачі, що допомагає дотримуватися норм захисту даних і зберігати довіру клієнтів.

Модель нульової довіри добре підходить для сучасних робочих середовищ, які часто включають віддалену роботу та використання персональних мобільних пристроїв. Перевіряючи кожен запит на доступ

незалежно від його походження, модель нульової довіри може забезпечити гнучкі робочі домовленості без шкоди для безпеки.

Однак, незважаючи на явні переваги додаткової безпеки, яку надає модель нульової довіри, вона має певні недоліки, такі як складність впровадження та витрати ресурсів, а також можливість виникнення розчарування через громіздкі процеси входу та хибні спрацьовування.

Впровадження моделі безпеки з нульовою довірою може бути складним завданням. Це потребує глибокого розуміння мережі, включаючи всіх користувачів, пристрої, програми та дані. Крім того, це може вимагати значних змін в існуючій інфраструктурі безпеки, що може бути дорогим і порушити звичний порядок. Організації повинні бути готові виділити час та ресурси, необхідні для успішного впровадження моделі нульової довіри [4].

Суворий контроль доступу в рамках моделі нульової довіри може викликати розчарування у користувачів. Співробітники можуть вважати постійні перевірки громіздкими, особливо якщо вони заважають ефективно виконувати робочі завдання. Це може призвести до опору впровадженню моделі нульової довіри, а в деяких випадках співробітники можуть намагатися обійти засоби контролю безпеки, створюючи нові вразливості.

Впровадження та підтримка моделі нульової довіри є ресурсоємними процесами. Це вимагає постійного моніторингу та керування мережевими діями, що може створити навантаження на IT-ресурси організації. Крім того, потреба в передових інструментах та технологіях безпеки може збільшити витрати. Організаціям необхідно враховувати ці вимоги до ресурсів при розгляді підходу нульової довіри.

Суворий характер моделі нульової довіри може призвести до помилкових спрацьовувань, коли законні користувачі або дії позначаються як підозрілі. Це може порушити робочі процеси та призвести до непотрібних розслідувань, витрачаючи час і ресурси. Хоча помилкові спрацьовування можна зменшити шляхом налаштування, вони залишаються проблемою в моделі нульової довіри.

Безпека нульової довіри значною мірою залежить від технологій, включаючи передові інструменти безпеки та технології для підтвердження особистості, шифрування та сегментації мережі. Якщо ці технології вийдуть з ладу, організація може стати вразливою. З розвитком технологій виникає потреба в постійних оновленнях та інвестиціях, щоб забезпечити ефективність моделі нульової довіри.

Незважаючи на ці виклики, існують різні методи, які допомагають зменшити проблеми, пов'язані зі створенням мережі з нульовою довірою, і при цьому отримати її переваги [5].

Поступове впровадження

Однією з тактик для подолання проблем, пов’язаних із нульовою довірою, є поетапне впровадження цієї моделі. Замість спроби змінити всю мережу одразу, організації можуть почати з невеликої частини своєї інфраструктури. Це може бути окремий відділ, конкретний тип даних або певний набір програм. Поступове впровадження дає можливість організаціям вчитися і адаптуватися в процесі, знижуючи ризик збоїв і роблячи перехід більш керованим.

Інвестиції в зручні рішення

Наразі існує багато інструментів і технологій безпеки нульової довіри, орієнтованих на зручність для користувача. Ці рішення забезпечують максимально плавні процеси перевірки та мінімізують перешкоди для робочих процесів співробітників. Вибираючи зручні рішення, організації можуть забезпечити більшу ймовірність прийняття моделі нульової довіри співробітниками.

Регулярне навчання та комунікація

Регулярне навчання і комунікація є важливими для подолання проблем, пов'язаних з нульовою довірою. Співробітники повинні розуміти, чому організація впроваджує модель нульової довіри, як вона працює та що потрібно робити, щоб відповідати вимогам. Регулярні тренінги можуть допомогти співробітникам усвідомити важливість нульової довіри та її роль у

захисті організації. Чітка і послідовна комунікація також може допомогти зменшити будь-які занепокоєння чи опір серед працівників [6].

Планування ресурсів

Організаціям можливо доведеться наймати додатковий IT-персонал або підвищувати кваліфікацію наявних співробітників для ефективної роботи з новими навантаженнями.

Постійне вдосконалення

Вирішення проблем, пов'язаних із нульовою довірою, потребує постійного вдосконалення. Це включає регулярний перегляд і налаштування засобів контролю доступу, моніторинг хибних спрацьовувань і оновлення технологій за необхідності. Постійне вдосконалення моделі нульової довіри дозволяє організаціям зберігати її ефективність і актуальність перед обличчям нових загроз і змін у бізнес-середовищі [7].

Актуальність та важливість досліджуваної проблеми

Проблеми безпеки в корпоративних мережах, використання Active Directory, концепція нульової довіри та захист від програм-вимагачів активно обговорюються у численних наукових роботах та дослідженнях. Проте нові цифрові загрози вимагають постійного оновлення та розвитку підходів до захисту інформації.

Active Directory (AD) — це технологія від Microsoft, що забезпечує управління ідентифікацією та авторизацією користувачів у корпоративних мережах. Вона надає єдину точку входу для управління ідентифікацією, політиками безпеки, інтернет-протоколами та іншими мережевими компонентами.

Концепція нульової довіри (Zero Trust) базується на принципі "нікому не довіряти", незалежно від того, чи знаходиться користувач або пристрій всередині мережі чи за її межами. Це означає, що кожен запит до системи повинен проходити незалежну верифікацію, незалежно від джерела запиту [8].

Програми-вимагачі — це шкідливе програмне забезпечення, яке блокує доступ до системи або файлів користувача і вимагає викуп за їх відновлення.

Вони можуть бути особливо небезпечними для корпоративних мереж, оскільки блокують доступ до критично важливих систем або даних.

Взаємозв'язок між елементами

Програми-вимагачі можуть атакувати корпоративні мережі, що використовують Active Directory для управління доступом. В цьому контексті концепція нульової довіри стає надзвичайно корисною, оскільки вона передбачає постійну верифікацію та перевірку всіх елементів системи, включаючи запити на доступ до ресурсів. Це допомагає виявити і заблокувати програми-вимагачі до того, як вони завдадуть шкоди [9].

Модель нульової довіри забороняє доступ до цифрових ресурсів організації за замовчуванням і надає його лише автентифікованим користувачам, які мають відповідні права, незалежно від фізичної локації пристрою чи його власності. Такий підхід допомагає виявляти програми-вимагачі завдяки суворій перевірці особи кожного користувача та пристрою при кожному запиті, зменшуючи ймовірність несанкціонованого доступу та поширення шкідливого ПЗ у мережі.

Перегляд та аналіз мережевого трафіку

Модель Zero Trust зосереджується на постійному аналізі мережевого трафіку для виявлення незвичної активності, яка може свідчити про можливу атаку зловмисників. Постійна перевірка кожного етапу доступу та ретельний моніторинг аномальної поведінки дозволяють виявляти програми-вимагачі на ранніх стадіях їхнього проникнення [10, с.72].

Мінімально необхідний доступ

Модель Zero Trust також акцентує увагу на наданні користувачам і пристроям тільки тих привілеїв, які необхідні для виконання конкретних завдань. Обмеження доступу знижує можливість здійснення зловмисних дій. Якщо користувач або пристрій з обмеженим доступом намагається виконати підозрілі дії або отримати доступ до несанкціонованих ресурсів, це може викликати сповіщення та ініціювати реагування на потенційну загрозу.

Комплексний підхід до виявлення програм-вимагачів

Поєднання моделі Zero Trust з іншими методами, такими як статичний аналіз файлів, моніторинг аномалій виконання файлів і розширений аналіз шкідливого програмного забезпечення, забезпечує комплексний підхід до виявлення та нейтралізації атак програм-вимагачів. Впровадження моделі Zero Trust дозволяє організаціям ефективніше виявляти та реагувати на загрози з боку програм-вимагачів, знижуючи їхній потенційний вплив [11, с.221].

Процес впровадження Zero Trust

Впровадження концепції Zero Trust є безперервним процесом, що включає широкий спектр процесів і технологій. Існують перевірені фреймворки, які спрощують впровадження цієї концепції, зокрема план швидкої модернізації Microsoft (RAMP). Цей план допомагає швидко прийняти стратегію привілейованого доступу, застосовуючи принцип найменших привілеїв до кожного рішення щодо доступу. Це дозволяє або забороняє доступ до ресурсів на основі кількох контекстних факторів, а не лише однієї попередньої автентифікації.

Інтеграція принципів Zero Trust

Для досягнення максимальних результатів принципи Zero Trust повинні пронизувати більшість аспектів IT-екосистеми. Кожен пункт у RAMP структурований як ініціатива, що відстежується та керується за допомогою методології цілей та ключових результатів. Деякі пункти потребують змін у процесах і підвищення кваліфікації персоналу, тоді як інші вимагають технологічних змін. Впровадження цих змін часто включає участь членів організації поза межами традиційного IT-відділу для забезпечення успішної інтеграції [12, с.34].

План включає наступні пункти[12]:

Відокремлення та управління привілейованими обліковими записами:

а. Створення облікових записів для екстреного доступу. Це передбачає створення спеціальних акаунтів, які допоможуть уникнути випадкового блокування в Active Directory в надзвичайних ситуаціях. Такі облікові записи

використовуються рідко, але їх наявність є критично важливою в певних сценаріях. При компрометації вони можуть завдати значної шкоди організації.

b. Визначення та категоризація привілейованих облікових записів. Це включає визначення всіх ролей та груп з високими привілеями, що потребують вищого рівня безпеки. Для них слід створити окремі облікові записи адміністраторів з мінімальними необхідними правами, а також видалити непотрібні акаунти.

Покращення управління обліковими записами:

a. Впровадження та документування самостійного скидання пароля та комбінованої реєстрації інформації безпеки. Налаштування самостійного скидання пароля дозволяє користувачам самостійно відновлювати свої паролі після реєстрації. Комбінована реєстрація забезпечує кращу взаємодію з користувачем, дозволяючи одночасно реєструватися для багатофакторної автентифікації та скидання пароля.

b. Захист облікових записів адміністратора. Всі привілейовані облікові записи повинні використовувати багатофакторну автентифікацію (MFA). Це стосується всіх користувачів, яким призначено одну або кілька адміністративних ролей. Для підвищення захисту слід впровадити методи входу без пароля, такі як ключі безпеки FIDO2 або Windows Hello, у поєднанні з унікальними, довгими і складними паролями [13, с.87].

c. Блокування застарілих протоколів автентифікації для привілейованих облікових записів. Застарілі протоколи автентифікації слід блокувати, оскільки для них неможливо застосувати багатофакторну автентифікацію, що створює потенційні точки входу для зловмисників. Деякі застарілі програми можуть покладатися на ці протоколи, тому організації можуть створювати окремі винятки для певних облікових записів, які слід ретельно відстежувати та впроваджувати додаткові засоби моніторингу.

d. Створення процесу погодження програмного забезпечення. Необхідно обмежити користувачів у можливості встановлювати стороннє програмне забезпечення, надаючи дозволи лише на обрані програми. Для

програмного забезпечення, яке не відповідає цим критеріям, слід запровадити процес централізованого прийняття рішень командою адміністраторів безпеки.

е. Моніторинг облікових записів та входів у систему. Важливо відстежувати маніпуляції з акаунтами користувачів та їх входи у систему, оскільки акаунти можуть бути скомпрометовані як зовнішніми загрозами, так і внутрішніми. Також слід розгортати спеціальні робочі станції для привілейованих облікових записів, таких як глобальні адміністратори, щоб захистити їх від атак. Захист робочих станцій, на яких виконуються адміністративні завдання, є критично важливим для зменшення площі потенційної атаки. Це розділення обмежує їхню вразливість до звичайних атак, зокрема атак, пов’язаних з електронною поштою.

Принципи нульової довіри у кібербезпеці передбачають, що жодна особа чи пристрій не має автоматичного довіряти за замовчуванням, навіть якщо вони знаходяться всередині захищеної мережі. Це означає, що кожен запит на доступ до ресурсів мережі повинен бути строго перевірений та авторизований перед наданням доступу. Основна ідея полягає в тому, щоб перевіряти ідентичність і права доступу кожного користувача і пристрою незалежно від їхнього місцезнаходження чи статусу в мережі [14, с.6253].

Цей підхід відрізняється від традиційних моделей захисту, які часто покладаються на периметральний захист, тобто захист на рівні кордону мережі. В контексті нульової довіри, периметр мережі розглядається як потенційно вразлива точка, а не як єдиний захисний бар'єр. Це дозволяє краще контролювати і моніторити активності всередині мережі і виявляти навіть найбільш витончені атаки, що існують.

Впровадження принципів нульової довіри передбачає використання таких технологій, як багатофакторна аутентифікація, мікросегментація мережі, шифрування даних та системи моніторингу поведінки користувачів і пристроїв. Це сприяє створенню більш надійного і безпечного інформаційного

середовища, яке відповідає сучасним викликам у сфері кібербезпеки і забезпечує захист від різноманітних загроз.

Принципи нульової довіри базуються на ідеї, що всі запити на доступ до ресурсів мережі повинні бути обґрунтовані, перевірені і авторизовані перед наданням доступу. Основний принцип полягає в тому, що жоден користувач чи пристрій не автоматично довіряються без додаткової перевірки. Це підходить як для зовнішніх, так і для внутрішніх користувачів мережі, незалежно від їхнього місцезнаходження чи статусу.

Інший важливий принцип - це строге контролювання і аудит кожного кроку доступу до ресурсів. Це означає, що кожен запит на доступ повинен бути відслідковуваний і записаний, щоб в разі потреби проводити розслідування та аналіз подій. Такий підхід дозволяє оперативно реагувати на потенційні загрози і мінімізувати ризики компрометації даних чи інформаційних ресурсів.

Нульова довіра включає в себе принципи мікросегментації мережі, що передбачає розділення мережі на окремі сегменти і обмеження доступу до кожного з них. Це дозволяє знизити поверхню атак і ускладнити задачу для потенційних зловмисників. Такий підхід сприяє збереженню безпеки навіть у разі компрометації одного з сегментів мережі [15, с.10].

Для створення нульової довіри в мережевих системах існує кілька ключових методів, які варто враховувати. Перший метод полягає в імплементації строгого контролю доступу, що включає в себе багатофакторну аутентифікацію, де кожен користувач має підтверджувати свою ідентичність не лише паролем, але й додатковими методами, такими як біометричні дані чи фізичні пристрої аутентифікації. Це дозволяє ускладнити завдання для потенційних зловмисників, які намагаються отримати несанкціонований доступ до системи.

Другий метод включає в себе мікросегментацію мережі, де мережа розділяється на окремі сегменти і кожному сегменту присвоюється власні правила доступу. Це дозволяє обмежити рух між сегментами і у разі

компрометації одного сегменту унеможливити зловмисникам вільний доступ до всієї мережі. Такий підхід сприяє збереженню безпеки даних і мінімізації ризиків.

Третій метод передбачає використання шифрування даних на всіх рівнях мережі, що включає в себе як шифрування даних в спокійному стані, так і під час їх передачі по мережі. Це забезпечує додатковий рівень захисту від перехоплення та несанкціонованого доступу до конфіденційної інформації. Комбінація цих методів дозволяє створити комплексну і ефективну систему нульової довіри, яка забезпечує високий рівень безпеки і захисту мережевих ресурсів в сучасному цифровому середовищі.

Нульова довіра, або Zero Trust, є концепцією кібербезпеки, яка базується на принципі, що жодному суб'єкту, незалежно від того, знаходиться він всередині чи зовні мережі, не можна довіряти за замовчуванням. Цей підхід виник у відповідь на зростання кількості кіберзагроз і витоків даних, які часто відбуваються через недостатній контроль доступу та відсутність належного моніторингу мережевої активності. У моделі нульової довіри кожен запит на доступ перевіряється незалежно від джерела, що дозволяє зменшити ризик внутрішніх і зовнішніх атак [16, с.50].

Основний принцип нульової довіри полягає в тому, щоб «нікому не довіряти, завжди перевіряти». Це означає, що доступ до ресурсів надається лише на основі строгих умов автентифікації і авторизації, навіть якщо користувач чи пристрій вже знаходяться в мережі. Кожен користувач і пристрій повинні бути постійно верифіковані, а їхні дії слід контролювати і аналізувати для виявлення аномалій. Таким чином, нульова довіра забезпечує більш високий рівень безпеки порівняно з традиційними підходами, які часто покладаються на периметральний захист.

Для реалізації моделі нульової довіри використовуються різні технології та інструменти, включаючи багатофакторну автентифікацію, шифрування даних, моніторинг мережевої активності та мікросегментацію. Мікросегментація дозволяє розділити мережу на дрібніші, ізольовані

сегменти, кожен з яких має свої власні правила доступу і безпеки. Це допомагає запобігти поширенню атак по всій мережі та забезпечити більш точний контроль доступу до критично важливих ресурсів.

Застосування принципів нульової довіри сприяє підвищенню кібербезпеки організації, зменшуючи ризики компрометації даних та забезпечуючи надійний захист від різних видів загроз. Цей підхід також дозволяє швидше виявляти і реагувати на інциденти, що покращує загальну стійкість організації до кіберзагроз. У сучасному світі, де кількість кіберзагроз постійно зростає, нульова довіра стає все більш актуальною і необхідною для забезпечення надійного захисту інформаційних ресурсів.

Впровадження моделі нульової довіри вимагає від організацій перегляду своїх поточних підходів до кібербезпеки і управління доступом. Одним з ключових кроків є створення детальної політики безпеки, яка визначає правила і процедури для перевірки кожного запиту на доступ. Це включає розробку та застосування механізмів автентифікації, що підтверджують особу користувачів, та авторизації, яка визначає їхні права доступу до ресурсів [17, с.21].

Іншим важливим аспектом є моніторинг і аналіз активності в мережі для виявлення аномалій та потенційних загроз. Використання засобів моніторингу дозволяє в реальному часі відслідковувати дії користувачів і пристроїв, а також швидко реагувати на підозрілу активність. Це дає можливість мінімізувати потенційні збитки від атак і запобігти подальшому поширенню загроз.

Нульова довіра передбачає сегментацію мережі для ізоляції різних компонентів і зменшення ризику поширення атак. Мікросегментація допомагає розподілити мережевий трафік на окремі сегменти, що дозволяє контролювати доступ до кожного з них незалежно від інших. Це забезпечує більш гнучке і точне управління безпекою та знижує ймовірність успішних атак на всю мережу.

Важливу роль в реалізації нульової довіри відіграє навчання персоналу та підвищення їхньої обізнаності щодо кібербезпеки. Користувачі повинні розуміти важливість дотримання політик безпеки та бути в курсі найсучасніших методів захисту інформації. Це включає регулярне навчання, проведення тренінгів і семінарів, а також запровадження системи заохочення за відповідальне ставлення до безпеки.

Загалом, модель нульової довіри є ефективним підходом до забезпечення кібербезпеки, який дозволяє значно знизити ризики компрометації даних і захистити критично важливі ресурси організації. Вона сприяє створенню більш надійного і стійкого інформаційного середовища, яке здатне протистояти сучасним кіберзагрозам. Організації, що впроваджують принципи нульової довіри, отримують можливість ефективніше захищати свої дані і забезпечувати безпеку своїх інформаційних систем.

На завершення, важливо враховувати, що успішна реалізація нульової довіри вимагає постійного вдосконалення і адаптації до нових загроз і технологій. Організації повинні систематично оновлювати свої підходи до кібербезпеки, враховуючи останні тренди та рекомендації індустрії. Крім того, важливо підтримувати партнерські відносини з провідними виробниками кібербезпечних технологій і спеціалізованими консультантськими компаніями, що дозволить вчасно реагувати на нові виклики і отримувати доступ до передових рішень.

Загалом, нульова довіра не лише підвищує рівень безпеки інформаційних ресурсів, але і сприяє збереженню довіри користувачів і партнерів. Вона стає основою для стійкого розвитку цифрових бізнес-екосистем, де кожен елемент мережі має захищений доступ і здатність функціонувати в умовах постійно змінюваного кіберзагрозами середовища.

Цей підхід до кібербезпеки є необхідним для сучасних організацій, що працюють в умовах високих технологічних викликів і потребують надійного захисту від різних форм кіберзагроз.

1.2. Історія та еволюція концепції нульової довіри

Концепція нульової довіри з'явилася у середині 2000-х років як відповідь на зростання кількості складних кіберзагроз і необхідність зміни підходів до кібербезпеки. Її виникнення пов'язане з усвідомленням того, що традиційні методи, які базуються на відносно м'яких периметральних заходах безпеки, не можуть ефективно захистити організації від сучасних атак.

Таблиця 1.2. – Еволюція концепції нульової довіри

Номер	Пункт	Опис
1.2.1	Початок концепції нульової довіри	Поняття нульової довіри (Zero Trust) було вперше сформульовано компанією Forrester Research в 2010 році. Ключова ідея полягає в тому, щоб не довіряти жодному користувачеві чи пристрою за замовчуванням, незалежно від того, де вони знаходяться.
1.2.2	Запровадження технологій мікропериметрів	З концепцією нульової довіри було пов’язано впровадження технологій мікропериметрів, що дозволяють створювати ізольовані сегменти мережі для кожного користувача чи пристрою.
1.2.3	Розвиток багатофакторної автентифікації	З ростом загроз та комплексності атак була розроблена багатофакторна автентифікація (MFA), яка стала необхідною складовою нульової довіри для підвищення рівня безпеки.
1.2.4	Застосування машинного навчання в кібербезпеці	Сучасні рішення нульової довіри використовують машинне навчання та аналітику для постійного моніторингу та виявлення аномалій в мережі, що дозволяє ефективно реагувати на потенційні загрози.

1.2.5	Розширення концепції на облічувані середовища	Останні роки свідчать про розширення концепції нульової довіри на облічувані середовища, такі як хмарні платформи і контейнеризація, що вимагає нових підходів до забезпечення безпеки.

Таблицю розроблено на основі джерела [2].

Перші концептуальні основи нульової довіри були сформульовані Джоном Хецерсоном з компанії Forrester Research, який висловив ідею, що в сучасному цифровому середовищі потрібно переглянути підходи до контролю доступу і ввести строгіші стандарти перевірки ідентифікації.

Протягом наступних десятиліть концепція нульової довіри зазнала значних еволюційних змін і вдосконалень. Вона перейшла від теоретичного концепту до практичної моделі безпеки, яка активно впроваджується в крупних корпоративних інформаційних системах і мережах.

Сьогодні нульова довіра визнається як один із найбільш передових і ефективних підходів до забезпечення кібербезпеки. Вона стала стандартом для багатьох організацій, які прагнуть максимально захистити свої цифрові активи від різних видів загроз і забезпечити безпеку даних і інформаційних ресурсів на всіх рівнях інфраструктури [18, с.15].

Один із ключових моментів у розвитку концепції нульової довіри був перехід від традиційної моделі "довіряй, але перевіряй" до "нікому не довіряй, завжди перевіряй". Це відображає змінений підхід до управління доступом і захисту даних, де кожен запит на доступ розглядається як потенційний ризик і повинен бути обгрунтованим і перевіреним перед наданням.

З часом концепція нульової довіри також динамічно адаптується до нових викликів і технологічних інновацій. Вона включає в себе використання штучного інтелекту і машинного навчання для виявлення аномальних активностей і попередження потенційних загроз з метою максимального захисту мережевих систем.

Сьогодні концепція нульової довіри є не просто технічним підходом, але й стратегічною ініціативою, яка спрямована на підвищення загального рівня кібербезпеки в організаціях у всіх галузях індустрії. Вона дозволяє підприємствам ефективно захищати свої інформаційні активи, забезпечуючи безпеку, прозорість і стійкість у цифровому середовищі, яке постійно змінюється і вдосконалюється.

На наступних етапах розвитку концепції нульової довіри очікується подальше зростання її значення і впровадження у різних секторах економіки. Очікується, що нові технології, такі як квантові обчислення і розширена реальність, також знайдуть своє місце в рамках нульової довіри, полегшуючи виявлення загроз і забезпечуючи ще вищий рівень безпеки.

Для успішного впровадження цієї концепції важливо буде продовжувати розвивати інноваційні підходи до кібербезпеки і забезпечити взаємодію між технологічними рішеннями, законодавчими і регуляторними ініціативами та бізнес-процесами організацій. Це дозволить створити гнучке і ефективне середовище для захисту від кіберзагроз і забезпечити сталість бізнес-операцій у динамічному цифровому світі.

Таким чином, концепція нульової довіри продовжує еволюціонувати і впроваджуватися як основний стандарт безпеки для організацій, що бажають залишатися попереду в конкурентній боротьбі і забезпечити надійний захист своїх інформаційних ресурсів.

1.3. Порівняння традиційних мережевих архітектур та мереж з нульовою довірою

Традиційні мережеві архітектури зазвичай базуються на моделі периметрального захисту, де основний акцент робиться на захисті кордонів мережі. Це може включати в себе застосування файерволів, інтранетів і екстранетів для контролю доступу. Однак такі підходи стають все менш ефективними в умовах зростаючої кількості розподілених робочих місць і змінюваної природи загроз.

У порівнянні з традиційними архітектурами, мережі з нульовою довірою пропонують більш гнучкий і безпечний підхід до кібербезпеки. Вони не покладаються на статичні периметри і вважають кожен запит на доступ як потенційну загрозу, яка повинна бути обгрунтованою і перевіреною. Це дозволяє знизити ризики витоку даних і зловживання привілегіями, оскільки навіть внутрішні користувачі мережі потребують авторизації для кожного окремого запиту [19, с.21].

Крім того, мережі з нульовою довірою активно використовують шифрування даних, багатофакторну аутентифікацію і мікросегментацію для підвищення рівня безпеки. Ці технології дозволяють створювати мережеві інфраструктури, які максимально захищені від сучасних кіберзагроз і забезпечують стабільну роботу бізнес-процесів у динамічному середовищі.

Таблиця 1.3. – Традиційні мережеві архітектури та мережі з нульовою довірою

Номер	Особливість	Традиційні мережеві архітектури	Мережі з нульовою довірою
1.3.1	Підхід до довіри	Довіра за замовчуванням до користувачів у внутрішній мережі	Не довіряти жодному користувачеві чи пристрою за замовчуванням
1.3.2	Автентифікація	Одноразова автентифікація, VPN, захищені мережі	Багатофакторна автентифікація (MFA), постійна перевірка доступу
1.3.3	Авторизація та доступ до ресурсів	Ідентифікація в межах мережі, різні рівні доступу	Принцип "мінімальних привілеїв", динамічне управління доступом
1.3.4	Сегментація мережі	Плоский дизайн мережі, обмежені застосування VLAN	Сегментація на основі ідентифікації та потреб користувача
1.3.5	Моніторинг та виявлення аномалій	Відсутність адекватного моніторингу або обмежений	Постійний моніторинг, аналітика

			поведінки, швидке реагування
1.3.6	Адаптація до змін у середовищі	Важкість зміни політик та доступу	Динамічні політики, що адаптуються до змін в середовищі

Таблицю розроблено на основі джерела [3].

На наступному етапі порівняння можна висвітлити, що традиційні мережеві архітектури часто мають обмежену можливість виявлення аномальних активностей і реагування на них через централізовані точки контролю. У той час як мережі з нульовою довірою акцентують увагу на неперервному моніторингу, аналізі великих обсягів даних і застосуванні штучного інтелекту для виявлення змін у поведінці користувачів і підозрілих активностей.

Також важливо зазначити, що мережі з нульовою довірою сприяють підвищенню відповідності з регуляторними вимогами, оскільки вони дозволяють ефективно контролювати доступ до конфіденційної інформації і забезпечувати аудит інцидентів безпеки. Це є критичним аспектом для багатьох організацій, що операційно діють в регульованих секторах [20, с.41].

Крім того, важливим аспектом є здатність мереж з нульовою довірою підтримувати безпеку при зростаючій мобільності та використанні різних типів пристроїв. Це включає в себе здатність ефективно управляти доступом до даних і ресурсів навіть з використанням зовнішніх мереж і переносних пристроїв, забезпечуючи безпеку де б то не було здійснювалася робота.

Таким чином, мережі з нульовою довірою не лише забезпечують високий рівень кібербезпеки, але й підтримують оперативність бізнес-процесів і відповідь на виклики сучасного цифрового середовища. Це робить їх привабливим вибором для підприємств, що прагнуть забезпечити безпеку своїх даних і інформаційних активів в умовах постійно змінюючихся загроз і технологій.

Усе більше компаній вибирають перехід до мереж з нульовою довірою через їхню здатність адаптуватися до нових викликів у сфері кібербезпеки і забезпечувати більш високий рівень захисту інформаційних активів.

Отже, розділ 1 "Теоретичні основи мереж з нульовою довірою" надає глибоке розуміння концепції нульової довіри в інформаційних системах. Основним принципом є відмова від перевірення довіри до будь-якого вузла чи користувача на початковому етапі взаємодії. Це підходить для сучасних вимог до безпеки, де традиційні мережі не можуть ефективно захищати від сучасних загроз.

Основні складові мереж з нульовою довірою включають сильне шифрування даних, аутентифікацію і авторизацію на кожному етапі доступу, а також строге управління доступом. Ці елементи спільно сприяють створенню безпечної інформаційної інфраструктури, що мінімізує ризики компрометації даних і систем.

Важливим аспектом є також інтеграція технологій нульової довіри з існуючими інформаційними системами. Це вимагає ретельного аналізу і адаптації існуючих процесів і структур до нових вимог безпеки. Застосування цих технологій може забезпечити високий рівень захищеності, але вимагає комплексного підходу до впровадження і підтримки в експлуатації.

Таким чином, розділ 1 надає теоретичну основу для розуміння концепції і практичного застосування мереж з нульовою довірою. Він акцентує увагу на інноваційних підходах до забезпечення безпеки інформаційних систем у сучасному цифровому середовищі, що стає все більш важливим у контексті зростаючих кіберзагроз і вимог до захисту конфіденційності та доступності даних.

РОЗРОБКА МЕТОДИКИ ВИКОРИСТАННЯ МЕРЕЖ З НУЛЬОВОЮ ДОВІРОЮ

2.1. Аналіз поточного стану безпеки мережі

Розглянемо процес впровадження архітектури Zero Trust у середній компанії з 500 співробітниками.

Для початку використовуємо Nessus для сканування вразливостей. Завантажуємо та встановлюємо Nessus Professional з офіційного сайту Tenable на виділений сервер у мережі компанії, налаштовуємо ліцензію та оновлюємо базу вразливостей. Плануємо сканування, визначаючи діапазони IP-адрес для сканування, створюємо розклад для мінімізації впливу на продуктивність мережі. Налаштовуємо та запускаємо сканування, створюючи різні профілі для серверів, робочих станцій та мережевого обладнання. Аналізуємо результати, зосереджуючись на критичних та високоризикових вразливостях, створюємо список пріоритетних вразливостей для усунення та аналізуємо тенденції.

Для аналізу поточних методів аутентифікації використовуємо Splunk. Встановлюємо Splunk Enterprise на виділений сервер, налаштовуємо форвардери Splunk на ключових системах для збору логів. Налаштовуємо збір логів аутентифікації з різних джерел (Active Directory, VPN, ключові програми) та створюємо спеціальні індекси для даних аутентифікації. Розробляємо запити для аналізу успішних та невдалих спроб аутентифікації, створюємо дашборди для візуалізації паттернів аутентифікації. Аналізуємо, які методи аутентифікації використовуються, частоту використання різних методів, виявляємо аномалії (наприклад, багаторазові невдалі спроби). Ідентифікуємо системи, які використовують слабкі методи аутентифікації, виявляємо користувачів з підвищеними привілеями без багатофакторної аутентифікації, аналізуємо час життя сесій. На основі аналізу створюємо список рекомендацій щодо покращення методів аутентифікації та пропонуємо впровадження додаткових заходів безпеки.

2.2. Ідентифікація активів та класифікація даних

Для ідентифікації активів у мережі використовуємо CMDB (Configuration Management Database). Вибираємо відповідну CMDB систему, наприклад, ServiceNow або BMC Helix CMDB, встановлюємо та налаштовуємо її на виділеному сервері. Імпортуємо дані з існуючих інвентаризаційних систем, якщо такі є, та проводимо автоматичне сканування мережі для виявлення активів за допомогою інструментів виявлення. Інтегруємо CMDB з системами моніторингу мережі для автоматичного виявлення нових пристроїв, налаштовуємо агенти на кінцевих пристроях для регулярного оновлення інформації. Створюємо схему класифікації активів, призначаємо кожному активу відповідну категорію та критичність. Документуємо взаємозв'язки між активами, визначаємо та документуємо залежності між активами, створюємо візуальні карти взаємозв'язків для кращого розуміння інфраструктури. Встановлюємо процедури регулярного аудиту CMDB для забезпечення актуальності даних, навчаємо персонал щодо важливості підтримки актуальності CMDB.

Для класифікації даних за рівнем важливості використовуємо Symantec DLP (Data Loss Prevention). Починаємо з розгортання Symantec DLP Enforce Platform на виділеному сервері, а також розгортання компонентів Network Prevent та Network Discover. Встановлюємо Endpoint Agents на робочих станціях та серверах.

Наступним кроком є налаштування політик класифікації даних: визначаємо категорії даних (конфіденційні, внутрішні, публічні) та створюємо правила для автоматичної класифікації даних на основі ключових слів, регулярних виразів та інших критеріїв. Налаштовуємо Network Discover для сканування файлових серверів, баз даних та інших сховищ даних, встановлюючи розклад регулярних сканувань для виявлення та класифікації нових даних.

Моніторинг передачі даних реалізуємо через налаштування Network Prevent для виявлення передачі конфіденційних даних у мережевому трафіку, встановлюючи правила блокування або сповіщення про несанкціоновану передачу важливих даних. Аналіз кінцевих точок здійснюється за допомогою Endpoint Agents, що моніторять та класифікують дані на робочих станціях. Встановлюємо політики для запобігання копіювання конфіденційних даних на зовнішні носії.

Створюємо регулярні звіти про розподіл даних за категоріями важливості, аналізуючи тенденції та паттерни у розміщенні та використанні конфіденційних даних. Інтегруємо Symantec DLP з SIEM системою для централізованого моніторингу інцидентів та налаштовуємо взаємодію з системами контролю доступу для автоматичного обмеження доступу до конфіденційних даних.

Для підвищення обізнаності співробітників проводимо тренінги щодо правил роботи з конфіденційними даними та впроваджуємо систему сповіщень для інформування користувачів про потенційні порушення політик безпеки.

Завдяки використанню CMDB та Symantec DLP, ми отримуємо повну картину всіх активів у мережі та чітке розуміння розміщення та важливості даних.

2.3. Впровадження засобів багатофакторної аутентифікації (MFA)

Для впровадження багаторазової аутентифікації (MFA) використовуємо Duo Security. Перш за все, проводимо аудит існуючих систем аутентифікації та визначаємо, які з них потребують інтеграції з MFA. Розробляємо план розгортання, включаючи графік впровадження для різних груп користувачів, і створюємо політику використання MFA, яка визначає обов'язковість його застосування для всіх співробітників.

Наступним кроком є налаштування Duo Security. Створюємо обліковий запис адміністратора в Duo Security, налаштовуємо основні параметри безпеки, включаючи політики блокування та дозволені методи аутентифікації.

Для розгортання Duo для користувачів створюємо облікові записи для всіх співробітників, надсилаємо запрошення для активації їхніх облікових записів Duo та проводимо навчання щодо встановлення та використання Duo Mobile app на їхніх смартфонах.

Активуємо різні методи другого фактору аутентифікації, такі як push-повідомлення, SMS, голосові виклики та апаратні токени. Налаштовуємо політики, які визначають, які методи аутентифікації дозволені для різних груп користувачів або типів доступу. Проводимо пілотне тестування з невеликою групою користувачів для виявлення можливих проблем та поетапно впроваджуємо MFA для різних відділів компанії, починаючи з IT-відділу та керівництва.

Моніторимо успішні та невдалі спроби аутентифікації через Duo, аналізуємо логи для виявлення аномалій або потенційних загроз безпеці. Регулярно переглядаємо та оптимізуємо політики MFA на основі отриманих даних та відгуків користувачів.

Для забезпечення безперебійної роботи інтегруємо Duo з Active Directory. Проводимо аудит структури Active Directory, перевіряємо актуальність даних користувачів, створюємо окрему організаційну одиницю (OU) в AD для керування користувачами Duo. Встановлюємо Duo Authentication Proxy на виділений сервер в мережі компанії та налаштовуємо Proxy для взаємодії з Active Directory та Duo Security cloud.

Створюємо додаток "Active Directory Sync" в панелі керування Duo, налаштовуємо параметри синхронізації, включаючи фільтри для користувачів та груп, встановлюємо захищене з'єднання між Duo Authentication Proxy та Active Directory. Активуємо Duo Single Sign-On (SSO) для безшовної інтеграції з корпоративними додатками, налаштовуємо SAML або інші протоколи SSO для інтеграції з ключовими бізнес-системами.

Автоматизуємо процеси створення та деактивації облікових записів Duo при змінах в Active Directory, налаштовуємо правила автоматичного оновлення груп користувачів в Duo на основі змін в AD. Проводимо

комплексне тестування процесу аутентифікації через AD з використанням Duo MFA, перевіряємо коректність роботи SSO для різних корпоративних додатків.

Налаштовуємо регулярні звіти про стан синхронізації між AD та Duo, встановлюємо сповіщення про критичні події, такі як невдалі спроби синхронізації або аномалії в аутентифікації. Розробляємо та документуємо процедури відновлення доступу у випадку проблем з Duo або втрати пристрою користувачем, навчаємо службу підтримки процедурам швидкого вирішення проблем з MFA.

2.4. Використання мікросегментації для мінімізації доступу

Для мікросегментації мережі будемо використуовувати VMware NSX. Мікросегментація за допомогою VMware NSX включає кілька ключових етапів. Спочатку проводимо аудит існуючої віртуальної інфраструктури, оновлюємо VMware vSphere до сумісної версії та забезпечуємо достатню кількість ресурсів для розгортання компонентів NSX. Далі розгортаємо NSX Manager як віртуальну машину в середовищі vSphere, встановлюємо NSX Controller кластер для централізованого управління та інсталюємо NSX Edge Services Gateway для мережевих сервісів на кордоні сегментів. Після цього налаштовуємо логічні комутатори для кожного сегмента мережі, налаштовуємо VXLAN для тунелювання трафіку між фізичними хостами. Аналізуємо бізнес-процеси та потоки даних для визначення оптимальної структури сегментів, створюємо віртуальні сегменти для різних груп серверів, додатків та робочих станцій. Поетапно мігруємо віртуальні машини в відповідні логічні сегменти та перевіряємо коректність роботи додатків після міграції.

Налаштування політик доступу включає кілька ключових етапів. Спочатку проводимо детальний аналіз, які робочі станції та користувачі потребують доступу до критичних серверів, та документуємо вимоги до доступу для кожного бізнес-процесу. Далі використовуємо NSX для створення

груп безпеки, що об'єднують віртуальні машини за функціональністю або рівнем доступу, включаючи критичні сервери та відповідні робочі станції до цих груп.

Розробляємо політики безпеки, створюючи набір правил фаєрволу в NSX Distributed Firewall для контролю трафіку між сегментами, налаштовуємо політики, що дозволяють доступ до критичних серверів лише з визначених робочих станцій, та встановлюємо правила за принципом "заборонено все, що явно не дозволено". Використовуємо функцію Application Rule Manager в NSX для аналізу трафіку та автоматичного створення рекомендованих правил, налаштовуємо правила на рівні додатків для більш точного контролю доступу.

Перед впровадженням у продуктивну мережу проводимо тестування політик в лабораторному середовищі та використовуємо режим моніторингу для виявлення потенційних проблем перед активацією блокування. Політики впроваджуємо поетапно, починаючи з некритичних систем, моніторимо вплив нових політик на продуктивність мережі та додатків.

Налаштовуємо детальне логування всіх спроб доступу, особливо до критичних серверів, інтегруємо логи NSX з SIEM-системою для централізованого аналізу безпеки. Використовуємо NSX API для автоматизації створення та оновлення політик безпеки, інтегруємо NSX з системами управління конфігураціями для автоматичного застосування політик до нових віртуальних машин. Регулярно переглядаємо та оновлюємо політики безпеки, проводимо періодичні тести на проникнення для перевірки ефективності мікросегментації.

Впровадження мікросегментації за допомогою VMware NSX є ключовим елементом стратегії Zero Trust, що дозволяє створити гранульований контроль доступу на рівні окремих віртуальних машин та додатків, значно зменшуючи поверхню атаки та обмежуючи можливості зловмисників у разі компрометації окремого сегмента мережі.

2.5. Вибір інструментів та технологій для реалізації Zero Trust

Для забезпечення захищеного доступу будемо використовувати Cisco AnyConnect. Спочатку налаштовуємо інфраструктуру, встановлюючи Cisco ASA (Adaptive Security Appliance) або Firepower Threat Defense (FTD) як основний шлюз VPN, та забезпечуємо відмовостійкість і балансування навантаження для безперервного доступу.

Після цього розгортаємо Cisco AnyConnect Secure Mobility Client на робочі станції та мобільні пристрої співробітників, налаштовуємо профілі підключення для різних груп користувачів з відповідними рівнями доступу. Інтегруємо AnyConnect з Active Directory та Duo Security для забезпечення багатофакторної аутентифікації.

Далі створюємо політики доступу на основі ролей користувачів та їх місцезнаходження, налаштовуємо перевірку стану пристрою перед наданням доступу (наявність антивірусу, актуальність оновлень). Для моніторингу та аудиту налаштовуємо детальне логування всіх VPN-сесій та інтегруємо логи AnyConnect з системою SIEM для централізованого аналізу.

Для обмеження та контролю мережевого трафіку будемо використовувати Palo Alto. Спочатку розгортаємо фізичні або віртуальні пристрої Palo Alto Next-Generation Firewall в ключових точках мережі, налаштовуємо відмовостійку конфігурацію для забезпечення безперервної роботи.

Далі використовуємо віртуальні системи (vsys) Palo Alto для створення логічних сегментів мережі, налаштовуємо політики міжзонального доступу відповідно до принципів Zero Trust. Активуємо App-ID для ідентифікації та контролю додатків незалежно від порту та протоколу, створюємо політики, які дозволяють використання лише необхідних бізнес-додатків.

Інтегруємо Palo Alto з Active Directory для ідентифікації користувачів, створюємо політики доступу на основі особистості користувача та групової приналежності. Активуємо та налаштовуємо модулі IPS, антивірус, анти-

спайвер та URL-фільтрацію, створюємо власні сигнатури для виявлення специфічних для компанії загроз.

Налаштовуємо вибіркову SSL-декрипцію для інспекції зашифрованого трафіку, визначаємо категорії сайтів та додатків, які потребують детальної перевірки. Налаштовуємо автоматичні дії у відповідь на виявлені загрози (блокування IP, карантин користувача) та інтегруємо Palo Alto з іншими системами безпеки для координованого реагування.

Використання Splunk для моніторингу та аналізу безпекових інцидентів включає кілька ключових етапів. Спочатку встановлюємо Splunk Enterprise на виділені сервери з урахуванням масштабованості та налаштовуємо Splunk Enterprise Security (ES) для розширених можливостей аналізу безпеки. Потім встановлюємо Splunk Universal Forwarder на всі ключові системи та пристрої, налаштовуємо збір логів з Cisco AnyConnect, Palo Alto, серверів, робочих станцій та інших критичних систем.

Далі розробляємо набір кореляційних правил для виявлення складних атак та аномальної поведінки, налаштовуємо тригери для автоматичного сповіщення про критичні інциденти. Активуємо модуль UEBA в Splunk ES для виявлення аномальної поведінки користувачів та систем, налаштовуємо базові профілі нормальної поведінки для різних груп користувачів.

Розробляємо набір дашбордів для візуалізації ключових метрик безпеки та налаштовуємо автоматичну генерацію регулярних звітів для керівництва та аудиторів. Інтегруємо Splunk з SIEM, системами управління вразливостями та іншими інструментами безпеки, створюємо єдину консоль для моніторингу всіх аспектів безпеки.

Впроваджуємо Splunk Phantom для автоматизації реакцій на інциденти, створюємо плейбуки для автоматичного реагування на типові загрози. Проводимо тренінги для команди безпеки з ефективного використання Splunk для аналізу інцидентів, розробляємо процедури ескалації та реагування на різні типи загроз.

Регулярно переглядаємо та оновлюємо правила кореляції та тригери на основі нових загроз, проводимо періодичні симуляції атак для перевірки ефективності системи моніторингу. Використання цього набору інструментів - Cisco AnyConnect, Palo Alto та Splunk - створює потужну екосистему для реалізації принципів Zero Trust. Cisco AnyConnect забезпечує безпечний віддалений доступ з суворою аутентифікацією, Palo Alto надає глибокий контроль та видимість мережевого трафіку, а Splunk забезпечує комплексний моніторинг та аналіз безпекових подій. Разом ці інструменти дозволяють реалізувати ключові аспекти Zero Trust: перевірку кожного запиту на доступ, мінімізацію привілеїв та постійний моніторинг активності для виявлення аномалій та загроз.

2.6. Постійний моніторинг та аналіз трафіку

Для постійного моніторингу трафіку будемо використовувати Splunk. Використання Splunk для постійного моніторингу трафіку та аналізу даних включає кілька ключових етапів. Спочатку впроваджуємо додаткові аплікації Splunk, такі як Splunk App for Infrastructure та Splunk IT Service Intelligence, щоб розширити функціональність. Налаштовуємо Splunk Stream для захоплення та аналізу мережевого трафіку в режимі реального часу.

Далі розробляємо комплексні моделі даних, що об'єднують інформацію з різних джерел для створення цілісної картини стану мережі та безпеки. Налаштовуємо прискорені звіти для швидкого доступу до критичної інформації.

Використовуємо Splunk Machine Learning Toolkit для виявлення складних патернів та прогнозування потенційних загроз, створюємо моделі для виявлення аномалій у мережевому трафіку та поведінці користувачів.

Налаштовуємо систему багаторівневих сповіщень для різних типів інцидентів та автоматичну ескалацію критичних подій до відповідних фахівців або команд реагування.

Інтегруємо Splunk з іншими системами безпеки, налаштовуємо двосторонню інтеграцію для автоматизованого обміну даними та координації дій.

Для виявлення вторгнень та реагування на них будемо використовувати Snort. Спочатку встановлюємо Snort на стратегічних точках мережі, включаючи периметр та ключові внутрішні сегменти, налаштовуємо його для роботи в режимі IPS (Intrusion Prevention System) для активного блокування загроз.

Далі імпортуємо та адаптуємо стандартні набори правил Snort, створюємо власні правила для виявлення специфічних для нашої мережі загроз та аномалій. Налаштовуємо пересилання логів Snort до Splunk для централізованого аналізу, створюємо спеціальні дашборди в Splunk для візуалізації даних Snort та швидкого реагування на виявлені загрози.

Налаштовуємо автоматичні дії у відповідь на виявлені загрози, такі як блокування IP-адрес або ізоляція скомпрометованих систем, інтегруємо Snort з системами управління мережевим доступом для динамічної зміни прав доступу при виявленні загроз.

Регулярно аналізуємо продуктивність Snort та оптимізуємо налаштування для зменшення кількості хибнопозитивних спрацювань, впроваджуємо систему балансування навантаження для Snort сенсорів у високонавантажених сегментах мережі.

Для аналізу поведінки користувачів та виявлення аномалій будемо використовувати Exabeam. Спочатку встановлюємо Exabeam Advanced Analytics для глибокого аналізу поведінки користувачів та сутностей, налаштовуємо Exabeam Data Lake для ефективного зберігання та обробки великих обсягів даних.

Далі налаштовуємо збір даних з різних джерел, включаючи Active Directory, VPN-логи, логи доступу до додатків та систем. Інтегруємо Exabeam з Splunk та іншими системами безпеки для обміну даними та збагачення аналізу.

Використовуємо можливості машинного навчання Exabeam для створення базових профілів нормальної поведінки користувачів та систем, налаштовуємо параметри для визначення аномальної поведінки в контексті нашої організації. Створюємо правила для виявлення специфічних для нашої організації загроз та сценаріїв атак, налаштовуємо виявлення складних атак, таких як lateral movement та privilege escalation.

Активуємо модулі UEBA в Exabeam для глибокого аналізу поведінки користувачів та сутностей, налаштовуємо скоринг ризиків для користувачів та сутностей на основі їхньої поведінки. Інтегруємо Exabeam з системами реагування на інциденти для автоматизації процесів розслідування та усунення загроз, створюємо автоматизовані робочі процеси для типових сценаріїв інцидентів.

Розробляємо набір дашбордів для візуалізації ключових метрик безпеки та аномалій поведінки, налаштовуємо регулярні звіти для керівництва та команди безпеки. Регулярно аналізуємо ефективність виявлення аномалій та налаштовуємо параметри системи для зменшення кількості хибнопозитивних спрацювань, проводимо періодичні тренінги для команди безпеки з ефективного використання Exabeam для аналізу поведінкових аномалій.

Використання цього комплексу інструментів - Splunk, Snort та Exabeam - створює потужну систему моніторингу та аналізу, яка є ключовим елементом архітектури Zero Trust. Splunk забезпечує централізований збір та аналіз даних, Snort надає можливості виявлення та запобігання вторгненням, а Exabeam фокусується на аналізі поведінки користувачів та виявленні аномалій.

Така комбінація дозволяє реалізувати принцип постійного моніторингу та верифікації, який є основою Zero Trust. Ми отримуємо можливість виявляти та реагувати на загрози в режимі реального часу, аналізувати складні сценарії атак та виявляти аномальну поведінку, яка може свідчити про компрометацію облікових записів або систем. Впровадження та ефективне використання цих інструментів вимагає постійного навчання персоналу, регулярного перегляду

та оновлення правил та політик, а також адаптації до нових типів загроз, що забезпечить постійне вдосконалення системи безпеки та її відповідність принципам Zero Trust.

2.7. Висновок

У цьому розділі було розглянуто та детально описано методику використання мереж з нульовою довірою, яка включає комплекс заходів і технологій для забезпечення високого рівня безпеки в організації. Основні аспекти впровадження архітектури Zero Trust в компанії з 500 співробітниками були досліджені та реалізовані за допомогою передових інструментів та технологій, таких як Nessus, Splunk, CMDB, Symantec DLP, Duo Security, VMware NSX, Cisco AnyConnect, Palo Alto, Snort та Exabeam.

Аналіз поточного стану безпеки мережі дозволив виявити критичні та високоризикові вразливості, розробити рекомендації щодо їх усунення та покращити методи аутентифікації. Ідентифікація активів та класифікація даних за допомогою CMDB та Symantec DLP забезпечили повну видимість мережевих активів та контроль за конфіденційною інформацією.

Впровадження багатофакторної аутентифікації (MFA) за допомогою Duo Security значно підвищило рівень захисту облікових записів користувачів, забезпечуючи додатковий рівень безпеки. Мікросегментація мережі за допомогою VMware NSX дозволила створити гранульований контроль доступу та мінімізувати поверхню атаки.

Використання Cisco AnyConnect та Palo Alto для захищеного доступу та контролю мережевого трафіку забезпечило надійний та безперервний захист мережевих ресурсів. Моніторинг та аналіз безпекових інцидентів за допомогою Splunk, Snort та Exabeam створили потужну систему виявлення та реагування на загрози в реальному часі.

Завдяки впровадженню архітектури Zero Trust, організація отримала можливість здійснювати постійний моніторинг активності, верифікацію кожного запиту на доступ та мінімізацію привілеїв, що значно підвищило

рівень безпеки та захисту даних. Постійне вдосконалення методів та інструментів безпеки забезпечить адаптацію до нових загроз та підтримку високого рівня захисту інформаційної інфраструктури.

ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

3.1. Розрахунок капітальних витрат

3.1.1. Визначення трудомісткості розробки політики безпеки інформації.

Трудомісткість визначається тривалістю кожної робочої операції, починаючи зі складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки)

$$t = t_{\text{тз}} + t_{\text{в}} + t_{\text{а}} + t_{\text{вз}} + t_{\text{озб}} + t_{\text{овр}} + t_{\text{д}}, \text{годин} \quad (3.1)$$

де $t_{\text{тз}}$ – тривалість складання технічного завдання,

$t_{\text{в}}$ – тривалість розробки концепції,

$t_{\text{а}}$ – тривалість процесу аналізу ризиків,

$t_{\text{вз}}$ – тривалість визначення вимог до заходів, методів та засобів захисту,

$t_{\text{озб}}$ – тривалість вибору основних рішень,

$t_{\text{овр}}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування,

$t_{\text{д}}$ – тривалість документального оформлення.

Визначено, що відповідно до етапів проектування, тривалість операцій складає наступні величини: $t_{\text{тз}}$ = 20 годин, $t_{\text{в}}$ = 32 години, $t_{\text{а}}$ = 16 годин, $t_{\text{вз}}$ = 15 годин, $t_{\text{озб}}$ = 12 годин, $t_{\text{овр}}$ = 14 годин, $t_{\text{д}}$ = 6 годин.

$$t = 20 + 32 + 16 + 15 + 12 + 14 + 6 = 115 \text{ годин}$$

3.1.2. Розрахунок витрат на розробку методики використання мереж з нульовою довірою

Витрати на розробку $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки $З_{мч}$:

$$К_{рп} = З_{зп} + З_{мч} = 21562{,}5 + 1275{,}12 = 22837{,}5 \text{ грн} \quad (3.2)$$

$$З_{зп} = t * З_{іб} = 115 * 187{,}5 = 21562{,}5 \text{ грн} \quad (3.3)$$

де t – загальна тривалість проектування в годинах,

$З_{іб}$ – середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

$$З_{мч} = t * C_{мч} = 115 * 11{,}088 = 1275{,}12 \text{ грн} \quad (3.4)$$

де $C_{мч}$ – вартість 1 години машинного часу ПК, грн/година.

$$C_{мч} = P * t_{нал} * C_e + \frac{Ф_{зал} * Н_а}{F_p} + \frac{К_{лпз} * Н_{апз}}{F_p} \quad (3.5)$$

де Р – встановлена потужність ПК,

C_e – тариф на електричну енергію,

$Ф_{зал}$ – залишкова вартість ПК на поточний рік,

$Н_а$ – річна норма амортизації на ПК,

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення,

$К_{лпз}$ – вартість ліцензійного програмного забезпечення,

F_p – річний фонд робочого часу (за 40-годинного робочого тижня F_p = 1920).

$$C_{мч} = 0{,}7 * 3 * 4{,}32 + \frac{40 * 0{,}8}{1920} + \frac{5499 * 0{,}7}{1920} = 9{,}072 + 0{,}016 + 2 = 11{,}088 \text{ грн/год}$$

Ціну повної роботи можна знайти таким чином:

$$K = K_{\text{рп}} + K_{\text{зпз}} + K_{\text{пз}} + K_{\text{аз}} + K_{\text{навч}} + K_{\text{н}} \quad (3.6)$$

$$K = 22837{,}5 + 5499 + 72000 + 46000 + 45000 + 10000 = 201336{,}5 \text{ грн}$$

де $K_{\text{рп}}$ – витрати на розробку методики,

$K_{\text{зпз}}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення,

$K_{\text{пз}}$ – вартість створення основного й додаткового програмного забезпечення,

$K_{\text{аз}}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів,

$K_{\text{навч}}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$K_{\text{н}}$ – витрати на встановлення обладнання та налагодження системи.

3.2. Розрахунок поточних витрат

Річні поточні витрати складають:

$$C = C_{\text{н}} + C_{\text{єв}} + C_{\text{з}} + C_{\text{ел}} + C_{\text{тос}} \quad (3.7)$$

де $C_{\text{н}}$ – витрати на навчання адміністративного персоналу ($C_{\text{н}}$ = 30000, 3 тренінги на рік, кожен 10000 грн.),

$C_{\text{єв}}$ – ЄСВ,

$C_{\text{з}}$ – річний фонд заробітної плати фахівцям, які будуть її обслуговувати,

$C_{\text{ел}}$ – вартість електроенергії,

$C_{\text{тос}}$ – витрати на технічне й організаційне адміністрування та сервіс.

Річний фонд заробітної плати фахівцям, які будуть її обслуговувати складає:

$$С_з = З_{осн} + З_{дод} \quad (3.8)$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата в розмірі від 8% до 10% від основної заробітної плати.

Основна заробітна плата спеціаліста задіяного для складає 30000 грн з урахуванням додаткової заробітної плати в 10%. Для обслуговування вистачить одного спеціаліста, отже:

$$С_з = 450 * 160 * 12 = 360000 \text{ грн}$$

Ставка ЄСВ складає 22%:

$$С_{єв} = 360000 * 0.22 = 79200 \text{ грн}$$

Вартість електроенергії, що споживається апаратурою протягом року ($С_{ел}$):

$$С_{ел} = P * F_p * Ц_е \quad (3.9)$$

де Р – встановлена потужність апаратури (1кВт),

F_p – Річний фонд робочого часу системи (8760 годин),

$Ц_е$ – тариф на електроенергію (4,32 грн/кВт),

Отже вартість електроенергії становить:

$$С_{ел} = 1 * 8760 * 4,32 = 37843,2 \text{ грн}$$

Витрати на технічне й організаційне адміністрування визначаються у відсотках від вартості капітальних витрат – 1% ($С_{тос}$ =201336,5 *0,01 = 2013,36 грн).

Загалом річні витрати визначаються:

$$С = 30000 + 79200 + 360000 + 37843,2 + 1121,36 = 509056,56 \text{ грн}$$

3.3 Розрахунок потенційних збитків

Для розрахунку потенціальних збитків можна використати спрощену модель оцінки. Необхідні вхідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла чи сегмента корпоративної мережі;

$З_о$ – заробітна плата обслуговуючого персоналу;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі;

$Ч_о$ – чисельність обслуговуючого персоналу;

$Ч_с$ – чисельність співробітників атакованого вузла чи сегмента корпоративної мережі;

О – обсяг продажів атакованого вузла чи сегмента корпоративної мережі;

I – число атакованих вузлів чи сегментів мережі;

N – середнє число атак на рік.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_{п} + П_{в} + V \quad (3.10)$$

де $П_{п}$ – оплачувані витрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі,

$П_{п}$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі,

V – втрати від зниження обсягів продажу.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки:

$$П_{п} = \frac{\sum З_{с}}{F} * t_{п} \quad (3.11)$$

де F – місячний фонд робочого часу (при 40-ка годинному робочому тижні становить 176 годин).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі становлять:

$$П_{в} = П_{ви} + П_{пв} \quad (3.12)$$

де $П_{ви}$ – витрати на повторне введення інформації,

$П_{пв}$ – витрати на відновлення вузла або сегменту корпоративної мережі.

Витрати на повторне введення інформації розраховується за формулою:

$$П_{ви} = \frac{\sum З_{с}}{F} * t_{ви} \quad (3.13)$$

Витрати на відновлення вузла або сегмента корпоративної мережі визначаються за формулою:

$$П_{пв} = \frac{\sum З_о}{F} * t_в \quad (3.14)$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегменту мережі виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегменту корпоративної мережі:

$$V = \frac{O}{F_г} * (t_в + t_п + t_{ви}) \quad (3.15)$$

де $F_г$ – річний фонд часу роботи організації (52 тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 годин.

Таким чином збитки від атаки на вузол або сегмент корпоративної мережі складе:

$$В = \sum_i \sum_n U \quad (3.16)$$

Для організації зі штабом 100 працівників, 3 з яких є обслуговуючим персоналом, відносно формул 3.14, 3.13, 3.12, витрати будуть складати:

$$П_{ви} = \frac{1455000}{176} * 3 = 24801 \text{ грн}$$

$$П_{пв} = \frac{86400}{176} * 3 = 1473 \text{ грн}$$

$$П_в = 24801 + 1473 = 26274 \text{ грн}$$

Втрати від зниження очікуваного обсягу за час простою вираховується за формулою 3.15 і буде дорівнювати:

$$V = \frac{43200000}{2080} * (3 + 3 + 3) = 186923 \text{ грн}$$

А упущена вигода за формулою 3.10:

$$U = 186923 + 26274 = 213197 \text{ грн}$$

Таким чином, при 14 атаках на рік, збитки для організації лише внаслідок простою складатимуть:

$$\text{В} = 14 * 213197 = 2984758 \text{ грн}$$

Загальний ефект від слідування рекомендаціям щодо впровадження методів протидії фішингу визначається з урахуванням ризиків порушення інформаційної безпеки, і становить:

$$E = B * R - C \quad (3.17)$$

$$E = 2984758 * 0{,}5 - 509056{,}56 = 983322{,}44 \text{ грн}$$

3.4. Визначення та аналіз показників економічної ефективності запропонованих рекомендацій

Для проведення оцінки економічної ефективності запропонованих рекомендацій, необхідно визначити наступні показники:

- Коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає ROSI

- Термін окупності капітальних інвестицій T_o

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на

впровадження системи інформаційної безпеки. Для його обчислення необхідно скористатися формулою:

$$ROSI = \frac{E}{K}, \text{частки одиниці} \quad (3.18)$$

де Е – загальний ефект від слідування рекомендаціям, тис.грн.,
К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис.грн.

$$ROSI = \frac{983,3}{201,3} = 4,88$$

Термін окупності капітальних інвестицій показує за скільки років окупаються капітальні інвестиції за рахунок отриманого ефекту від впровадження рекомендованих методів, та обчислюється за формулою:

$$\mathrm{T_o} = \frac{\mathrm{K}}{\mathrm{E}} \quad (3.19)$$

$$\mathrm{T_o} = \frac{201,3}{983,3} = 0,20 \text{ років} = 2,5 \text{ місяці}$$

3.5. Висновки

Під час виконання економічного розділу було розраховано капітальні витрати на впровадження. Були розраховані витрати на персонал, обладнання, програмне забезпечення, витрати на експертів для проектування систем захисту.

Окрім капітальних витрат, були розраховані витрати на підтримування функціональності систем захисту та обладнання, підготовку персоналу для роботи з цими системами, та періодичне навчання.

Були розглянуті потенційні збитки у разі вдалої атаки.

За отриманими даними було розраховано ефект від впровадження ефективних методів захисту, окрім цього було визначено коефіцієнт повернення інвестицій ROSI та термін окупності впровадження Zero Trust.

Враховуючи всі розрахунки можна сказати, що є доцільним використання Zero Trust, так як коефіцієнт повернення інвестицій дорівнює майже 5 одиницям за одиницю капітальних витрат, окупність наступить лише за 2,5 місяці, що є швидко порівняно с тим, які потенційні втрати може понести компанія.

ВИСНОВКИ

Засновуючись на проведеному аналізі у дипломній роботі, можна зробити наступні висновки. У першому розділі, що присвячений теоретичним основам мереж з нульовою довірою, було визначено, що концепція нульової довіри базується на принципі "Довіряй, але перевіряй", де кожен запит на доступ до ресурсів мережі перевіряється та автентифікується перед наданням доступу. Це підходить для захисту від внутрішніх і зовнішніх загроз, знижуючи ризики компрометації даних і систем.

Щодо історії та еволюції концепції нульової довіри, виявлено, що вона почала активно розвиватися у зв'язку з розширенням хмарних технологій та потреби в безпеці віртуалізованих середовищ. Порівняння з традиційними мережевими архітектурами показало, що нульова довіра пропонує більш гнучкий та масштабований підхід до захисту, ніж традиційні підходи, які зазвичай базуються на периметральній обороні.

У другому розділі, де проведено аналіз розвитку мереж з нульовою довірою, було виявлено, що сучасні рішення та технології нульової довіри включають в себе різноманітні інструменти для аутентифікації, авторизації та контролю доступу. Їх використання показує значні переваги у банківській сфері, медичних установах та інших галузях, де зберігання конфіденційної інформації є критично важливим.

Переваги нульової довіри полягають у зменшенні ризику втрати даних із-за некоректного управління доступом, але вони також мають свої недоліки, зокрема, висока складність впровадження та підтримки, потреба у великій кількості спеціалістів і високі витрати на обслуговування інфраструктури.

У третьому розділі, що стосується розробки методики використання мереж з нульовою довірою, було визначено основні етапи впровадження, включаючи аналіз потреб користувачів, проектування і розгортання інфраструктури, та постійне моніторинг і апгрейд системи для забезпечення

безпеки. Інструменти і технології для реалізації нульової довіри включають аутентифікаційні пристрої, системи управління доступом і шифрування даних.

Рекомендації щодо оптимального використання нульової довіри в мережах включають врахування особливостей індивідуальних бізнес-потреб, надійність і комплексність впровадження, а також постійну підтримку і навчання персоналу. Такий підхід може забезпечити високий рівень захисту інформації та підвищити ефективність бізнес-процесів організації в умовах сучасних кіберзагроз.

Аналізуючи розвиток та розробку методики використання мереж з нульовою довірою, можна зазначити, що такий підхід виявляє значний потенціал у сфері інформаційної безпеки. Він спрямований на зменшення ризиків компрометації даних та систем завдяки відсутності довіри до будь-якого внутрішнього або зовнішнього з'єднання. Методика нульової довіри дозволяє підвищити ефективність захисту, зокрема через зосередження на аутентифікації та авторизації на рівні користувачів і пристроїв.

Додатково, впровадження такої методики спрощує управління ключами та сертифікатами, що відповідно знижує витрати на управління інфраструктурою безпеки. Велика перевага полягає також у збільшенні мобільності та гнучкості, оскільки користувачі можуть безпечно отримувати доступ до ресурсів з будь-якого місця і на будь-якому пристрої. Цей підхід підтримує модернізацію інфраструктури та сприяє більшому використанню хмарних та гібридних рішень без втрати безпеки.

Отже, можна висновувати, що методика використання мереж з нульовою довірою є перспективною в сучасних умовах, де зростає значення кібербезпеки та потреба у надійних заходах захисту інформації. її впровадження може сприяти забезпеченню високого рівня безпеки, мінімізації ризиків та збільшенню ефективності в управлінні інформаційними ресурсами організацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gartner визначає три фактори, що впливають на зростання витрат на безпеку. [Електронний ресурс]. URL: https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartneridentifies-three-factors-influencing-growth-i.

2. Міграція хмари з використанням методу підйому та переміщення. [Електронний ресурс]. URL: https://www.teradata.com/Trends/Cloud/Lift-andShift-Migration1.

3. Парадигма розподілу Spoke-Hub. [Електронний ресурс]. URL: https://hmn.wiki/ru/Hub_and_spoke.

4. Matrix таблиця мікро-сегментації та макро-сегментації. URL: https://networkinterview.com/micro-segmentation-vs-network-segmentation/

5. Що ZTX означає для постачальників послуг та користувачів. [Електронний ресурс]. URL: https://go.forrester.com/blogs/what-ztx-means-forvendors-and-users/

6. Безпека хмари. [Електронний ресурс]. URL: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

7. Антивірусна програма. Вікіпедіа. Вільна енциклопедія. [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D1%96%D1%80%D1%83%D1%81%D0%BD%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0

8. Geneve: Загальна віртуалізація інкапсуляції мережі. [Електронний ресурс]. URL: https://tools.ietf.org/html/rfc8926

9. TLV vs Bit Fields. [Електронний ресурс]. URL: https://tools.ietf.org/html/draft-ietf-nvo3-encap-05#section-6.6

10. Khalil I, Khreishah A, Azeem M (2014) Cloud computing security: a survey. Computers 3(1):1–35 73

11. Singh S, Jeong Y-S, Park JH (2016) A survey on cloud computing security: issues, threats, and solutions. J Netw Comput Appl 75:200–222

12. Khalil IM, Khreishah A, Azeem M (2014) Cloud computing security: a survey. Computers 3(1):1–35

13. Ahmed M, Litchfield AT (2018) Taxonomy for identification of security issues in cloud computing environments. J Comput Inf Syst 58(1):79–88

14. Sumitra B, Pethuru C, Misbahuddin M (2014) A survey of cloud authentication attacks and solution approaches. Int J Innov Res Comput Commun Eng 2(10):6245–6253

15. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(1):1–11

16. A. Alshammari, S. Alhaidari, A. Alharbi and M. Zohdy, "Security Threats and Challenges in Cloud Computing," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017, pp. 46-51, doi: 10.1109/CSCloud.2017.59.

17. Pavan Muraidhara, "Security issues in cloud computing and its countermeasures", International Journal of Scientific & Engineering Research, vol. 4, no. 10, October 2013.

18. M. Zeller, R. Grossman, C. Lingenfelder, M. Berthold, E. Marcade, R. Pechter, et al., "Open standards and cloud computing: KDD-2009 panel report" in , Paris, France:KDD, pp. 11-18, 2009.

19. Tabrizchi, H., Kuchaki Rafsanjani, M. A survey on security challenges in cloud computing: issues, threats, and solutions. J Supercomput 76, 9493–9532 (2020). https://doi.org/10.1007/s11227-020-03213-1

20. Subramanian N, Jeyaraj A (2018) Recent security challenges in cloud computing. Comput Electr Eng 71:28–42

21. Mell P, Grance T (2018) SP 800-145, The NIST Definition of cloud computing CSRC (online) 74 Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-145/final. Accessed 11 Dec 2018

22. Ramachandra G, Iftikhar M, Khan FA (2017) A comprehensive survey on security in cloud computing. Proc Comput Sci 110:465–472

23. Kaur M, Singh H (2015) A review of cloud computing security issues. Int J Adv Eng Technol 8(3):397–403

24. Kumar PR, Raj PH, Jelciana P (2018) Exploring data security issues and solutions in cloud computing. Proc Comput Sci 125:691–697

25. Огляд моделей хмарних послуг / Н. А. Шевченко, М. В. Валігула, Т. О. Маєвський, Г. В. Шимчук // Матеріали міжнародної наукової конференції „Іван Пулюй: життя в ім'я науки та України“ (до 175-ліття від дня народження), 28-30 вересня 2020 року. — Т. : ФОП Паляниця В. А., 2020. — С. 109–110. — (Важливі аспекти практичного застосування здобутків сучасної науки і новітніх технологій).

26. ГОСТ 12.1.005-88. ССБТ. Загальні санітарно-гігієнічні вимоги до повітря робочої зони. [Електронний ресурс]. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=6264.

27. Kindervag, J., 2010. Build security into your network's DNA: The zero-trust network architecture. Forrester Research Inc, pp.1-26.

28. Haber, M.J., 2020. Zero trust. In Privileged Attack Vectors (pp. 295-304). Apress, Berkeley, CA.

29. Stafford, V.A., 2020. Zero Trust Architecture. NIST Special Publication, 800, p.207.

30. Gilman, E. and Barth, D., 2017. Zero Trust Networks. O'Reilly Media, Inc.

31. DeCusatis, C., Liengtiraphan, P., Sager, A. and Pinelli, M., 2016, November. Implementing zero trust cloud networks with transport access control and first packet authentication. In 2016 IEEE International Conference on Smart Cloud (SmartCloud) (pp. 5-10). IEEE.

32. Kerman, A., Borchert, O., Rose, S. and Tan, A., 2020. Implementing A Zero Trust Architecture. The MITRE Corporation, Tech. Rep.

Flanigan, J., 2018. Zero Trust Network Model.

33. Vanickis, R., Jacob, P., Dehghanzadeh, S. and Lee, B., 2018, June. Access control policy enforcement for zero-trust-networking. In 2018 29th Irish Signals and Systems Conference (ISSC) (pp. 1-6). IEEE.

34. Espadas, J., Molina, A., Jiménez, G., Molina, M., Ramírez, R. and Concha, D., 2013. A tenant-based resource allocation model for scaling Software-as-a-Service applications over cloud computing infrastructures. Future Generation Computer Systems, 29(1), pp.273-286.

35. Rasthofer, S., Arzt, S., Lovat, E. and Bodden, E., 2014, September. Droidforce: Enforcing complex, data-centric, system-wide policies in android. In 2014 Ninth International Conference on Availability, Reliability and Security (pp. 40-49). IEEE.

36. Cox, K. and Kneidinger, M., 2017. Protecting the crown jewels of the government through infrastructure resilience and the DHS Continuous Diagnostics and Mitigation programme. Cyber Security: A Peer-Reviewed Journal, 1(2), pp.147-155.

37. Perrichon, A., Liu, B.H., Chevalier, J., Gremillard, L., Reynard, B., Farizon, F., Liao, J.D. and Geringer, J., 2017. Ageing, shocks and wear mechanisms in ZTA and the long-term performance of hip joint materials. Materials, 10(6), p.569.

38. Bhatt, S., Manadhata, P.K. and Zomlot, L., 2014. The operational role of security information and event management systems. IEEE security & Privacy, 12(5), pp.35-41.

39. Trivellato, D., Zannone, N. and Etalle, S., 2014. GEM: A distributed goal evaluation algorithm for trust management. Theory and practice of logic programming, 14(3), pp.293-337.

40. Zaihrayeu, I., Da Silva, P.P. and McGuinness, D.L., 2005, May. IWTrust: Improving user trust in answers from the web. In International Conference on Trust Management (pp. 384-392). Springer, Berlin, Heidelberg.

41. Wu, Y., Qiao, Y., Ye, Y. and Lee, B., 2019, October. Towards Improved Trust in Threat Intelligence Sharing using Blockchain and Trusted Computing. In 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (pp. 474-481). IEEE.

42. Ahad, A., Tahir, M. and Yau, K.L.A., 2019. 5G-based smart healthcare network: architecture, taxonomy, challenges and future research directions. IEEE access, 7, pp.100747-100762.

43. Schroth, C., 2008. A Service-oriented Reference Architecture for Organizing Cross-Company Collaboration. In Enterprise Interoperability III (pp. 71-83). Springer, London.

ДОДАТКИ

Додаток А

Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Зміст	2	
3	А4	Вступ	3	
4	А4	Розділ 1	20	
5	А4	Розділ 2	13	
6	А4	Розділ 3	10	
7	А4	Висновки	2	
8	А4	Перелік посилань	5	
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	
13	А4	Додаток Ґ	1	
14	А4	Додаток Д	2	

Додаток Б

Таблиця. – Перспективи використання мереж з нульовою довірою

Перспективи використання мереж з нульовою довірою	Опис
Підвищення кібербезпеки	Зменшення ризику компрометації даних і систем.
Менша потреба в периметральних заходах захисту	Фокус на внутрішній безпеці, а не на обмеженні доступу ззовні.
Підвищення мобільності і гнучкості	Забезпечення безпечного доступу з будь-якого місця і пристрою.
Можливість впровадження більш розгалужених та змішаних інфраструктур	Використання комбінацій хмарних та локальних обчислювальних ресурсів без втрати безпеки.
Зменшення витрат на управління ключами і сертифікатами	Спрощення управління інфраструктурою безпеки.

Додаток В

Таблиця. – Аналіз розвитку та розробки методики використання мереж з нульовою довірою

Етап розвитку	Опис	Характеристика
1. Початковий етап	Вивчення теоретичних основ та концепцій з нульовою довірою.	Огляд літератури та наукових публікацій.
2. Розробка методики	Створення рамок інфраструктури та інструментів.	Розробка технічних специфікацій і планування реалізації.
3. Впровадження	Тестування та налагодження методики.	Пілотні проекти та апробація на реальних середовищах.
4. Оцінка ефективності	Аналіз результатів та коригування методики.	Оцінка впливу на безпеку і ефективність мережі.

Додаток Г

Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку _____ б.

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (прізвище, ініціали)

Додаток Г

Перелік документів на оптичному носії.

1. Презентація_Шаповалов.ppt
2. Кваліфікаційна робота_ Шаповалов.doc
3. Кваліфікаційна робота_ Шаповалов.pdf

Додаток Д

Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-20-3 Шаповалова Є.В. на тему: «Аналіз розвитку та розробка методики використання мереж з нульовою довірою»

Пояснювальна записка містить 89 сторінок, 9 таблиць, 6 додатків, 43 джерел.

Метою даної кваліфікаційної роботи є забезпечення безпеки інформаційних активів шляхом впровадження методики використання мереж з нульовою довірою.

У першому розділі кваліфікаційної роботи проведено аналіз теоретичних основ мереж з нульовою довірою, досліджено еволюцію цієї концепції, проаналізовані сучасні підходи до забезпечення кібербезпеки, а також сформульовані основні задачі даної кваліфікаційної роботи.

У спеціальній частині проведено аналіз розвитку мереж з нульовою довірою, розроблено методику їх використання, запропоновані організаційні та технічні заходи щодо впровадження принципів нульової довіри в мережеву інфраструктуру.

В економічному розділі визначені витрати на розробку і впровадження мережі з нульовою довірою та проведено аналіз її економічної ефективності.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні рівня кібербезпеки підприємств шляхом впровадження розробленої методики використання мереж з нульовою довірою.

Серед недоліків проєкту слід відзначити: незначні відхилення від стандартів при оформленні пояснювальної записки; недостатньо детально розглянуто питання інтеграції запропонованої методики з існуючими системами безпеки підприємств.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Шаповалов Є.В. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., ас. **Рибальченко Ю.П.**