ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ПОБУДОВА ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА З ЗАСТОСУВАННЯМ СИСТЕМ БЕЗДРОТОВОГО ЗВ'ЯЗКУ НА ОСНОВІ ОБЛАДНАННЯ CISCO SYSTEMS»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Мирослав СТЕЖКО*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач(ка) вищої освіти гр. КСДМ-62
Мирослав СТЕЖКО
Ім'я, ПРІЗВИЩЕ
Керівник: Людмила АСЄЄВА
доцент, к.філ.н. Ім'я, ПРІЗВИЩЕ
Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Інститут ННІІТ
Кафедра Комп'ютерної інженерії
Ступінь вищої освіти Магістр
Спеціальність 123 Комп'ютерна інженерія
Освітньо-професійна програма Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедри КІ
_____ Лащевська Н.О.
"___"_____ 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Стежку Мирославу Вадимовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: «Побудова локальної обчислювальної мережі підприємства з застосуванням систем бездротового зв'язку на основі обладнання Cisco Systems»

керівник кваліфікаційної роботи Асєєва Людмила, д.філ., доц.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від «15» жовтня 2024 року № 320.

2. Строк подання студентом кваліфікаційної роботи 20.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
корпоративна інформаційна система;
програмно-апаратний комплекс Cisco Systems;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми захисту периметру корпоративної системи.
2. Склад та умови функціонування корпоративної інформаційної системи.
3. Методи та засоби захисту периметру корпоративних систем.
4. Варіант топології корпоративної інформаційної системи із застосуванням бездротових рішень.

5. Перелік графічного матеріалу

1. Тема магістерської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Результати аналізу складу та умов функціонування корпоративної інформаційної системи.

4. Результати аналізу технологій для побудови локальних мереж

5. Результат аналізу обладнання Cisco Systems для побудови локально-обчислювальних мереж.

6. Варіант топології корпоративної інформаційної системи із застосуванням засобів бездротового зв’язку від Cisco Systems.

7. Результат аналізу технології Cisco TrustSec як елементу корпоративних локальних обчислювальних мереж.

8. Висновки за результатами роботи.

6. Дата видачі завдання 16.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми розробки корпоративних інформаційних систем.	01.09.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	21.09.2024 р.	
3.	Аналіз ринку мережевих рішень та дослідження портфоліо лідерів ринку.	14.10.2024 р.	
4.	Розроблення варіанту топології корпоративної інформаційної системи із застосуванням бездротових систем від Cisco	01.11.2024 р.	
5.	Розроблення варіанту покращення мережі за рахунок сегментації з використанням технології TrustSec.	15.11.2024 р.	
6.	Оформлення результатів дослідження.	06.12.2024 р.	
7.	Підготовка доповіді до захисту.	20.12.2024 р.	

Здобувач Мирослав СТЕЖКО
(підпис) прізвище та ініціали

Керівник кваліфікаційної роботи Людмила АСЄЄВА
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача СТЕЖКА Мирослава
на тему: «Побудова локальної обчислювальної мережі підприємства з застосуванням систем бездротового зв'язку на основі обладнання Cisco Systems»

Актуальність: Актуальність теми кваліфікаційного дослідження зумовлена тим, що розвиток людства тісно пов’язаний з розвитком різних систем комунікації. Розвиток електричного та електронного обладнання дав змогу розробити на підприємствах локальні мережі з власними мережевими ресурсами, декількома каналами зв’язку з мережею Інтернет та багатьма іншими сервісами.

У цьому дослідженні автор зосередився на*:* розробці адаптивної топології мережі на основі багаторівневої архітектури Cisco Systems; моделюванні сценаріїв сегментації мережі для підвищення інформаційної безпеки; аналізі та впровадженні Cisco Trust Sec як інноваційної технології сегментації; комплексному моделюванні та тестуванні мережевої інфраструктури в Cisco Packet Tracer. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. Запропоновано методику сегментації локальної мережі на основі логічного поділу користувачів та впровадження VLAN і технологій, таких як TrustSec, з метою мінімізації ризиків компрометації корпоративної інфраструктури.
2. Виконано імітаційне моделювання запропонованого варіанту мережевої топології у середовищі Cisco Packet Tracer для оцінки їхньої продуктивності та ефективності.
3. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. Є певні зауваження до рівня авторської рефлексії: в першому теоретичному розділі не завжди хід думки дослідника видається самостійним. Проте ці зауваження суттєво не впливають на якість дослідження.

Висновок: кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку «**відмінно»**, а здобувач **СТЕЖКО Мирослав** заслуговує присвоєння кваліфікації магістр з комп’ютерної інженерії за освітньо-професійною програмою комп’ютерні системи та мережі.

Рецензент:
науковий ступінь, вчене звання _____ *підпис* _____ *Ім’я, ПРІЗВИЩЕ*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач СТЕЖКО Мирослав до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 123 Комп'ютерна інженерія
(код, найменування спеціальності)

освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

на тему: «Побудова локальної обчислювальної мережі підприємства з застосуванням систем бездротового зв'язку на основі обладнання Cisco Systems».

Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ Катерина НЕСТЕРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ***Стежко М.В.*** обрав тему роботи, метою якої було розробити варіант топології захисту периметру корпоративних інформаційних систем та рекомендації щодо її реалізації. Під час виконання кваліфікаційної роботи **СТЕЖКО Мирослав** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача **СТЕЖКО Мирослав** на оцінку **«відмінно»** та присвоїти йому кваліфікацію магістр з комп'ютерної інженерії за освітньо-професійною програмою комп'ютерні системи та мережі.

Керівник кваліфікаційної роботи _____ Людмила АСЄЄВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **СТЕЖКО Мирослав** допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри Комп'ютерної інженерії _____ Наталія ЛАЩЕВСЬКА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина магістерської роботи: 69 сторінки, 24 рисунки, 25 джерел.

Об'єкт дослідження – процес побудови локально-обчислювальної мережі підприємства.

Предмет дослідження – технології та засоби побудови локально-обчислювальної мережі.

Мета роботи – розробка варіанту локально-обчислювальної мережі типового підприємства та пропозиція рішення для ефективної роботи мережі.

Методи дослідження – опрацювання необхідної тематичної літератури, аналіз документації, українських та міжнародних стандартів та їх порівняння, моделювання топології локально-обчислювальної мережі.

Локально-обчислювальні мережі є надзвичайно важливим елементом організацій, в яких циркулює важлива службова інформація, яка не має бути доступна неавторизованим користувачам. Вразливості інформаційної технології, яка реалізується в корпоративній інформаційній системі, визначають можливості порушення кібербезпеки даних систем.

В роботі проаналізовано проблему побудови корпоративної інформаційної системи та визначено варіанти захисту та покращення локальної мережі з урахуванням викликів часу. Проведено аналіз існуючих технологій побудови корпоративних мереж з акцентом на безпеку та бездротові рішення.

Досліджено методи та засоби побудови корпоративної інформаційної системи на прикладі обладнання Cisco Systems. Визначено призначення, основні функції та склад апаратних та програмних рішень Cisco.

На основі досліджень, що проведено в роботі, розроблено варіант топології корпоративної інформаційної системи з застосуванням апаратно-програмних рішень Cisco Systems. Розроблено рекомендації щодо застосування технології Cisco TrustSec для покращення захисту та актуальності мережі з мінімальними вкладеннями.

Галузь використання – адміністрування корпоративних інформаційних систем.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, БЕЗДРОТОВІ ЛОКАЛЬНІ МЕРЕЖІ, CISCO SYSTEMS, CISCO TRUSTSEC, МАРШРУТИЗАЦІЯ ЛОКАЛЬНИХ МЕРЕЖ, КОМУТАЦІЯ ЛОКАЛЬНИХ МЕРЕЖ.

ABSTRACT

Text part of the master's qualification work: 69 pages, 24 pictures, 25 sources.

The purpose of the work – the process of building a local computer network for an enterprise.

Object of research – technologies and resources of building a local area network.

Subject of research – development of a local area network variant for a typical enterprise and proposal of a solution for effective network operation.

Summary of the work – processing of the necessary thematic literature, analysis of documentation, Ukrainian and international standards and their comparison, modeling of the topology of the local computer network.

Local area networks are an extremely important element of organizations in which important official information circulates, which should not be accessible to unauthorized users. Vulnerabilities of information technology implemented in a corporate information system determine the possibilities of violating the cybersecurity of these systems.

The qualification work analyzes the problem of building a corporate information system and identifies options for protecting and improving the local network, taking into account the challenges of the time. An analysis of existing technologies for building corporate networks is carried out with an emphasis on security and wireless solutions.

Methods and means of building a corporate information system using Cisco Systems equipment as an example are investigated. The purpose, main functions, and composition of Cisco hardware and software solutions are determined.

Based on the research conducted in the work, a variant of the corporate information system topology using Cisco Systems hardware and software solutions has been developed. Recommendations have been developed for the use of Cisco TrustSec technology to improve network protection and relevance with minimal investment.

Field of use – administration of corporate information systems.

CORPORATE INFORMATION SYSTEM, WIRELESS LOCAL AREA NETWORKS, CISCO SYSTEMS, CISCO TRUSTSEC, LOCAL NETWORK ROUTING, LOCAL NETWORK SWITCHING.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВОЛЗ – волоконно-оптична лінія зв’язку

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

ЦОД – центр обробки даних

API – Application Programming Interface

DDoS – Distributed denial-of-service

DoS – Denial-of-service

ELA – Enterprise License Agreement

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

NaaS – Network as a service

NGFW – Next-Generation Firewall

QoS – Quality of Service

SD-WAN – Software-Defined Networking in a Wide Area Network

VPN – Virtual Private Network

WAF – Web Application Firewall

ВСТУП

Актуальність дослідження. Розвиток людства тісно пов’язаний з розвитком різних систем комунікації. Історично системи передачі даних пройшли шлях від багать та гінців до високошвидкісних високопродуктивних ВОЛЗ. Разом з тим ремісники пройшли шлях від невеликих майстерень до великих підприємств та корпорацій.

Однак проблема комунікації між працівниками, а також контроль керівництва за бізнес-процесами, стає все більш актуальною пропорційно масштабам підприємства.

Розвиток електричного та електронного обладнання дав змогу розробити на підприємствах локальні мережі, які було використано на початку як системи оповіщення, надалі як системи керування процесами, а на сьогодні це вже повноцінні локально-обчислювальні мережі з власними мережевими ресурсами, декількома каналами зв’язку з мережею Інтернет та багатьма іншими сервісами.

Подальша еволюція електронних пристроїв та поширення концепції BYOD (Bring Your Own Device – з англ. «Візьми свій пристрій») призвела до необхідності використання локально-обчислювальних мереж з системами бездротової передачі даних. Подібні системи дають змогу легко масштабувати мережу та мають відносно невисоку вартість розгортання та обслуговування, порівняно з класичними рішеннями дротових систем передачі.

Згідно з дослідженням Gartner компанія Cisco Systems є одним з лідерів серед виробників пристроїв дротової та бездротової інфраструктури LAN для підприємств. Досить висока оцінка стала можливою завдяки широкому асортименту пристроїв та поширенню продукції по всьому світу, а також інвестиційним вкладенням в розробку систем, що дозволяють поєднати лінійку кінцевого, серверного обладнання та обладнання для побудови хмарних мереж в одну систему з централізованим управлінням та моніторингом. З цієї причини основою для дослідження та розробки проекту стало обладнання саме даного вендора.

Підсумовуючи викладене, можна оцінити актуальність теми магістерської роботи, основним змістом якої є дослідження та розробка варіанту локальної обчислювальної мережі підприємства на основі обладнання та технологій Cisco Systems.

Об'єкт дослідження – процес побудови локально-обчислювальної мережі підприємства.

Предмет дослідження – технології та засоби побудови локально-обчислювальної мережі.

Мета роботи – розробка варіанту локально-обчислювальної мережі типового підприємства та пропозиція рішення для ефективної роботи мережі.

Наукові завдання:

1. Розробка адаптивної топології мережі на основі багаторівневої архітектури Cisco Systems. Вивчення й реалізація ефективного підходу до проектування локальної обчислювальної мережі підприємства середнього розміру, що враховує масштабованість, продуктивність, надійність, безпеку та управління в рамках інтеграції сучасного мережевого обладнання Cisco.

2. Моделювання сценаріїв сегментації мережі для підвищення інформаційної безпеки. Запропоновано методику сегментації локальної мережі на основі логічного поділу користувачів та впровадження VLAN і технологій, таких як TrustSec, з метою мінімізації ризиків компрометації корпоративної інфраструктури.

3. Аналіз та впровадження Cisco TrustSec як інноваційної технології сегментації. Дослідження застосування Cisco TrustSec для автоматизації мережевої сегментації, підвищення рівня безпеки та зручності управління політиками доступу в розподілених корпоративних мережах.

4. Комплексне моделювання та тестування мережевої інфраструктури в Cisco Packet Tracer. Виконано імітаційне моделювання запропонованих варіантів мережевих топологій у середовищі Cisco Packet Tracer для оцінки їхньої продуктивності та ефективності. Це дозволяє верифікувати запропоновані рішення до їх реального впровадження.

Методи дослідження – опрацювання необхідної тематичної літератури, аналіз документації, українських та міжнародних стандартів та їх порівняння, моделювання топології локально-обчислювальної мережі.

Практичне значення одержаних результатів полягає в розробці варіанту локально-обчислювальної мережі підприємства в загальному вигляді та пропозиція застосування технологічних рішень для впровадження та покращення безпеки локальних обчислювальних мереж.

Апробація: Результати дослідження були представлені на наступних конференціях, опубліковані в фахових виданнях та впроваджені на підприємстві.

Конференції:

- II всеукраїнська науково-технічна конференція «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу»;
- V науково-практична конференція «Проблеми комп’ютерної інженерії»;
- Сучасні досягнення компанії Hewlett Packard Enterprise в галузі іт та нові можливості їх вивчення і застосування;
- II міжнародна науково-практична конференція «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії».

Наукові публікації

«Дослідження проблематики сучасних бездротових мереж» / Стежко М.В., Лащевська Н.О. // Збірник II Всеукраїнської науково-технічної конференції «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу» – 2024.

«Розслідування кіберінцидентів в корпоративній інформаційній системі на основі рішень Autopsy та Volatility» / Гончаренко М.Ф., Стежко М.В. // Сучасний захист інформації №2(50) – 2022. – С. 22-29.

«Інтеграція бездротових локальних мереж підприємства та хмарних сервісів для оптимізації адміністрування інформаційної інфраструктури» / Вьюник Ю.О., Стежко М.В. // Науковий журнал «Вісник Херсонського національного технічного університету» №4 – 2024.

Акт впровадження: Результати дослідження були впровадженні на приватному підприємстві «Уніфільтр»

1 АНАЛІЗ ЗАВДАНЬ ПОБУДОВИ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ СИСТЕМИ ПІДПРИЄМСТВА

1.1. Аналіз складових частин локальної обчислювальної мережі підприємства

Розвиток інформаційного суспільства тісно пов’язаний з еволюцією інформаційних систем та систем передачі даних, підвищується інтенсивність збору, обробки та передачі великих обсягів даних.

Це є причиною змін в сторону автоматизації та комплексних підходів до обробки та обміну інформацією як в загальному потоці даних, так і відокремлюючи кожне підприємство, організацію та компанію окремо. Особливо актуальним рішенням є створення, планування, розробка та впровадження єдиного інформаційного простору окремо для кожної бізнес-одиниці з вище перерахованих для забезпечення якісного менеджменту, планування ризиків та зручної ефективної роботи працівників як на робочих місцях, так і віддалено. Особливу увагу слід приділити захисту корпоративних та персональних даних, забезпечення цілісності, актуальності та доступності інформації на загальнодоступних та корпоративних ресурсах, а також створити комфортний інтерфейс для роботи з необхідними застосунками в конкретних робочих задачах без фізичної прив’язки працівника до конкретного фізичного місця.

На сьогодні, плануючи майбутні виклики часу та тенденції розвитку хмарних сервісів, локальні обчислювальні мережі підприємств мають забезпечувати високу ефективність працівників як на місцях, так і віддалено, покращувати управління бізнесом та пришвидшити прийняття важливих управлінських рішень. Окремо слід виділити автоматизацію документообігу, підвищення швидкості та якості підготовки звітних документів, а також раціоналізацію бізнес-процесів та потоків інформації.

Інформаційна (автоматизована) система визначається як організаційно-технічна система, в якій реалізовано технологію обробки інформації з використанням технічних та програмних засобів [3].

Для підприємства інформаційними ресурсами є, власне, інформація та пов'язані з нею ресурси, такі як, наприклад, персонал, фонди, обладнання та інформаційні технології [2].

Термін «інформаційна технологія» (або IT) означає будь-яке обладнання або взаємопов'язану з ним систему чи підсистему, що використовується керуючим органом для збору, обробки, збереження, керування, управління, передачі або прийому даних чи інформації в автоматичному режимі. До обладнання, яке розуміють при описі даного терміну, відносять комп'ютери, допоміжне обладнання, ПЗ, вбудоване ПЗ та аналогічні рішення, послуги (включно зі службою підтримки) та пов'язані з ними ресурси [2].

Для більш повного розуміння корпоративної інформаційної системи розглянемо приклади інформаційних систем сучасних підприємств.

Першою для огляду візьмемо Enterprise Resource Planning (ERP). ERP – система планування ресурсів підприємства. ERP система – це пакет інтегрованих бізнес-додатків, інструменти якої мають спільну модель процесів та даних, які охоплюють широкі та глибокі операційні процеси при керуванні будь-яким типом проекту, виробничими операціями, постачанням, фінансовими транзакціями, персоналом та іншими активами. Додатки ERP автоматизують та підтримують більшість адміністративних та операційних процесів у бізнесів різних галузях, включно з напрямками бізнесу, клієнтські, адміністративні та аспекти управління активами підприємства. Характерною рисою ERP-систем є інтеграція баз даних усіх відділів компанії, а також синхронізація завдань та бізнес-процесів [4, 5].

Як приклад, використання однієї системи такого типу, є можливість відслідковування усього шляху замовлення, від першого контакту з клієнтом до підписання угоди, виконання необхідних робіт та подальше обслуговування. Окрім того ERP-система забезпечує прозорість усіх процесів та дозволяє одночасно виконувати декілька операцій, таких як ведення обліку та планування активів, відстеження фінансів підприємства та оцінка ефективності роботи [5].

Ринок ERP-систем пропонує сьогодні декілька варіантів системи, які між собою відрізняються лише інтерфейсом та функціональними можливостями. Архітектура таких систем, як і архітектура будь-яких інших комплексних систем, що створюються для певної задачі, дуже схожа. Так, стандартна ERP-система складається з двох основних блоків – платформи та модулів [5].

Платформа – це основа ERP-системи, яка складається з:

- ядра (або програмного середовища виконання операцій);
- базових функції (інструментарій користувача, різноманітні товарні, сервісні та клієнтські довідники);
- системи управління даними (включає інструментарій для роботи з даними та базами даних та самі бази даних).

Модулі ERP-системи – компоненти, які за необхідності можна підключити до платформи. Модулі виконують свої функціональні завдання окремо, однак використовуються інформацію з однієї бази даних. Тобто є можливість встановлення лише необхідних модулів. Процес впровадження дуже гладкий, рішення запускаються послідовно, завдяки чому вплив на діяльність компанії або підприємства мінімальний. Модулі можна також змінювати та видаляти. Архітектура такого роду є відмінною рисою ERP-систем [5].

Основними модулями ERP-систем є [5]:

- модуль управління виробництвом (дозволяє керувати виробничими процесами, операціями, витратами, виробничим потоком тощо);
- модуль управління фінансами (служить для керування розрахунками з сторонніми юридичними чи фізичними особами, обліку та планування фінансових операцій, ведення книги обліку, бухгалтерії тощо);
- модуль управління проектами (дозволяє здійснювати керування повного життєвого циклу певного проекту, включно з підрахунком витрат, моніторингом термінів, обробкою та створенням рахунків тощо);
- модуль управління людськими ресурсами (дозволяє проводити облік персоналу, розрахунок заробітної плати, фіксування часів роботи, управління мотиваційними моментами тощо);

- модуль управління відносинами з клієнтами (модуль даного типу використовують для збільшення кількісної складової збуту і якісної роботи з клієнтами як існуючими, так і потенційними).

Окрім основних модулів існують так звані модулі-конектори, які забезпечують зв'язок з додатками третьої сторони (з англ. Connection – зв'язок). Такі модулі необхідні для коректної роботи системи з застосуванням додатків, які відсутні в пакеті даної певної ERP-системи. Наприклад, такі модулі забезпечують інтеграцію телефонії будь-якого виду, обмін даними зі сторонніми програмами, програмними комплексами або сайтами тощо [5].

Також для прикладу розглянемо CRM-систему як варіант інформаційної системи підприємства.

Customer relationship management (або CRM) – це сучасний спосіб керування відносинами між компанією та клієнтами та оптимізації бізнес-процесів [6]. CRM допомагає організувати ефективну роботу з потенційними клієнтами, відстежувати дії постійних замовників та автоматизувати комунікації. Також системи такого роду дозволяють ефективно керувати замовленнями і спілкуватися з клієнтами в електронному форматі (e-mail та чат-боти соціальних мереж).

CRM-системи досить масштабовані і підходять для бізнесу та компаній різної величини та досить широкого спектру сфер підприємництва. Однак, незалежно від масштабу системи, CRM має низку загальних завдань:

- Консолідація даних: CRM повинна в автоматичному режимі збирати контакти постійних та потенційних клієнтів, їх приблизне місцерозташування, вподобання та низку інших даних, що дозволить здійснити маркетинговий аналіз та надасть можливість скорочення маркетингових процесів;
- Відстеження взаємодії: система надає можливість відстежувати комунікацію між представниками компанії та клієнтами заданими каналами зв'язку;
- Оцінка продуктивності: CRM має інструменти для створення детальної звітності щодо ефективності роботи компанії з клієнтами;
- Автоматизація: основна задача CRM-системи, яка полягає в автоматизації обліку, маркетингу та продажах.

CRM-системи, як продукт, досить поширень використовуються для найрізноманітніших бізнес-задач. Однак універсальна система такого роду є рідкістю. В більшості кожен розробник створює ПЗ, яке здатне виконувати одне завдання краще за інші. Відбувається фокусування на певному типі завдань, тому вибір CRM, налаштування та подальше обслуговування є досить важливим та трудомістким процесом.

В загальному CRM-системи умовно можна поділити на:

- Операційні: розроблені з фокусом на виконання повсякденних рутинних задач та завдань;
- Аналітичні: в основі мають об’ємні бази даних з інформацією про бізнес-процеси та клієнтів;
- Колективні: орієнтовані на підвищення ефективності взаємодії відділів та служб всередині однієї компанії.

Також варто відзначити, що функції CRM-системи можна розширити за допомогою додаткових модулів та взаємодії з супутніми застосунками, як, наприклад, можливість впровадити документообіг як частину системи.

Усі інформаційні системи, які описано вище і застосовуються на підприємствах, а також і інші, які не згадувалися як приклади, зазвичай розгортаються та функціонують за архітектурою «клієнт-сервер».

Як видно з назви, в основі архітектури є два основних компоненти – клієнт та сервер. Суть моделі полягає в тому, що клієнт відправляє запити серверу, який обробляє дану інформацію і надсилає в зворотному напрямку результат обробки або відповідь на запит. Сервер може обслуговувати кілька клієнтів одночасно за умови достатньої потужності. Якщо від декількох клієнтів приходять запити, які сервер з тієї чи іншої причини не встигає обробити, то він встановлює певну чергу очікування і виконує обчислення послідовно за кожним з запитів. Трапляється, що запити мають певні мітки пріоритету. Інформація з даною міткою буде оброблена поза чергою залежно від рівня пріоритету.

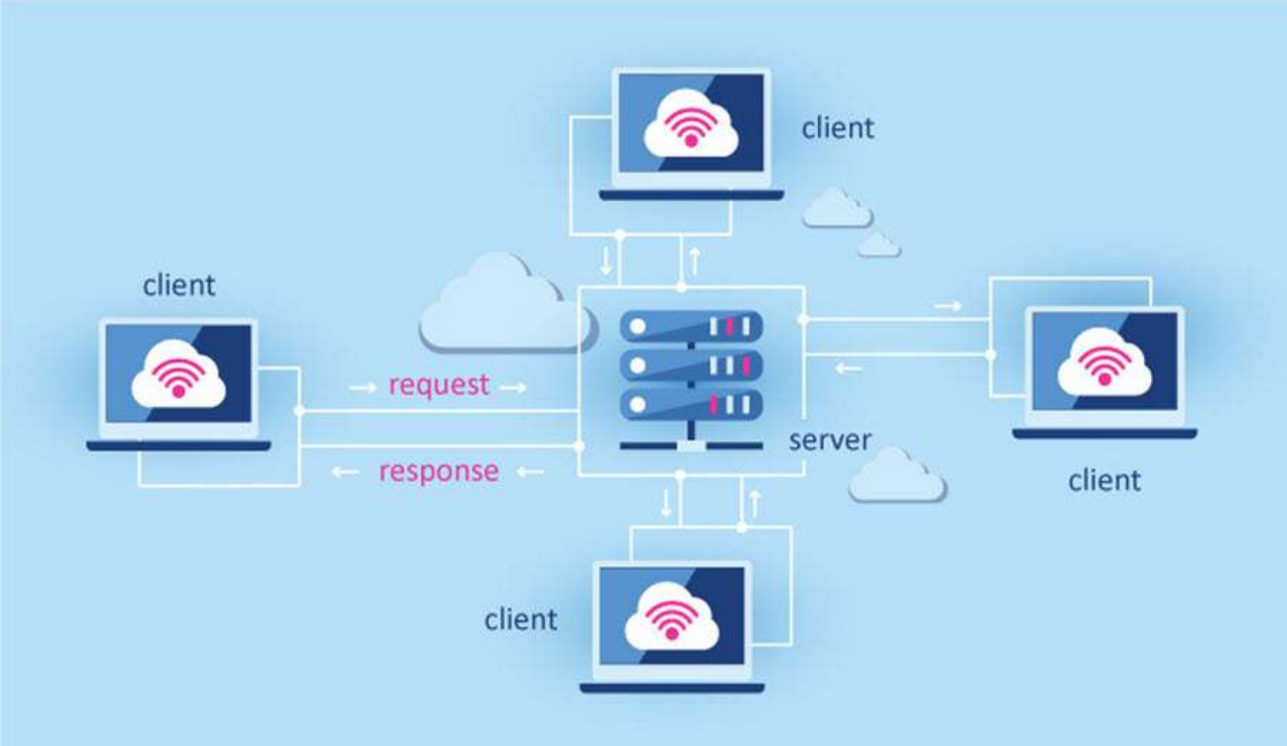

Рисунок 1.1 – Основні компоненти архітектури «клієнт-сервер» [7]

Серед основних функцій сервера виділяють [7]:

- Збереження, доступ, захист та резервне копіювання даних;
- Обробка запитів від клієнтів;
- Відправка відповіді клієнту.

Клієнт реалізує наступні функції [7]:

- Надання UI (User Interface, інтерфейсу користувача);
- Формування запиту та його відправка клієнту;
- Отримання відповіді на запит та формування додаткових команд (наприклад, додавання, оновлення або видалення даних).

Архітектура клієнт-сервер передбачає постійну взаємодію між пристроями, для якої необхідні певні правила. Такими правилами є протоколи взаємодії. Мережеві протоколи є певною сукупністю правил, за допомогою яких комп’ютери розуміють, як взаємодіяти один з одним в мережі.

Серед протоколів для взаємодії в межах підприємств найчастіше використовуються:

- MAC (Media Access Control): протокол ідентифікації мережевих пристроїв. Працює з фізичними адресами мережевих карт кожного пристрою, які

записуються виробником і не можуть бути змінені (випадки підміни MAC наразі до уваги не беруться);

- TCP/IP: стек протоколів для взаємодії пристроїв в мережі з маршрутизацією мережевого рівня (L3 моделі OSI);
- HTTP/HTTPS: протокол передачі гіпертексту. На основі нього працюють усі сайти в мережі. Служить для запиту даних у віддалених системах і відображенні їх на ПК, який дав запит на ці дані;
- FTP: протокол файлового обміну. Служить для передачі файлів на або з файлового сервера;
- SMTP, POP3, IMAP: протоколи для обміну електронними листами. Кожен з них має свої задачі та особливості, виконуючи при цьому спільну задачу.

Архітектура «клієнт-сервер» в першу чергу визначається розподілом обов'язками між сервером та клієнтом. Логічно можна виокремити три рівні операцій [8]:

- рівень представлення даних, який є інтерфейсом користувача. Він відповідає за представлення даних користувачеві та отримання від останнього керуючих команд;
- прикладний рівень, на якому проводяться обробка інформації та реалізація основної логіки програми;
- рівень керування даними, який забезпечує збереження даних та доступ до них.

З точки зору побудови для клієнт-серверної архітектури виділили два підтипи: дволанкова та триланкова. До останнього належать також багатоланкові структури мережі.

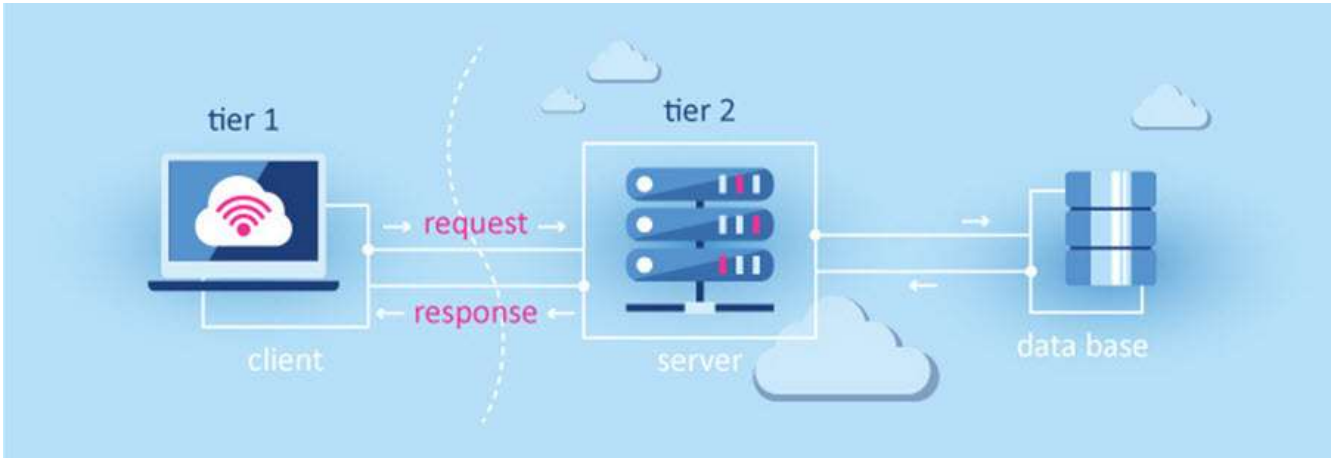

Рисунок 1.2 – Дворівнева архітектура [7]

Дворівневі архітектури передбачають взаємодію лише двох типів вузлів:

- сервера, який виконує роботу зі збереження даних, прийом, обробку запитів та надання на них відповіді, використовуючи при цьому лише власні ресурси;
- клієнта, який надає лише інтерфейс взаємодії, формує запити та отримує відповіді від сервера.

Для дворівневої архітектури також вирізняють два типи клієнтів. Вони відрізняються кількістю інформації, що обробляється сервером.

Перший тип – модель «слабкого» (або «тонкого») клієнта. При такій системі усі дані та логіка обробки даних відбувається на сервері. Клієнт тільки показує результат обробки даних. За приклад можна взяти будь-який поштовий клієнт (наприклад, Microsoft Outlook), де клієнтський застосунок лише відображає дані, що знаходяться на сервері, та взаємодіє з ними.

Другий тип клієнтів – «сильний» (або «товстий») клієнт. В даному випадку серверна частина передає клієнту для обробки інформацію, виступаючи більше як сховище даних, а клієнт проводить обробку та подання інформації. Прикладом виступає будь-який ігровий онлайн клієнт, де при встановленні на ПК копіюються усі дані гри, а в подальшому під час ігрової сесії клієнт здійснює обробку інформації щодо взаємодії ігрових ресурсів та, використовуючи попередньо завантажену інформацію, відображає поточний статус та дії як локального користувача, так і віддалених гравців.

Дворівнева архітектура має низьку вартість розгортання та проста в налаштуванні та обслуговуванні, що є її перевагою. Однак недоліком є те, що інформація завжди зберігається на сервері. Будь-яка технічна несправність сервера може призвести до часткової або повної втрати даних. Тому широкого поширення набула наступна, трирівнева архітектура.

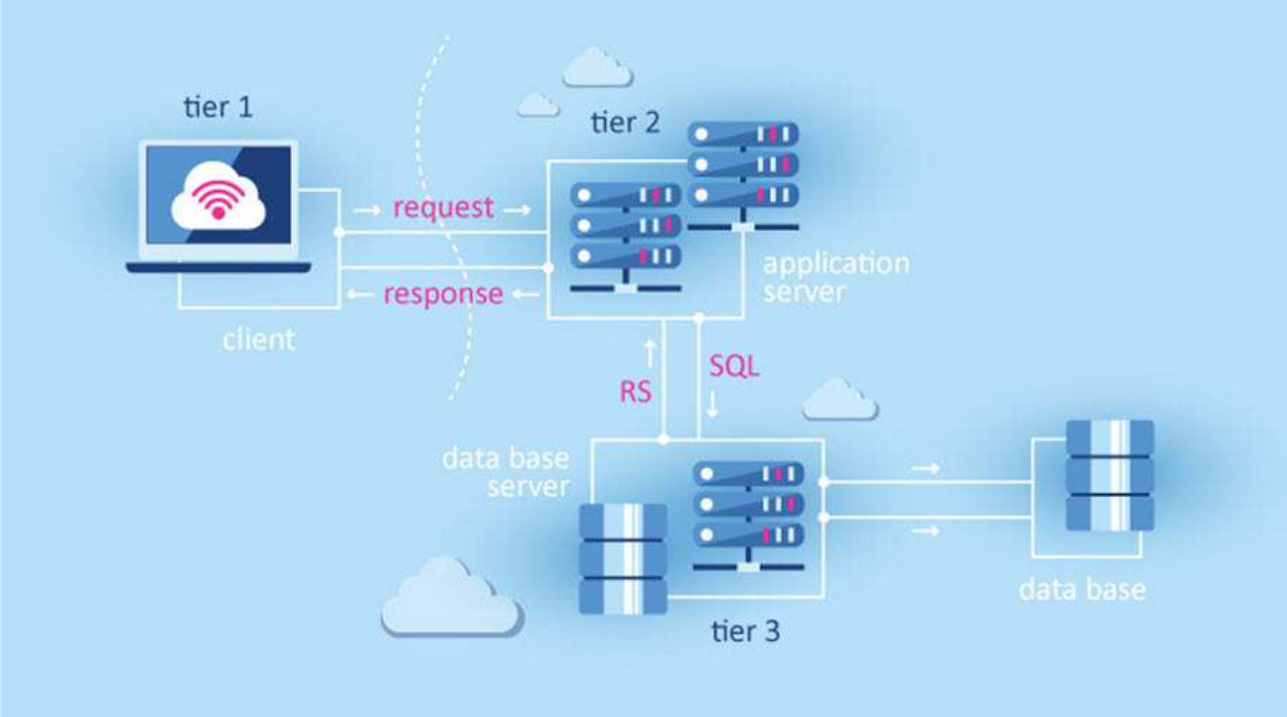

Рисунок 1.3 – Трирівнева архітектура [7]

Трирівнева архітектура, яка є подальшим розвитком, передбачає відділення прикладного рівня від управління даними. При даному розподілі представлення даних залишається на стороні клієнта, сервер виконує лише прикладну логіку обчислень та обробку алгоритмів, а за збереження даних відповідає сервер даних. Сервер даних зберігає інформацію і надає її на запит в необробленому вигляді.

Якщо порівняти два підтипи архітектури, то дворівнева архітектура простіша, оскільки всі запити виконуються на одному сервері, однак це також є недоліком, оскільки має нижчу надійність та для ефективної роботи вимоги до продуктивності сервера більш високі [8].

Трирівнева архітектура складніша, однак завдяки розподілу функцій між сервером та базою даних архітектура проявляє [8]:

- високий показник гнучкості та масштабованості;

- вищий рівень безпеки (оскільки захист визначається окремо для кожного сервісу, рівня або фізичного приладу);
- більшу продуктивність (завдяки розподілу задач між серверами).

Завдяки масштабованості трирівневу архітектуру можна перетворити у багаторівневу, встановивши додаткові сервери. Це дозволить оптимізувати навантаження на серверну одиницю, підвищить ефективність обчислень та підвищить стійкість до відмов всієї системи.

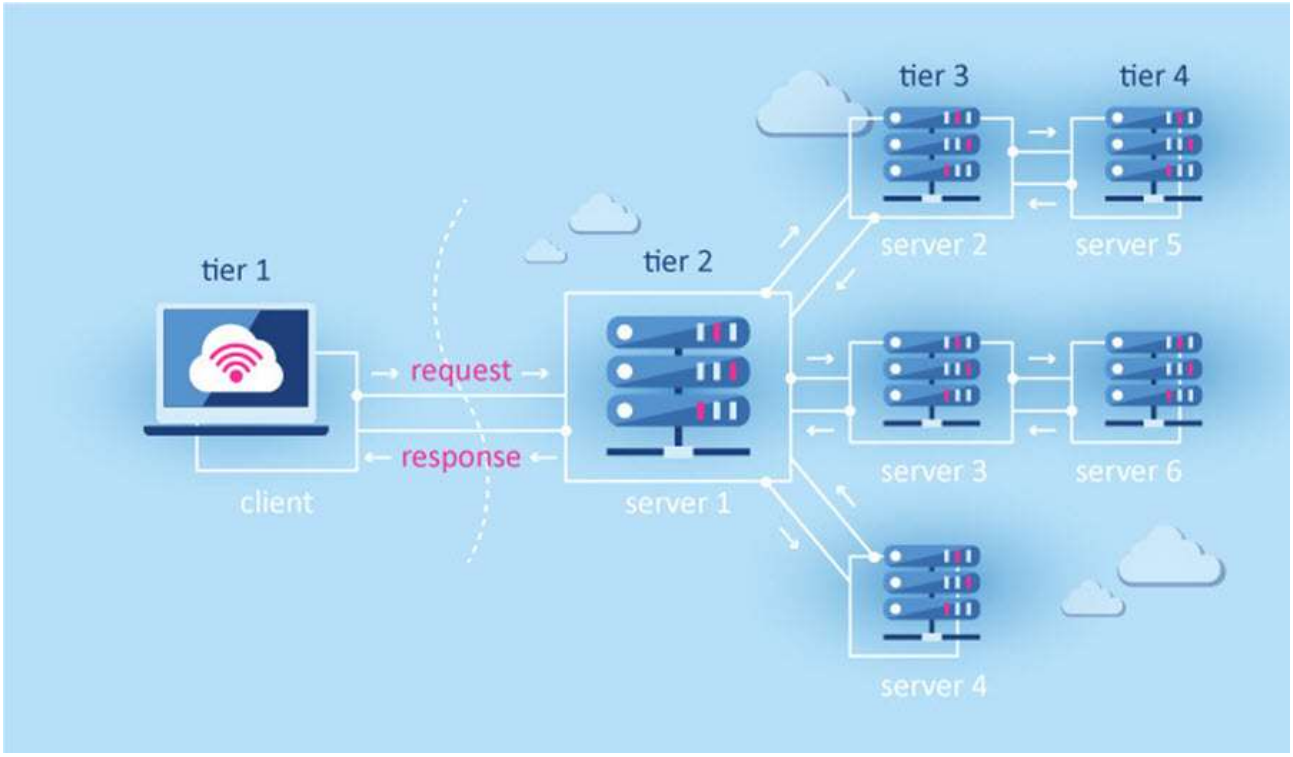

Рисунок 1.4. Багаторівнева архітектура [7]

Основна ідея архітектури «клієнт-сервер» полягає у розподілі функцій мережевого додатку на компоненти, кожен з яких реалізує свій специфічний набір сервісів. Компоненти можуть виконуватися на різних комп'ютерах, що реалізують клієнтські та/або серверні функції. Це робить можливим підвищення надійності, безпеки та продуктивності мережевих додатків та, відповідно, мережі в цілому.

Окремою важливою складовою мережі підприємства є IP-телефонія. Станом на сьогодні саме цей тип телефонного зв'язку має найбільшу кількість переваг для бізнесу, оскільки є доступним, багатофункціональним та якісним каналом зв'язку.

IP-телефонія – технологія передачі даних через Інтернет або локальні мережі від одного абонента до іншого [9]. Дані на стороні передачі стискаються у так звані пакети, а на стороні прийому з пакетів видобувається інформація та відтворюється

в розгорнутому вигляді. За подібну взаємодію відповідає спеціалізований сесійний протокол SIP (Session Initiation Protocol), задачею якого є побудова якісного зв’язку між двома точками у віртуальному просторі.

В цілому IP-телефонія є досить узагальненим поняттям, що об’єднує набір окремих протоколів та стандартів передачі даних. Для розуміння принципу роботи та розуміння того, на що треба буде звертати увагу під час проектування та обслуговування мережі підприємства, визначимо послідовність виклику за допомогою даної технології в деталях:

1. Під час набору номера протокол SIP визначає спосіб створення надійного каналу зв’язку та протоколи для обміну інформацією;

2. Після на IP-адресу АТС відправляється сигнал-запрошення для встановлення зв’язку;

3. Відбувається прийом запиту сервером;

4. Сервер визначає розташування абонента, який має прийняти виклик, його IP-адресу, шлях передачі даних та номер віртуального порта;

5. Разом з тим протокол SDP (Session Description Protocol) визначає параметри обміну даними між двома кінцевими точками сеансу зв’язку;

6. Спеціалізоване програмне забезпечення за допомогою кодеків конвертує аналоговий сигнал в цифровий та зашифровує дані для більшої безпеки та завадостійкості;

7. ISP (Internet Service Provider) передає пакети через АТС на телефон-отримувач (для мережі підприємства передача здійснюється локальними маршрутизаторами до АТС та від неї);

8. Кінцевий абонент приймає сигнал в декодованому вигляді, сеанс зв’язку встановлено, логічний канал передачі даних побудовано.

Процес встановлення сеансу зв’язку відбувається за долі секунди в реальному часі, протоколи зв’язку діють з вимогами QoS (Quality of Service), що означає високу якість зв’язку або ж мінімізацію втрат якості сигналу.

Викладене вище надає розуміння того, які системи мають працювати всередині корпоративної мережі, яке буде орієнтовне мережеве навантаження, розрахункова кількість користувачів, а також багато іншого. Також розуміння того,

які системи та застосунки мають працювати, визначає принципи побудови, виставляє вимоги до певних типів обладнання та ліній зв’язку.

Однак розвиток мережевих технологій, концепцій BYOD (Bring Your Own Device) та поширення пристрої IoT (Internet of Things) вносить певні корективи та нововведення в мережі підприємств класичного типу.

На сьогодні розвиток бездротових технологій та вищезгадані концепції розвитку персональних пристроїв надають можливість оптимізувати витрати на розробку та побудову мереж, забезпечити мобільність працівників, а також багато більш персоналізованих до потреб конкретного підприємства можливостей. Тому бездротовий зв’язок є найбільш оптимальним та ефективним рішенням для використання в мережах підприємств.

1.2. Аналіз технологій для побудови локальної мережі підприємства

Для розуміння, які технології можуть бути використані в мережах підприємств, визначимо суть самого поняття локальної мережі.

Локальна мережа (LAN, Local Area Network) – набір пристроїв, з’єднаних разом територіально в одному місці (офіс, цех, підприємство) [10]. Локальні мережі бувають різного масштабу, від квартири до офісної будівлі.

Склад локальної мережі може варіюватися, але постійними компонентами будуть кабелі, маршрутизатори, точки доступу та комутатори. За допомогою даного набору пристроїв користувачі можуть підключатися до внутрішніх та віддалених серверів, а також до інших мереж. Також з розвитком технологій набули поширення віртуальні локальні мережі, що дало змогу адміністраторам без змін фізичної інфраструктури групувати мережеві вузли і створювати підмережі, керуючи кожною з них окремо.

Серед переваг створення локальних мереж варто виділити збереження адресного простору, оскільки протокол IPv4, який досі широко розповсюджений, має скінченну кількість адрес, яка менше за число активних пристроїв. Саме тому кожна локальна мережа має універсальний виділений пул IP-адрес для роботи всередині мережі, а завдяки протоколу NAT відбувається взаємодія пристроїв

однієї мережі з зовнішніми методом підміни IP-адреси. Також перевагою є полегшення адміністрування за рахунок сегментування мережі.

Серед локальних мереж розрізняють дротові та бездротові різновиди побудови. Дротові мережі більш стабільні, швидші та безпечніші, однак більш вартісні за рахунок витрат на кабельну інфраструктуру та меншу мобільність. Бездротові мережі використовують радіоканал для з'єднання користувацьких пристроїв з маршрутизатором. Серед переваг можна виділити мобільність користувачів та низьку вартість утримання інфраструктури. Недоліками ж є фізичні процеси, властиві радіохвилям (інтерференція сигналів, залежність сигнал-шум та втрата потужності через перешкоди), а також залежність пропускної здатності від кількості користувачів.

Для дротових мереж характерна робота по технології Ethernet. Ethernet – технологія, яка використовується для підключення пристроїв в кабельних мережах [11]. Вона використовує свій протокол, який описує взаємодію пристроїв, порядок форматування та передачі інформації.

Технологія дозволяє забезпечити баланс між вартістю, швидкістю та простотою розгортання. Технологія описується стандартом IEEE 802.3, де вказано правила налаштування мережі, процедуру взаємодії елементів мережі Ethernet та ін.

Звичайно Ethernet має пропускну здатність 10Мб/с. З часом розвиток технологій та збільшення кількості інформації було розроблено стандарт IEEE 802.3u або Fast Ethernet. Даний стандарт збільшив швидкість передачі в кабельних мережах до 100Мб/с з мінімальними змінами компонентів інфраструктури. В першу чергу стандарт забезпечує більш надійне і точне виявлення та виправлення помилок, а також забезпечує більшу пропускну здатність, що підвищило швидкість завантаження сторінок та має кращі властивості для користування застосунками реального часу.

Існує декілька типів Fast Ethernet. 100BASE-TX використовується з кабелем UTP cat.5 і є найбільш популярним рішенням за рахунок сумісності зі стандартом 10BASE-T Ethernet. 100BASE-FX є стандартом для поєднання пристроїв оптоволоконним кабелем, що забезпечує більшу відстань передачі (табл. 1.1). 100BASE-T4 використовує два додаткові дроти до кабелів UTP cat.3.

Надалі стандарт Fast Ethernet було модернізовано до стандарту Gigabit Ethernet IEEE 802.3z. Модернізація дозволила передавати дані на швидкості до 1Гб/с. Даний стандарт передбачає роботу всіх чотирьох пар жил кабелю. Даний стандарт підходить для систем, для яких рекомендована мінімальна затримка передачі сигналу (системи відеозв'язку та з'єднання маршрутизаторів). Для розширення дальності підключення можна використовувати оптоволоконні кабелі багатомодових систем стандарту 1000BASE-SX або одномодових систем 1000BASE-LX. Найбільш важливою відмінністю стандартів є збільшення пропускної здатності та підтримка повнодуплексного режиму на рівні MAC.

Останньою модернізацією стандарту є 10 Gigabit Ethernet (або IEEE 802.3ae). Стандартом передбачено підвищення пропускної здатності до рівня 10Гб/с. Даної пропускної здатності стало можливим досягнути за умови широкого використання оптоволоконних кабелів. Однак обмежено використовуються мідні кабелі UTP Cat.6a та Cat.7.

Усі стандарти Ethernet. разом з граничними швидкостями та максимальною дальністю ефективної передачі сигналу, подано в таблиці 1.1.

	IEEE Standard	Швидкість	Тип протоколу	Максимальна відстань
Ethernet	802.3	10 Mbps	10Base-T	100 meters
Fast Ethernet/ 100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 meters 275/550 meters 550/5000 meters
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW	300 meters 300m MMF/ 10km SMF 10km/40km 300m/10km/40km

Таблиця 1.1 – Стандарти Ethernet [11]

Бездротові локальні мережі, в більшості своїй, працюють по технології Wi-Fi. Дана технологія розроблена консорціумом «Wi-Fi Alliance» на базі стандарту IEEE 802.11.

Побудова мереж на базі бездротових технологій є більш економним варіантом, надає певну мобільність користувачів, однак вимагає своїх правил побудови та налаштувань безпеки.

Прототипом даного зв’язку є технологія WaveLAN, яку було застосовано для оптимізації роботи систем супермаркетів. На час впровадження дана система мала змогу передавати дані на швидкості 2Мб/с.

В подальшому відбулася стандартизація та створення робочої групи, що в подальшому призвело до розробки нових специфікацій і стандартизації. Завдяки роботі групи відбувся розвиток нової технології, обладнання різних виробників почало нормально взаємодіяти одне з одним, а швидкість першого стандарту, що був розробленим, була 11Мб/с. Пропускна здатність постійно збільшується, підвищується рівень безпеки та можливості підключення. Нинішній перелік стандартів приведено в табл. 1.2.

Назва покоління	Стандарт IEEE	Прийнятий	Максимальна швидкість з'єднання (Мбіт/с)	Смуги радіочастот (ГГц)
Wi-Fi 8	802.11bn	(2028)	≤ 100000	2.4, 5, 6, 7, 42.5, 71
Wi-Fi 7	802.11be	(2024)	≤ 46120	2.4, 5, 6
Wi-Fi 6E	802.11ax	2020	≤ 9608[1]	6[2]
Wi-Fi 6		2019		2.4, 5
Wi-Fi 5	802.11ac	2014	≤ 6933	5[3]
Wi-Fi 4	802.11n[en]	2008	≤ 600	2.4, 5
*(Wi-Fi 3)**	802.11g	2003	≤ 54	2.4
*(Wi-Fi 2)**	802.11a[en]	1999	≤ 54	5
*(Wi-Fi 1)**	802.11b	1999	≤ 11	2.4
*(Wi-Fi 0)**	802.11[en]	1997	≤ 2	2.4
* Назви Wi-Fi 0, 1, 2, 3 є широковживаними, однак неофіційні[4][5][6]				

Таблиця 1.2 – Покоління Wi-Fi [12]

Як видно з таблиці, першим частотним діапазоном став 2.4 ГГц. Даний діапазон є неліцензованим, саме тому для роботи пристроїв, що не виходять за рамки стандартів та технічних обмежень, не потрібно додаткових дозволів та ліцензій. Однак в даному діапазоні до появи Wi-Fi працював і розроблявся інший тип бездротового підключення – Bluetooth. Ця технологія створена для передачі даних між пристроями в обмеженому радіусі. Саме тому з часом та розробкою

нових стандартів діапазон 2.4 ГГц став перевантаженим, відбувається інтерференція радіохвиль, що призводить до погіршення якості сигналу, некоректності роботи обладнання та завад. При цьому така частота радіохвиль дозволяє краще огинати перешкоди і має більшу проникність, тому радіохвиля менше втрачає потужність при проходженні таких завад, як стіни, дерева і т.д.

В подальшому для розвантаження даного частотного діапазону Міжнародним союзом електрозв'язку було виділено додаткові частотні спектри для роботи нових стандартів Wi-Fi. Саме тому нові покоління стандартів були розроблені в частотних діапазонах 5 ГГц та 6 ГГц. Дані діапазони мають меншу проникність за рахунок меншої довжини хвилі, але дозволяють за одиницю часу передати більшу кількість інформації, маючи пряму залежність від частоти сигналу. Додатково стандарти передбачає механізми частотного поділу каналу та відповідну модуляцію, що значно підвищує ефективність використання каналу.

Наразі більшість обладнання, що функціонує в мережі, використовує обидва типи підключення при функціонуванні в окремо взятій локальній мережі. Користувацькі маршрутизатори зачасту мають можливості дротового підключення та виконувати функцію точки доступу Wi-Fi одночасно. З урахуванням перспектив розробки бездротового зв'язку та їх порівняно меншу вартість розгортання та обслуговування, бездротові локальні мережі стають більш вигідним варіантом для розгортання в межах підприємств, офісів та установ різного призначення.

1.3. Необхідні критерії для створення локальної обчислювальної системи підприємства

Як раніше було зазначено, локальна мережа – набір клієнтських та мережевих пристроїв з'єднаних разом на відносно невеликій території. Розглядаючи побудову локальної мережі для підприємств, варто врахувати специфіку завдань та внутрішніх ресурсів, тому до корпоративних мереж можна висунути певні критерії. Для можливості ж правильно сформулювати дані критерії необхідно чітко визначити мету створення локально-обчислювальної мережі.

В якості мети побудови можна визначити переваги з її створення. Для бізнесу важливим є те, що скорочує витрати та приносить прибуток. Тому з переваг корпоративних локальних мереж є оптимізація витрат на розгортання та утримання інфраструктури, створення єдиного закритого простору для обміну службовою інформацією та можливість віддаленої роботи за допомогою певних інструментів доступу.

Відповідно до цього можна виділити критерії, які можна висунути до локальних обчислювальних мереж підприємства.

1. Одним з головних критеріїв є продуктивність та масштабованість. За час роботи корпоративної мережі на локальних серверах може накопичуватися велика кількість службової інформації, яка має довго зберігатися. Система з часом потребуватиме оновлення, модернізації чи заміни. Тому при проектуванні локальних мереж необхідно враховувати можливість обробки серверним обладнанням службового трафіку, роботи програм на фізичних та віртуальних серверах, передбачити можливість модернізації/заміни обладнання «на гарячу» без простою мережі, а також можливість розширення парку пристроїв без необхідності глобальної перебудови мережі. Сюди ж варто включити розрахунок пікової пропускної здатності як внутрішніх каналів зв’язку, так і зовнішнього каналу для виходу в мережу, а також резервування, з урахуванням можливого масштабування мережі.

2. Не менш важливим є критерій безпеки. Для бізнесу досить важливим є фактор недопущення витоку службової інформації або комерційної таємниці. Саме тому система захисту часто включає в себе не лише специфічні налаштування брандмауера, а й налаштування мережі, створення VPN, встановлення та налаштування систем виявлення та запобігання вторгненню (IPS/IDS) та коректну роботу міжмережевих екранів. Також можливо налаштування контролю доступу за допомогою домен-контролера, що не дозволить користувачам отримати доступ як до мережевих ресурсів, так і до систем на робочих станціях. До даного критерію також можна включити такі дії, як резервне копіювання даних, створення заходів та планів відновлення після будь-якого роду аварійних ситуацій.

3. Надійність. До даного критерію входить проектування системи з мінімальним рівнем відмов і високим рівнем доступності ресурсів. Сюди можна віднести організацію зберігання інформації на серверах за допомогою технології RAID-масивів (дана технологія дозволяє збереження файлу на декількох носіях одночасно або ж частини файлу на різних носіях з подальшим копіюванням, залежно від використовуваного стандарту), підбір серверного обладнання з резервуванням джерел живлення, розрахунок автономного живлення для випадків відключення основних джерел електроенергії, організація додаткових каналів зв'язку для виходу в зовнішню мережу та створення резервного парку пристроїв для оперативної заміни тих, що вийшли з ладу.

4. Критерій сумісності має на меті узгодити можливості мережевих пристроїв та програмних застосунків для стабільної роботи мережі. Сюди відноситься постійний моніторинг сумісності програмного і апаратного забезпечення, підтримка стандартів обміну даними (наприклад, підтримка актуальних стандартів Wi-Fi, Ethernet, стеку протоколів TCP/IP), а також можливість інтеграції нових комплексних систем в існуючу мережеву інфраструктуру.

5. Енергоспоживання. Даним критерієм визначають ефективність використання елекроенергії мережевими пристроями в користувацьких зонах та серверних приміщеннях. Цей розрахунок також впливає на екологічний аспект, тобто враховується тенденція зменшення вуглецевого сліду за рахунок обладнання з більшою ефективністю роботи і меншим споживанням енергії.

6. Економічна ефективність. Даний критерій показує фінансову складову створення, впровадження та обслуговування локально-обчислювальної мережі, оскільки тут враховуються початкові (закупівля обладнання, ПЗ та супутніх матеріалів для створення мережі) та операційні (обслуговування, оновлення, електроенергія) витрати. Також цей критерій дасть змогу оцінити орієнтовний термін окупності інвестицій, що може стати одним з ключових факторів для початку фізичного створення мережі.

7. Зручність управління та обслуговування. Даний критерій важливий з точки зору адміністрування мережі, адже різниця в адміністрування невеликого офісу та великої компанії досить суттєва. До цього критерію відносяться інструменти для

моніторингу та діагностики мережі, легкість та інтуїтивність освоєння інтерфейсів налаштування та адміністрування мережевих пристроїв та розробка правил для налаштування корпоративних персональних пристроїв. Варіантом буде налаштування пристроїв з одної утиліти, тобто будувати систему на одному сімействі приладів. Прикладом такої взаємодії є Fortinet Security Fabric або Cisco DNA Center (зараз Catalyst Center).

Усі ці критерії є основними, але не єдиними, які варто врахувати при створенні локальної мережі підприємства. Кожна локальна мережа має свої задачі, що закладені під час проектування. Тому для розробки варто проаналізувати потреби підприємства, визначивши таким чином переважаючий тип трафіку, застосунки клієнт-серверного типу, орієнтовна кількість користувачів, очікуване навантаження на мережу, а також певні вимоги до конфіденційності та швидкості обробки даних.

При розробці планів та кошторисів мережі доцільним буде закласти можливість адаптації до появи нових технологій та їх зворотної сумісності. До прикладу, варто врахувати можливість подальшого впровадження штучного інтелекту в системи моніторингу мережі, перехід на гібридну архітектуру з використанням хмарних рішень.

Як бачимо, при розробці локальної обчислювальної мережі варто звертати увагу на досить велику кількість аспектів та критеріїв для побудови оптимальної швидкодіючої системи, готової до викликів часу та подальших технологічних нововведень. Системи, побудовані з урахуванням усіх необхідних нюансів є фундаментом для стабільної роботи бізнесу та інструментом взаємодії в бізнес-процесах для максимізації результату.

1.4. Аналіз ринку мережевих технологій

На сьогодні ринок мережевих технологій може запропонувати досить широку лінійку пристроїв для різного роду задач та під різні вимоги від замовників. В користувацькому сегменті, до якого відносять пристрої здебільшого домашнього

користування, існує велика кількість різноманітних виробників та приладів, різницею в яких є, здебільшого, програмне забезпечення та дизайн.

Однак локальні мережі підприємств включають не лише кінцеві точки доступу, а й маршрутизатори рівня ядра мережі. Рівень ядра мережі – це потужні комутатори та маршрутизатори, здатні обробити сотні гігабіт трафіку за секунду. За допомогою подібних пристроїв реалізовується сегментування мережі, агрегація та розподіл трафіку за мітками рівня L3 та багато іншого.

Гарним рішенням є проектування мережі починаючи саме з кореневих концентраторів та маршрутизаторів і продовжити до кінцевих пристроїв. З урахуванням викликів часу і беручи до уваги тенденцію розширення лінійок продукції з закриттям повного спектру можливих рішень для локальних та магістральних мереж, аналіз ринку варто провести на основі даних про виробників пристроїв корпоративної мережної інфраструктури.

Стан ринку найкраще показує дослідження Gartner. Згідно з дослідженням, більшість бізнес-додатків не вимагатимуть розширених можливостей стандарту Wi-Fi 7, тому до 2026 року більше 70% бездротових локальних мереж не матимуть особливих потреб для переходу на нові стандарти. Однак до 2027 року близько 70% підприємств, що оновлюватимуть або масштабуватимуть свою локальну мережу, перейдуть на Wi-Fi 7 через майбутні можливі очікування щодо даної технології та агресивну маркетингову роботу постачальників.

В даному дослідженні Gartner визначає ринок корпоративної інфраструктури як дротові та бездротові мережеві пристрої та відповідне ПЗ. Пов’язаними з цим рішеннями визначені корпоративні комутатори, точки доступу та комплекс необхідних інструментів для захисту, керування, тестування та оптимізації мережевої інфраструктури, що забезпечує доступ для користувачів як всередині фізичної мережі, так і віддалено.

Усі види підприємств використовують корпоративні мережі для підключення та передачі даних з персональних пристроїв до застосунків всередині мережі. Окрім фізичного підключення, усі розглянуті рішення надають наступні можливості у різних видах підприємств, а саме:

- виявлення, ідентифікація, захист, керування та сегментування пристроїв інтернету речей та/або операційних технологій;
- підтримка, тестування та обслуговування компонентів мережевої інфраструктури;
- забезпечення стійкості мережі;
- забезпечення захисту вузлів мережевої інфраструктури;
- забезпечення масштабування та гнучкості процесів зв'язку.

Серед необхідних критеріїв для дослідження ринку фахівці Gartner виділили наступне:

- точки доступу з сертифікацією Wi-Fi IEEE 802.11 з підтримкою частотних діапазонів 2,4 ГГц, 5 ГГц і 6 ГГц;
- мережеві комутатори з можливостями роботи в мережах розподілу, рівнях доступу та ядра мережі;
- контроль Wi-Fi та функціональні можливості управління, що розміщені фізично або на віртуальній машині, яка, в свою чергу, може розташовуватися на краю периметру мережі, в дата-центрі або в хмарі;
- наявність спеціалізованих програм для керування мережею;
- захист пристроїв сторонніх виробників з можливістю керування;
- захист для автентифікації та авторизації пристроїв;
- застосунок для застосування політик безпеки;
- система виявлення вторгнень в дротових та бездротових сегментах;
- застосунки телеметрії для оптимізації та перевірки мережі.

Серед стандартних можливостей пристроїв фахівці виділяють наступне:

- точки доступу з можливостями встановлення як всередині приміщень, так і ззовні з додатковими зовнішніми антенами та підтримкою стандартів Wi-Fi 5, 6 та 6e;
- можливість роботи з технологією Power on Ethernet (PoE);
- можливість створення гостьового сегменту мережі для підключення до інтернету в обхід брандмауера;
- можливість відслідкувати статистику мережевого підключення для користувачів, а також програми, якими вони користуються в мережі;

- мережева структура, яка може створювати відокремлені канали, підключення якими регулюється політиками безпеки. подібні правила мають працювати також через обладнання сторонніх компаній;
- моніторинг та аналітика поведінки користувачів та об’єктів з можливістю інтеграції з політикою мережевої безпеки для виконання відповідних дій в реальному часі;
- здатність збирати та експортувати дані телеметрії, що дозволяють автоматизованим системам безпеки з підтримкою ші виявляти несправності та оптимізувати мережу;
- здатність виявити, ідентифікувати, захистити та керувати некористувацькі пристрої;
- менеджмент видимості та/або продуктивності програм;
- можливість керування за допомогою експортованого API, SNMP та інших застарілих методів керування точками доступу да комутаторами.

Знаючи, що обрали для дослідження фахівці Gartner, проведемо аналіз лідерів (рис. 1.5) ринку щодо мережевих пристроїв [1]. Серед лідерів оберемо Juniper, Cisco, Aruba та Fortinet як найбільш цікаві для дослідження. Huawei Technologies, через низку проблем з законодавством США і підозрами до витоків даних, не розглядатимемо.

Cisco. В дослідженні Gartner Cisco є одним з лідерів ринку. Компанія має досить широкий вибір обладнання в лінійках Catalyst та Meraki для дротового та бездротового підключення, а також мережевих програм та послуг. Продукція компанії представлена на ринках багатьох країн і покриває запити клієнтів як малого і середнього бізнесу, так і великих підприємств. Бачення Cisco в області хмарних технологій полягає в симбіозі локального апаратного забезпечення Catalyst з простотою керування хмарних технологій Meraki для надання клієнтам більшої гнучкості в роботі. Очікування від дослідників такі, що Cisco продовжить інвестиції в рішення з локального централізованого управління (DNA Center, тепер Catalyst Center), NAC (Identity Services Engine [ISE]) і SDA Fabric, оскільки видно прагнення компанії до паритету сценаріїв використання та узгодження досвіду в обох портфоліо.

Рисунок 1.5 – Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure [1]

Переваги:

Портфоліо. Cisco має досить широкий спектр обладнання дротового та бездротового зв’язку, а також спеціалізоване програмне забезпечення для різних організацій та для розгортання мереж будь-якого типу складності.

Вдосконалена мережева підтримка. Інтеграція Cisco ThousandEyes у кожен продукт лінійки, а також глибока співпраця з постачальниками клієнтських персональних пристроїв (Apple, Intel, Samsung)надає реальну інформацію для IT та безпекових випадків будь-якого виду.

Географія продажів. Глобальне охоплення ринків в межах прямих та непрямих продажів позиціонує Cisco як постачальника мережевого обладнання кампусів, що здатен надавати та підтримувати ефективні рішення для клієнтів по всьому світу.

Рисунок 1.6 – Серія Catalyst Industrial wireless solutions [13]

Недоліки.

Зростання цін. Скарги клієнтів стосуються досить високих цін на закупівлю, оновлення та обслуговування інфраструктури обладнання Cisco.

Недостатній мережний паритет. Оператори обладнання Cisco мають визначитися, що буде їм важливіше для розгортання – рішення Meraki для хмарних сервісів чи Catalyst Center для локального фізичного рішення. Відмінності серед цих двох рішень полягають в ключових генеративних функціях штучного інтелекту та аналітики безпеки.

Портфоліо безпеки. Обширне портфоліо безпекових пристроїв створює плутанину в покупців, оскільки збільшується загальна вартість володіння, термін окупності та є необхідність вибору з спектру додаткових функцій компонентів ПЗ.

Fortinet. Fortinet є одним з лідерів дослідження. Їх розробка Fortinet Security Fabric, з допомогою уніфікації пристроїв з допомогою FortiOS, забезпечує досить тісну інтеграцію між дротовими та бездротовими рішеннями компанії. Завдяки протоколу власної розробки FortiLink, FortiAPs та FortiSwitches можуть стати апаратним та програмним розширенням для їх NGFW FortiGate. Діяльність Fortinet є географічно широкою та диверсифікованою, її клієнти варіюються від малих до великих підприємств та офісів/офісних споруд у різних секторах. Фахівці Gartner очікують, що компанія продовжить інвестувати у свої можливості штучного інтелекту включно з розширеним стороннім керуванням та моніторингом

продуктивності мережі. Також очікується, що Fortinet покращуватиме можливості виявлення загроз за допомогою аналітики поведінки користувачів та об’єктів на рівні мережі.

Рисунок 1.7 – Обладнання Fortinet для побудови WLAN [14]

Переваги:

Диференційована пропозиція щодо LAN-сегменту з фокусом на безпеку. Fortinet забезпечує таку архітектуру, де дротові, бездротові та безпекові рішення інтегровані в єдину уніфіковану ОС і хмарну платформу керування.

Спеціальний модуль ШІ. Механізм ШІ FortiAIOps забезпечує надійність мережі в безпековому сегменті, дротових та бездротових мережах, використовуючи дані з бази FortiGate.

Ефективне рішення для невеликих філій. Fortinet має досить продумане рішення для невеликих офісів. Рішення дозволяє FortiAP діяти як кінцева точка уніфікованого безпечного доступу для користувачів (SASE). Уніфікований SASE разом з цифровим моніторингом досвіду забезпечує конвергентний доступ для гібридної робочої мережі.

Недоліки:

Маркетинговий вплив на клієнтів. Більшість покупців безпекової продукції Fortinet надають перевагу WLAN та комутаційним рішенням конкурентів, оскільки маркетинг та продажі мережевих пристроїв та NGFW не взаємодіють. Частка

прибутку Fortinet від мережевих рішень приблизно в 10 разів менше за частку ринку брандмауерів.

Інтерфейси керування. Fortinet має можливість керування декількома шляхами: менеджер FortiGate, FortiManager в хмарі та локально, FortiLAN та FortiMonitor, які використовуються для керування різними мережевими архітектурами. Це призводить до заплутаного поєднання варіантів управління.

Відсутність модульного шасі. Ця прогалина в портфоліо компанії заважає покрити запит клієнтів на використання каналів доступу з високою щільністю або високошвидкісного ядра мережі, де необхідне використання високошвидкісної плати, резервного керування та додаткові джерела живлення в одному корпусі.

Hewlett Packard Enterprise (Aruba). Hewlett Packard Enterprise також є одним з лідерів в Магічному квадранті Gartner'а. Компанія пропонує комплексний підхід до корпоративних мереж завдяки платформі Aruba Edge Service для дротових та бездротових рішень. Aruba Central, доступна як локально, так і в хмарі, отримала оновлення інтерфейсу користувача хмарної платформи, яке має більшість ключових можливостей, наприклад, NetConductor fabric. Діяльність фірми географічно диверсифікована, що дозволяє Aruba закривати потреби бізнес-клієнтів будь-якого розміру. Компанія проводить агресивну політику маркетингу в сфері NaaS, включно з новими пропозиціями, що охоплюють широку екосистему HPE GreenLake. Очікування Gartner полягають у тому, що Aruba продовжить інвестиції в передові мережеві рішення, інтегруючи разом з тим технології Axis Security (хмара безпеки SSE) та Athonet (основне ПЗ для бездротового зв'язку) в єдину хмарну систему керування. Акцентуємо увагу на те, що на момент дослідження HPE має намір заключити договір з придбання Juniper. Однак наразі триває процес узгодження та переговорів, тому кожна компанія відповідає критеріям дослідження і розглядаються окремо.

Рисунок 1.8 – Обладнання Aruba [18]

Переваги:

Управління мережею та безпекою. Aruba ESP (Edge Service Platform) надає автоматизовану та безпечну дротову та бездротову мережі, що включає в себе підключення пристроїв, призначення політик безпеки та моніторинг клієнтів. Це дозволяє запропонувати ключові можливості для розгортання zero-trust архітектури.

Вдосконалення комутації. Aruba пропонує інноваційну особливість своїх пристроїв, що вигідно відрізняє продукцію від конкурентів: оновлення ПЗ під час роботи (in-service software upgrade, ISSU) для комутаторів та керування додатками рівня 7 на портах доступу.

Інклюзивні функції ШІ. Стандартна ліцензія Aruba Central включає такі ключові опції, як AIOps, що мають значну цінність «з коробки». Користувачі отримують вигоду з користування без додаткових витрат на розширену ліцензію, як того вимагають конкуренти.

Недоліки:

Хмарний контроль доступу до мережі. Aruba має в портфоліо нове рішення з назвою Cloud Auth, яке, однак, не відповідає рівню ClearPass. Клієнти мають

ретельно розглянути вимоги до системи та розрахувати загальну вартість володіння за умови придбання додаткових програмних компонентів.

Відсутність можливості керування мережею від сторонніх розробників. Компанія зосередила інвестиції в центральній хмарі та рішеннях локального керування замість застарілої системи AirWave.

Заплутана пропозиція NaaS. Для замовників Aruba пропонує кілька пропозицій NaaS, що приводить до розгубленого стану покупців при виборі варіантів ліцензії та пакетів послуг.

Juniper. Juniper Networks також є одним з лідерів дослідження. Виробник має широкий асортимент рішень для дротової та бездротової мережі, що включає комутатори серії EX та серії QFX, а також точки доступу з керуванням за допомогою Mist AI. Асортимент покриває запити більшості випадків побудови для локальних мереж великих корпорації та ринку mid-small enterprise. Клієнтами Juniper мають різнобічну направленість роботи, включно з освітою, торгівлею, державним управлінням та охороною здоров'я. Інвестувати Juniper продовжує в операції з ШІ, а також у хмарні сервіси безпеки. Очікування дослідників полягають в тому, що буде інвестовано в інтеграцію інструментів GenAI для роботи з інтерфейсом на будь-якій мові без необхідності ручного перекладу.

Рисунок 1.9 – Обладнання Juniper [19]

Переваги:

Автоматизація на основі ШІ. Juniper лідирує завдяки можливостям розробленого ШІ, включно з моніторингом настроюваних SLE, що забезпечить кращу роботу кінцевих користувачів. А кероване виявлення несправностей та можливість автоматичного виправлення стандартних проблем спрощують мережеві операції.

Безпека. Фреймворк WxLAN забезпечує застосування політик в усій мережі як для користувачів, так і для кінцевих точок IoT, а нещодавно представлена служба Juniper Mist Access Assurance додатково надає можливості NAC без агентів.

Спрощене керування мережею. Juniper Campus Fabric, робота якого заснована на накладенні VXLAN з площиною EVPN, має на меті спростити керування пристроями у кампусі та філіях, зменшуючи складність мережі та неузгодженість розгортання.

Недоліки.

Залежна від хмари платформа керування. Хоч Mist Edge обробляє певні мережеві функції локально, для отримання максимальної користі потрібне підключення до Mist Cloud. Застаріле рішення Junos Space не має функціоналу як повністю централізована альтернатива хмарі.

Відсутня підтримка сторонніх розробників. Незважаючи на те, що мережа Juniper побудована на основі стандартної архітектури і взаємодіє з структурами сторонніх розробників, керування сторонніми пристроями не передбачено.

Обмеження на NaaS. Компанія оголосила про пропозицію NaaS, але серед запитів вона майже не з’являється.

Як бачимо, лідери дослідження демонструють здатність задовольнити потреби замовників за рахунок широкого асортименту рішень для всього спектру задач та завдань, а також надавати послуги на підтримку по всьому світу та пропонувати велике різноманіття корпоративних мережевих програм. Особливо важливим є здатність підтримання діалогу з замовниками, мати якнайменше прогалин в портфоліо рішень або перекривати недоліки досить сильними сферами.

2 ВИБІР ОБЛАДНАННЯ ФІРМИ CISCO ТА ДЛЯ ПОБУДОВИ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

2.1. Вибір обладнання для побудови системи захисту

Усім відомий факт, що Зона 51 є найбільш секретним об’єктом у світі з потужною системою безпеки усіх рівнів. Незважаючи на гектари землі навколо бази, що підконтрольні військовим, огорожа по периметру, ключ-карти, спеціалізовані замки, сканери біометрії та безліч засобів сигналізації – жодна з даних функцій окремо не може забезпечити належним чином захист Зони 51. Кожна з них – окрема нитка у плетиві надзвичайно міцної мережі безпеки для захисту як ззовні, так і зсередини [15].

Даний системний підхід може бути застосований до безпеки корпоративних мереж. Хоч міжмережевий екран на краю периметру (edge firewall) з задачами захисту мережі від атак ззовні впорається, однак він не зможе забезпечити захист від атак зсередини[15].

Сучасні загрози призначені для обходу традиційних брандмауерів та початку своєї роботи у незахищеній внутрішній мережі. Поняття довіреної внутрішньої мережі нині є архаїзмом. Покладатися на традиційні методи захисту периметру вже недостатньо. Концепція BYOD (Bring Your Own Device), що стала більш актуальною з урахуванням подій 2020 року, бездротовий та незахищений дротовий доступ – це лише невелика частина способів, якими шкідливий код може потрапити до внутрішньої мережі [15].

Станом на сьогодні більшість критично важливих програм для бізнесу мають в своїй структурі поєднання локальних та хмарних технологій. Саме через це користувачам необхідний безпечний доступ до ресурсів з будь-якої точки світу. У гібридному робочому середовищі програми є новою зоною для захисту в багатьох організаціях. Типове розгортання міжмережевого екрана перетворилося на поєднання фізичних, віртуальних та хмарних рішень. Наслідком є намагання запровадити підтримку сучасних прикладних середовищ [16].

Компанія Cisco розробляє власну концепцію мережевої безпеки для забезпечення гнучкого, автоматизованого та інтегрованого підходу до гармонізації застосування політик безпеки в сучасних програмах та мережах, що мають тенденцію до гетерогенності. З урахуванням підходу до монобрендовості мережі, для дипломної роботи обрано саме брандмауер Cisco, що може надати широкий набір інтеграцій між мережевими функціями та безпекою мережі. Результатом використання є повний портфель засобів безпеки для захисту програм та користувачів як для малого та середнього бізнесу, так і для корпоративних ЦОД та постачальників послуг [16].

Серед переваг можна виділити:

- спрощення операцій завдяки безлічі параметрів керування, оновленню користувацького інтерфейсу застосунків керування та AI Assistant for Security;
- засоби безпеки Cisco підтримуються системою аналізу загроз Talos та мають власний зашифрований механізм безпеки для виявлення зашифрованих загроз;
- компанія пропонує корпоративні ліцензійні угоди та гнучкі варіанти оплати, завдяки чому є можливість заощадити кошти на додаткові рішення або більш потужні пристрої.

Враховуючи те, що загрози та мережі стають більш складними, вкрай важливо мати правильні інструменти для захисту корпоративних даних, програм та мереж. Брандмауери Cisco мають необхідну потужність та гнучкість, що дає змогу бути впевненим у захищеності периметру локально-обчислювальної системи. Кожен пристрій має на борту систему апаратного криптографічного прискорення Secure Firewall, яка може в реальному часі перевіряти зашифрований трафік в великому масштабі або перевіряти його без дешифрування, що значно підвищує ефективність міжмережевого екрану. Окрім того, багатопотоковий механізм перевірки Snort 3 зі зрозумілими для людини правилами допомагає спростити рівень налаштувань безпеки без погіршення самого захисту. Динамічна видимість додатків та контроль доступу доступні через інтеграцію до системи Cisco Secure Workload для цілодобового захисту сучасних додатків.

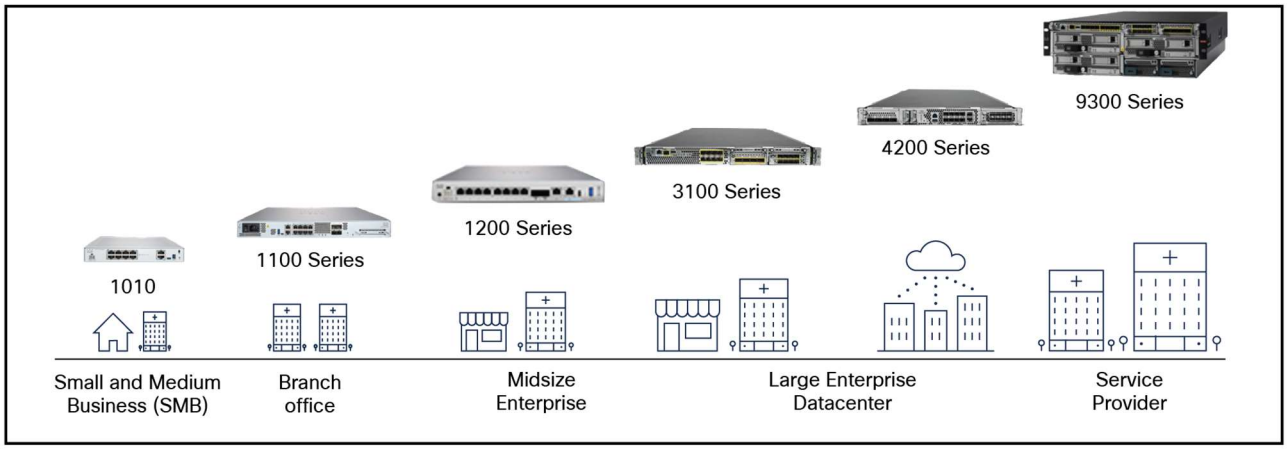

Рисунок 2.1 – Портфоліо пристроїв Cisco Secure Firewall [16]

Згаданий раніше Snort є системою запобігання вторгненням, що здатна виконувати аналіз трафіку в реальному часі та проводити реєстрацію пакетів в мережі. Завдяки алгоритмам роботи система здатна виконувати аналіз протоколів, пошук/зіставлення вмісту та використовуватися для виявлення різноманітних атак, серед яких переповнення буфера, приховане сканування портів, CGI-атаки, SMB-зонди, спроби зняти відбитки ОС та багато інших.

Сам по собі продукт Snort є розробкою компанії Sourcefire. Компанія була придбана Cisco у 2013 році, що дозволило провести інтеграцію технології в рішення від мережевого гіганта.

Керування пристроями захисту можливе за допомогою Cisco Secure FMC. Cisco Secure Firewall Management Center є адміністративним центром з можливістю керування усіма підпорядкованими пристроями. Дана утиліта забезпечує повне та уніфіковане керування міжмережевими екранами, контроль програм, функції системи запобігання вторгненням, фільтрацію URL та розширений захист від ШПЗ. Це є однією з ключових частин портфоліо Cisco Secure, яке забезпечить поглиблений аналіз, оптимізоване керування безпекою як в мережі, так і в хмарі, а також прискорене розслідування інцидентів та реагування на них.

Застосунок надає також комплексну видимість мережі та контроль політик. Це досягається завдяки цілому ряду особливостей роботи рішення, а саме:

- забезпечення виняткової видимості того, що працює в мережі та хмарі;

- швидке виявлення підозрілого або зловмисного трафіку та оперативне створення власних автоматичних правил, що дозволяє запобігти просуванню кібератаки
- вбудований модуль криміналістики для детального аналізу ШПЗ з подальшим безпечним усуненням та можливістю графічно відобразити усі пристрої, що було вражено;
- надання спільного доступу до Cisco Secure Workload з метою розпізнавання іншими пристроями робочого навантаження для кращого захисту динамічних програм в усьому периметрі;
- визначення рівня запобігання вторгненню, правил репутації інтернет-адрес та політик захисту від ШПЗ. При цьому вирішується така проблема, як: «Якщо трафік надходить з такої країни за допомогою такої програми з таким вкладеним файлом, то чи можна застосувати даний рівень перевірки вторгнень, провести аналіз на наявність ШПЗ та надіслати до пісочниці за необхідності».

Secure FMC постійно стежить за змінами в мережі. Застосунок в автоматичному режимі проводить співвіднесення та визначення пріоритетів нових атак з можливими вразливостями в мережі. Завдяки цьому обладнання попереджає фахівців з безпеки про можливо успішні атаки і дозволяє персоналу зосередитися на найбільш значущих. Також наявна функція автоматичного аналізу вразливостей в мережі та рекомендацій щодо застосування політик безпеки того чи іншого виду. Таким чином досягається адаптація захисту до потреб конкретної мережі. Також система використовує критерії файлової політики. Тобто якщо система бачить файл, що відповідає необхідним критеріям, проводиться автоматичний аналіз для виявлення відомого ШПЗ та/або відбувається переміщення файлу в розділ «пісочниці» для виявлення невідомого шкідливого коду.

Графічний інтерфейс Центру управління є досить інформативним. Під час роботи спеціаліст отримує повну контекстну основу для прийняття чітких обґрунтованих рішень. Інтерфейс приведено на рис. 2.2.

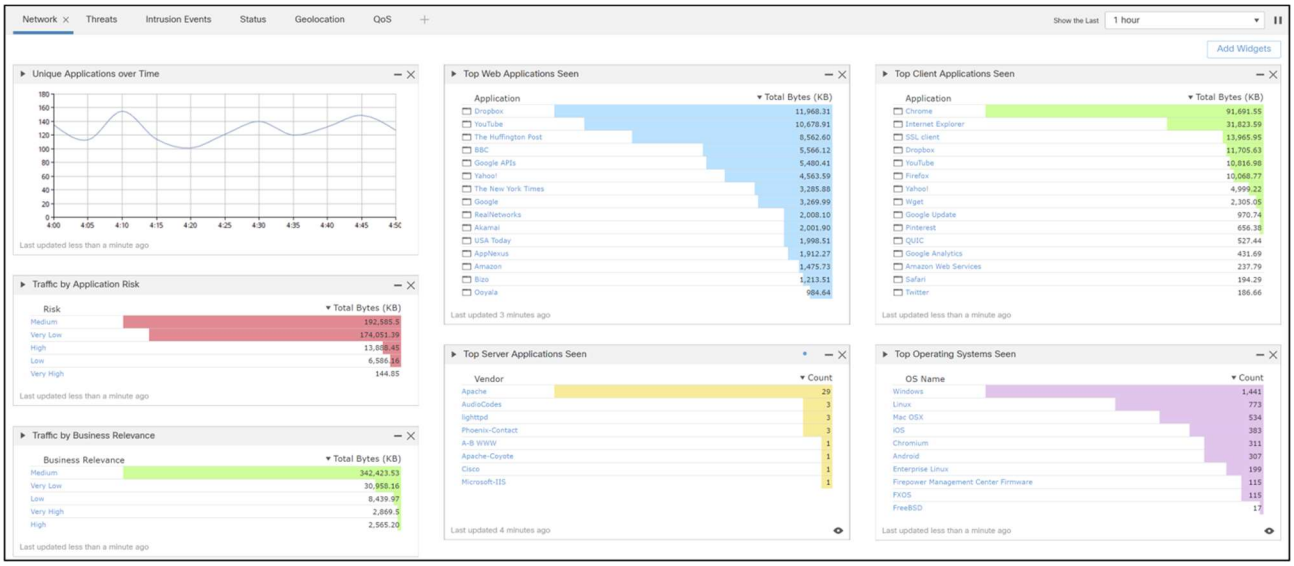

Рисунок 2.2 – Головний екран з основною інформацією [17].

Окрім широкого спектру інтелектуальних даних, Центр управління забезпечує високий рівень деталізації параметрів для отримання точного розуміння стану кожного засобу. Сюди входять:

- високорівнева тенденція та статистика (інформація цього роду надасть розуміння безпеки в певний момент часу та вектор змін);
- деталізація подій, відповідність та криміналістика (даний набір можливостей надасть розуміння того, що відбулося під час події безпеки. Інформація такого роду надає дані для покращення захисту, підтримки зусиль зі стримування порушень та допомогу в правоохоронних діях);
- дані робочого процесу (можливість експорту даних для використання з іншими рішеннями);
- моніторинг в режимі реального часу.

Приклад вікна з показниками пристрою подано на рис. 2.3.

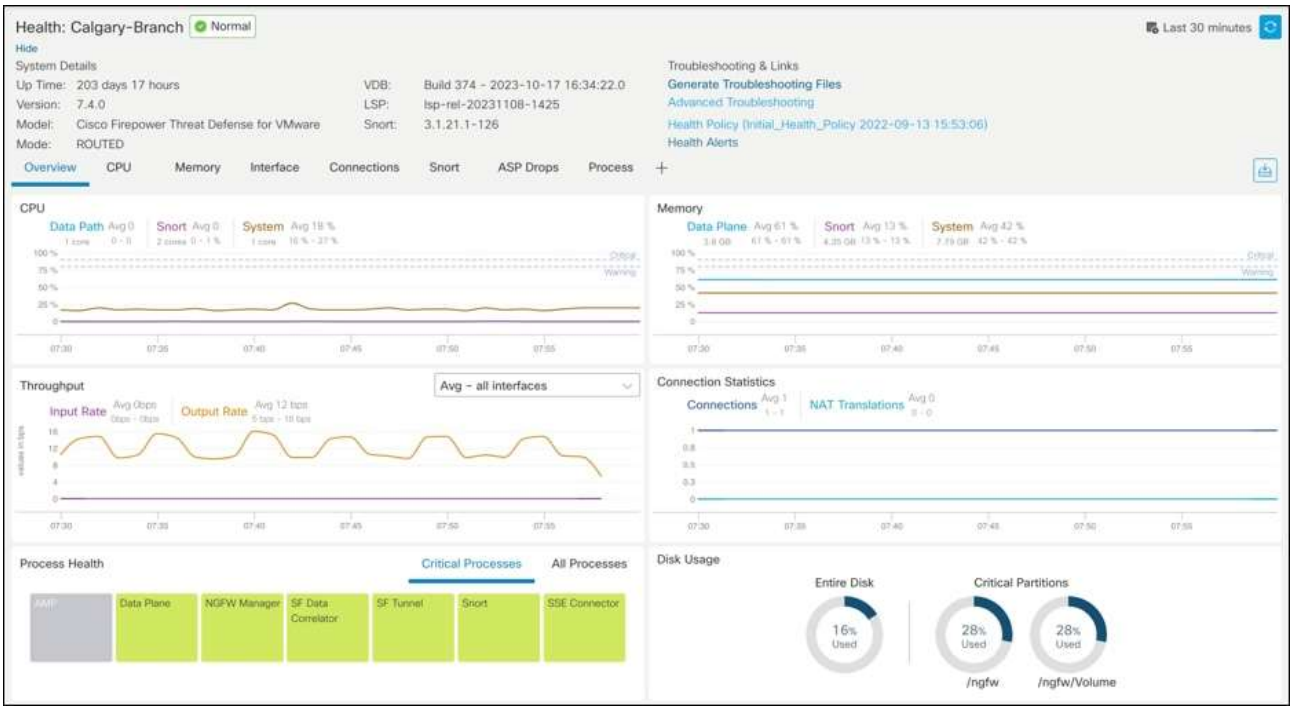

Рисунок 2.3 – Монітор стану пристрою [17]

Центр управління робить можливим інтеграцію зі сторонніми рішеннями за допомогою потужного та багатофункціонального інтерфейсу прикладного програмування (API). В інтерфейсі реалізовано можливості для:

- переміщення даних про події з FMC до іншої платформи, наприклад SIEM системи;
- покращення інформації з бази даних Cisco IPS за допомогою даних від сторонніх рішень;
- запуск робочих процесів та кроків виправлення, що активуються визначеними адміністратором правилами кореляції;
- підтримка сторонніх звітів та аналітики.

Дані API також використовуються для інтеграції з декількома продуктами безпеки Cisco. Серед них Cisco Secure Malware Analytics (раніше Cisco AMP) для ізольованого програмного середовища, Cisco Identity Service Engine для даних ідентифікації та сегментації мережі, а також Cisco Umbrella для видимості домену.

Альянс Cisco Secure Technology Alliance, до складу якого входять усі вище перераховані рішення, є екосистемою безпеки, що сприяє відкритій інтеграції продуктів різних постачальників з метою підвищення безпеки за рахунок автоматизації та простоти експлуатації. Компанія активно та тісно співпрацює з

сотнями ключових постачальників засобів безпеки з метою інтеграції більш ніж десяти продуктів безпеки Cisco.

Одним з важливих продуктів в системі безпеки є Cisco SecureX. Це рішення поєднує широкий спектр інтегрованого портфоліо безпеки Cisco та існуючу інфраструктуру безпеки для узгодженої роботи. Відбувається уніфікація видимості, забезпечується автоматизація та посилення безпеки в мережі, в кінцевих точках, хмарі та застосунках.

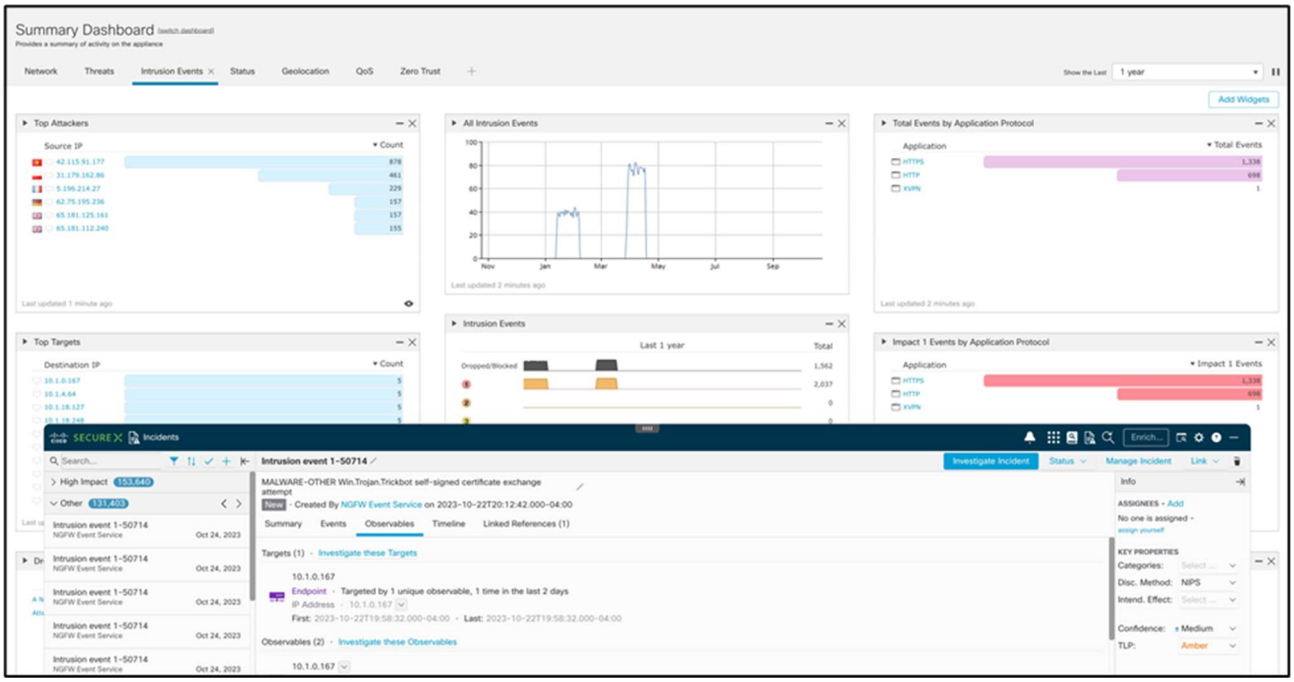

Рисунок 2.4 – Рішення Cisco SecureX в системі Secure FMC [17]

Cisco SecureX об’єднує дані про загрози від системи Cisco Talos і доповнює інформацію зі сторонніх джерел для автоматичного дослідження індикаторів компрометації та швидкого підтвердження загроз.

З точки зору користувача Центру управління міжмережевими екранами, інтегроване рішення SecureX дозволяє адміністратору миттєво повертатися вперед чи назад для більш детального дослідження загроз.

2.2. Вибір обладнання для мережної інфраструктури

Наступним кроком варто обрати обладнання комутації та маршрутизації рівня ядра мережі та пристрої агрегації трафіку. Ядро локальної мережі є ключовим компонентом інфраструктури підприємства, яке забезпечує централізовану

маршрутизацію, управління трафіком і комутацію даних між підмережами. Вибір правильного мережевого обладнання для ядра мережі має вирішальне значення для забезпечення надійності, масштабованості та продуктивності всієї мережі.

Основні компоненти для ядра мережі на базі обладнання Cisco включають комутатори серії Catalyst і маршрутизатори серії ISR та ASR.

Комутатори Cisco Catalyst забезпечують високу швидкість комутації та підтримку новітніх технологій безпеки та управління трафіком. Вони ідеально підходять для ядра мережі, де потрібна висока пропускна здатність і відмовостійкість. Серія Catalyst, яка є одним з основних елементів побудови ядра фізичної мережі та мережевої хмари, допомагає зменшити рівень складності розгортання та обслуговування, оптимізувати процеси та зменшити експлуатаційні витрати за рахунок використання ШІ, автоматизації та людського досвіду.

Рисунок 2.5 – Комутатори серії Catalyst [20]

Комутатори даної серії забезпечують такі функції безпеки, які здатні захистити не лише цілісність апаратного забезпечення, а й програмне забезпечення та дані, що проходять через порти комутатора. Дане рішення, завдяки повній підтримці стандарту PoE+, резервуванню систем живлення та охолодження, високій пропускній здатності на рівні 160 Гб/с, модульним аплінкам, підтримці функціоналу рівня L3 та холодним виправленням, є гарним рішенням для побудови економічно ефективних корпоративних мереж з диференціацією відмовостійкості та прогресивною архітектурою мережі. Управління може здійснюватися як через консоль завдяки Cisco CLI, так і за допомогою програмних рішень Cisco Catalyst Center або хмарного моніторингу панелі Meraki.

Catalyst Center є більш зручним рішенням для побудови мереж гібридного типу. Це потужний мережевий контролер та інформаційна панель, що надає можливості для керування мережею, оптимізувати інвестиції та зменшити витрати на IT складову компанії.

Маршрутизатори Cisco забезпечують ефективне управління трафіком, високу швидкість маршрутизації та підтримку передових технологій безпеки. Їхня інтеграція з іншими рішеннями Cisco дозволяє створювати надійні мережі з низькими затримками.

Одним з оптимальних рішень є Cisco 1000 Series integrated service routers (ISR). Портфоліо маршрутизаторів даної серії давнє і постійно доповнюється. Дані рішення поєднують комутацію, маршрутизацію, доступ по Wi-Fi, інтегровані можливості забезпечення безпеки та варіант підключення DSL та LTE ліній зв’язку як зовнішній вихід з маршрутизатора, в одному високопродуктивному пристрої.

Рисунок 2.6 – Серія пристроїв Cisco ISR 1000 [21]

Серед ключових особливостей варто виділити:

- одне з найкращих апаратних рішень, що поєднано з багатофункціональним ПЗ;
- технології стільникового зв’язку стандарту 5G, включно з підтримкою двох несучих, агрегацією несучих та 5G SA;
- гнучкі рішення керування мережею;
- бездротовий зв’язок з підтримкою стандарту Wi-Fi 6, що вбудовано в невеликий корпус без активного охолодження;
- розширені функції безпеки, що доступні «з коробки», включно з брандмауером з розпізнаванням додатків, IPS/IDS системами, розширеним захистом від ШПЗ, фільтром IP-адрес та захищеним інтернет-шлюзом Cisco.

Як видно, обладнання Cisco для ядра локальної мережі забезпечує високу продуктивність, гнучкість і безпеку, що робить його ідеальним вибором для підприємств будь-якого масштабу. Завдяки різноманіттю моделей і підтримці сучасних мережевих технологій, Cisco пропонує рішення для побудови стабільних і надійних мереж.

2.3. Вибір обладнання точок доступу та клієнтських терміналів

В безпровідних мережах найближче до користувача знаходяться точки бездротового зв'язку (або AP – access point). Сучасні підприємства активно використовують бездротові мережі для забезпечення зручного доступу до інформації та корпоративних ресурсів. Один з варіантів серед рішень Cisco є точки доступу серії 9176. Це обладнання нового покоління з підтримкою ШІ, що забезпечує кращий досвід роботи з пристроями як в фізичному, так і мережевому плані.

Бездротові точки доступу Cisco Wireless 9176 підтримують новітній стандарт Wi-Fi 7 (802.11be), який забезпечує підвищену швидкість передачі даних, покращену ефективність роботи в умовах високої щільності клієнтів та знижену затримку. Пропонуючи безпрецедентну швидкість, підвищену безпеку та стійке підключення, ці продукти ідеально підходять для середовищ із високою щільністю та критичних програм. Вони легко інтегруються в існуючу мережу, будь то локальна, хмарна чи гібридна, забезпечуючи гнучкі варіанти розгортання відповідно до різноманітних потреб організації.

Підприємства можуть використовувати передбачуваність і низьку затримку Wi-Fi 7 для підтримки кращого потокового відео, програм доповненої реальності (AR) і віртуальної реальності (VR). Поєднуючи людей і речі у фізичному просторі, бездротові рішення Cisco з Wi-Fi 7 пропонують статистику в реальному часі та дії, такі як навігація в приміщенні та персоналізований досвід користувача.

Завдяки вищій швидкості передачі даних, зменшеному перевантаженню мережі та спрощеному управлінню мережею завдяки аналізу та автоматизації на

основі штучного інтелекту бездротові точки доступу Cisco серії 9176 створюють основу для бездротового зв’язку майбутнього.

Рисунок 2.7 – Cisco Wireless 9176 [22]

Глобальні точки доступу серії 9176 пропонують стійке, масштабоване рішення для сучасних бездротових мереж. Ці точки здатні працювати безперебійно працюють в будь-якому режимі розгортання, що забезпечує гнучкість та захист інвестицій.

Дані пристрої також мають можливість інтелектуального виявлення процесу керування, що є плавним, масштабованим та простим. Процес адаптації точок доступу до глобального використання усуває потребу в продуктах, пов’язаних зі стеком і регуляторними доменами, заощаджуючи час і зусилля під час встановлення.

Поєднання точок доступу Cisco Wireless 9176 Series з WLC Catalyst 9800 Series і Cisco Catalyst Center забезпечує повну трансформацію мережі. Cisco Catalyst Center дозволяє зрозуміти мережу за допомогою аналітики в реальному часі, швидко виявляти та стримувати загрози безпеці, а також легко забезпечувати узгодженість усієї мережі завдяки автоматизації та віртуалізації. Серія Cisco Wireless 9176 підтримує програмно-визначений доступ (SD-Access), одну з провідних корпоративних архітектур Cisco.

Головною особливістю пристроїв є, звісно, підтримка стандарту Wi-Fi 7. Стандарт IEEE 802.11be, також відомий як Extremely High Throughput (EHT) або Wi-Fi 7, є найновішим у Wi-Fi із такими вдосконаленнями, як 4K-QAM,

багатоканальна робота (MLO), розширений ортогональний частотний множинний доступ (OFDMA), підтримка пробивання преамбули для каналу шириною 320 МГц, створеного для збільшення швидкості передачі даних і продуктивності підключення, особливо для додатків вимагають низької затримки, як додатки AR і VR.

Серед переваг Wi-Fi 7 можна виділити наступне:

- Збільшення швидкості передачі даних для потреб відео 8K, 16K, потокових ігор і VR.
- Покращена робота в мережах із високою щільністю клієнтів, наприклад, на стадіонах, у торгових центрах і офісах.
- Підтримка більшої кількості одночасно підключених пристроїв без зниження продуктивності.
- Мінімізація затримок, що критично важливо для ігор і потокового відео в реальному часі.

Для реалізації технології Wi-Fi 7 в своїх пристроях Cisco вирішила ряд питань, що стоять перед виробниками пристроїв з підтримкою даного рішення:

- Вимоги до апаратного забезпечення: Для використання всіх переваг Wi-Fi 7 потрібні сумісні пристрої (точки доступу, маршрутизатори, клієнтські пристрої).
- Складність налаштування: Більша кількість доступних каналів і технологій вимагає складнішого управління та конфігурації мережі.
- Енергоспоживання: Підтримка 4K-QAM і ширших каналів може підвищити енергоспоживання пристроїв.

Для вирішення проблеми енергоспоживання Cisco розробила механізм оптимізації живлення. Оптимізація живлення AP (режим енергозбереження AP) дозволяє точці доступу зменшити енергоспоживання, наприклад вимикання радіомодуля в неробочий час і у вихідні – при цьому залишаючись достатньо кмітливим, щоб повторно задіяти всі функції, якщо вони знадобляться. Це економить енергію та зменшує викиди вуглекислого газу під час роботи бездротової мережі.

Одним з покращених рішень є регулювання частоти. Це покращення допомагає клієнтам, які працюють на частоті 6 ГГц, залишити радіосмугу 5 ГГц і підключитися до модуля 6 ГГц. Клієнти з підтримкою Wi-Fi 6E автоматично спрямовуються на підключення до радіомережі 6 ГГц, щоб скористатися перевагами, які пропонує ця частота, одночасно очищаючи смуги частот 2,4 та 5 ГГц для клієнтів з обладнанням, що працює з попередніми стандартами зв'язку.

Також, оскільки портфоліо пристроїв Cisco має таку позицію, яка стосується локальної мережі підприємства, варто розглянути рішення IP-телефонії.

Cisco пропонує новий стандарт для настільних телефонів із портфоліо, створеним для роботи в сучасному офісному середовищі. Настільні телефони серії 9800 були розроблені з урахуванням інформаційних технологій і можливостей. До кожного телефону входить нещодавно випущене програмне забезпечення PhoneOS, яке спрощує взаємодію з користувачем і доповнює відеопортфоліо пристроїв RoomOS, щоб забезпечити безперебійну роботу від робочого столу до конференц-залу. Завдяки розширеним функціональним можливостям серія 9800 поєднує в собі безпечні корпоративні виклики, зустрічі, , надійність і екстрені сповіщення – все в одному пристрої.

Рисунок 2.8 – Настільні телефони Cisco 9800 Series [23]

Настільний телефон серії 9800 полегшує придбання, розгортання, керування та навчання. Щоб ще більше спростити, можна використовувати один пристрій для Cisco Unified Communications Manager (CUCM), Webex Calling, Broadworks або інших сторонніх хмарних платформ для викликів. Поряд з широким портфоліо настільних пристроїв, серія 9800 займає унікальне місце на ринку, щоб допомогти трансформувати робоче місце, долаючи розрив між гібридною роботою, дзвінками

та зустрічами, і є найбільш рентабельним рішенням для робочих станцій у великому масштабі.

Стандартизація технологій і консолідація постачальників є одним із способів, за допомогою якого IT-команди спрощують свою стратегію. Це економить час і ресурси на кожному кроці – вибір пристрою, розгортання, а також постійне керування та аналітика простіше. З настільним телефоном серії 9800 можна стандартизувати одну з чотирьох моделей, які можна налаштувати як для локальної роботи, так і для хмари. Усі вони працюють на PhoneOS, яка була розроблена для роботи разом із RoomOS для конференц-залів. Це дає користувачам стабільну роботу від робочих столів до кімнат для переговорів.

Розгортання та керування також є ефективнішими завдяки мітці NFC, вбудованій у кожен телефон – ініціалізацію можна виконати, навіть не відкриваючи коробку. Це економить час і ресурси для розгортання більших клієнтів і постачальників послуг. Налаштування та усунення несправностей можуть відбуватися безпосередньо в Control Hub. Використовуючи ThousandEyes, користувачам надається можливість детально ознайомитися з продуктивністю мережі та справністю пристрою, сприяючи швидкому та обґрунтованому реагування на будь-які проблеми, що виникають.

В підсумку, для дослідження та побудови варіанту локальної обчислювальної мережі підприємства було проаналізовано та обрано оптимальні варіанти рішень, які є універсальними для більшості підприємств в процесі побудови LAN. Варто зауважити, що портфоліо Cisco є досить широким, а пристрої є в модульному виконанні. Тобто майже будь-який пристрій може бути змінено саме під потреби конкретного підприємства. Тому було розглянуто саме ті варіанти, які є універсальними та закривають багато можливих запитів за свою вартість.

3 РОЗРОБКА ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА НА БАЗІ МЕРЕЖЕВОГО ОБЛАДНАННЯ CISCO SYSTEMS

3.1 Узагальнений варіант топології підприємства середнього розміру

Локально-обчислювальна система підприємства може базуватися як на однорівневому, так і на багаторівневому встановленні рішень в топології мережі компанії. Топологія мережі визначає фізичні та логічні з'єднання між мережевими пристроями та формує основу для забезпечення ефективного обміну даними всередині підприємства. Вибір підходу до розробки та реалізації топології залежить від розмірів інформаційної системи компанії, фрагментації мережі та виокремлення критичних місць інфраструктури.

При розробці варіанту топології варто враховувати наступні вимоги:

- Масштабованість: топологія мережі має враховувати можливості збільшення кількості користувачів та/або пристроїв в майбутньому;
- Продуктивність: мережа має забезпечити високошвидкісний обмін даними як між внутрішніми сервісами підприємства, так і доступ до сервісів поза локальною мережею з заданими параметрами;
- Надійність: наявність в мережі певних механізмів відмовостійкості для безперервності роботи критичних служб;
- Безпека: реалізація механізмів захисту мережі для протидії зовнішнім та внутрішнім загрозам;
- Ефективність управління: можливість централізованого моніторингу та адміністрування мережі.

Переважна більшість підприємств розробляє багаторівневу топологію мережі для сегментування необхідних важливих зон та адміністрування їх окремо одна від одної. Зазвичай мережі такого роду є ієрархічними і мають наступні рівні:

1. Рівень ядра: основний рівень, де відбувається високошвидкісна маршрутизація між багатьма сегментами мережі та підключення до зовнішніх ресурсів;

2. Рівень розподілу: даний рівень виконує агрегацію трафіку з різних сегментів, застосовує політики безпеки та контроль доступу;

3. Рівень доступу: забезпечує підключення кінцевих користувацьких пристроїв та датчиків до мережі.

Розглянемо більш детально кожен рівень.

Рівень ядра також називається мережевим магістральним рівнем. Він відповідає за забезпечення високошвидкісного транспорту між розподіленими комутаторами в межах підприємства.

Внутрішній підрівень влаштовано комутаторами високого класу і високопродуктивними рішеннями комутації, що мають модульний форм-фактор. Це пристрої з можливостями резервування, що підтримують розширені функції комутації 3 рівня і протоколи динамічної маршрутизації. Основною їх задачею є збереження конфігурації пропускної здатності вище мінімально необхідної на рівні ядра.

Через дуже високу критичність цього рівня, проектування його вимагає високої стійкості для швидкого і плавного відновлення після будь-якого збою мережі в межах блоку ядра.

Далі наведемо основні характеристики внутрішнього підрівня:

- висока продуктивність і наскрізна комутація;
- забезпечення надійності та відмовостійкості;
- масштабованість.

Серед комутаторів Cisco, що працюють на рівні ядра можна виокремити Catalyst серії 9500/6800/6500 і Nexus серії 7000.

Розподільчий рівень розташований посередині між рівнями доступу та ядра. Основна функція даного рівня – забезпечити маршрутизацію, фільтрацію трафіку та WAN-доступ, а також показати зв'язок між рівнями доступу та ядра. Крім того, комутатори рівня розподілу можуть надавати певні мережеві та безпекові служби для багатьох комутаторів рівня доступу. Рівень розподілу гарантує, що пакети

маршрутизуються між підмережами VLAN в середовищі корпорації. В якості стандартного підходу, шлюзи за замовчуванням для всіх VLAN будуть комутатори рівня розподілу. Однак, за звичайних умов, серверні пристрої не повинні бути безпосередньо підключені до розподільчих комутаторів. Даний підхід забезпечує економію витрат на порт за рахунок високої щільності портів при менш дорогих комутаторах рівня доступу.

Розглянемо основні функції, що покладаються на розподільчий рівень:

- акумулювання каналів LAN/WAN;
- контроль доступу та фільтрація, такі як ACLs і PBR;
- маршрутизація між LAN і VLAN, а також між доменами маршрутизації;
- надмірність і балансування навантаження;
- підсумовування підмереж і агрегування маршрутів на кордонах/до рівня ядра;
- управління широкомовним доменом (пристрій рівня розподілу діє як точка поділу між широкомовними доменами).

Основними моделями комутаторів Cisco, що працюють на розподільному рівні, є Catalyst серії 6800/6500/4500/3850

Рівень доступу включає в себе комутатори рівня 2 і точки доступу, що забезпечують підключення до робочих станцій і серверів. На лініях зв'язку до рівня розподілу пристрої рівня доступу підключаються WAN-портами до розподільчих комутаторів. Адміністратор мережі має можливості керування контролем доступу і політиками безпеки, створювати окремі домени і забезпечувати безпеку портів на рівні доступу. Комутатори даного рівня забезпечують доставку пакетів трафіку на кінцеві пристрої.

Рівень доступу виконує ряд функцій, в тому числі:

– комутація рівня 2;

– висока доступність;

– безпека портів.

Варіанти топології будемо розглядати на прикладі однієї загальної топології (рис. 3.1).

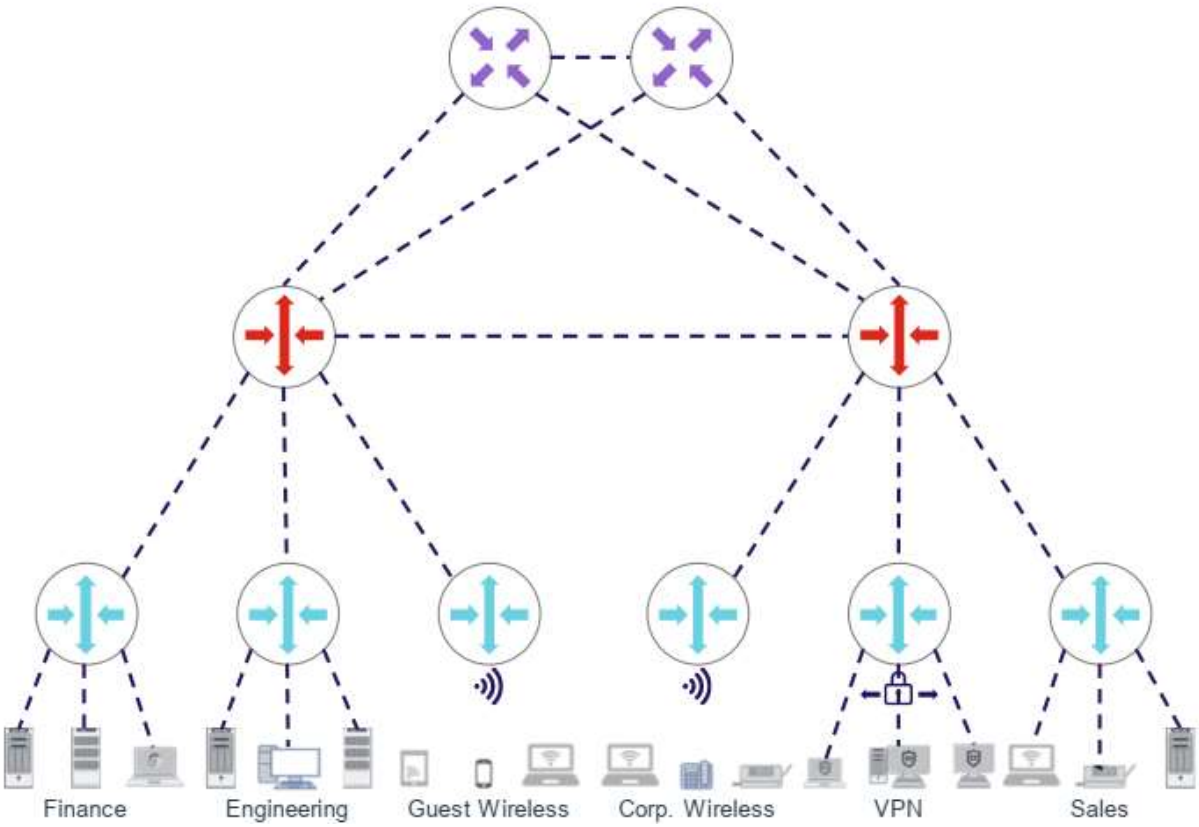

Рис. 3.1 – Варіант загальної топології [24]

Дана топологія включає класичне виконання корпоративного офісу. Відділи фінансів, інженерів та продажів мають свої окремі комутатори, окремо розташовано комутатор з робочими місцями з активним VPN та дві точки доступу, з яких одна для відвідувачів офісу, а друга для корпоративних безпровідних пристроїв. Умовно назвемо їх першим рівнем комутації офісу.

Другий рівень комутації в даному варіанті топології представлено двома комутаторами, які поділяють весь офіс на дві великі зони та спілкуються з комутаторами своєї частини першого рівня комутації, на своєму рівні та з третім рівнем комутації, де працюють маршрутизатори з виходом в загальну мережу.

Таку топологію можна вважати загальною, оскільки більшість офісів компаній побудовано саме таким чином, де в якості першого рівня комутації виступають некеровані хаби або Wi-Fi роутери для потреб персоналу та відвічувачів/гостей офісу.

Для зручності згенеруємо топологію, що представлена вище, в більш конкретному варіанті за допомогою Cisco Packet Tracer.

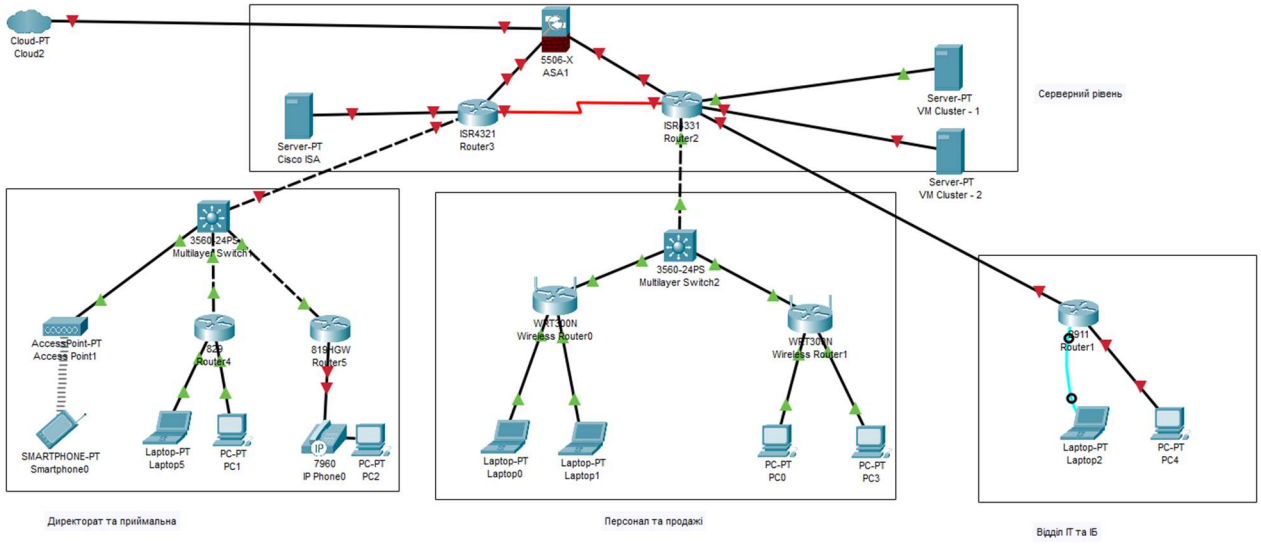

Рисунок 3.2 – Варіант топології мережі

В даному випадку обладнання Cisco Firepower або аналог виступає в ролі граничного маршрутизатора з функцією міжмережевого екрану. В рішеннях даного типу вирішуються проблеми захисту бізнесу від зовнішніх загроз, захисту користувачів від Інтернет-загроз та забезпечення загальної продуктивності користувачів на високому рівні.

Такий випадок використання передбачає концентрацію захисту на кордоні мережі між Інтернетом та внутрішньою мережею офіс. Однак, незважаючи на об’єднання пристроїв Cisco в одну програмно-апаратно екосистему, недоліками даного рішення є те, що плоска мережа не забезпечує внутрішньої безпеки, видимість в мережі сильно обмежена та наявний дуже високий ризик компрометації.

В даній мережі довіреними є мережеві адреси, ідентифікація користувачів та застосунки. Додаткові інструменти захисту представлені налаштованими антивірусом, контролем програм, веб-фільтром та IPS.

3.2 Сегментація мережі

Локально-обчислювальна мережа підприємств є критично важливим інструментом бізнесу в багатьох сферах, оскільки саме вона забезпечує роботу незліченної кількості бізнес-процесів, що пов'язано з передачею інформації службового та конфіденційного характеру. Разом з тим загрози інформаційної

безпеки безупинно еволюціонують, тому актуальність потреби в ефективних засобах захисту інформації залишається високою.

Довгий час увага фахівців з інформаційної безпеки була зосереджена на захисті периметра мережі. Однак в сучасних мережах класичне поняття периметра поступово розмивається. Користувачі підключаються до мережі різними способами, включно з дротовими та бездротовими сегментами, а також VPN-підключеннями. Концепція BYOD (Bring Your Own Device), що стала більш актуальною з урахуванням подій 2020 року, поширюється на все більшу кількість підприємств. При цьому в рамках IT-інфраструктури організації, як правило, існує безліч типів користувачів і пристроїв, яким для виконання своєї роботи потрібен доступ до різних ресурсів мережі. Реалізація належного сегментування мережі та контроль доступу в сучасній розподіленій та динамічній IT-інфраструктурі є досить непростим завданням. З урахуванням великої кількості векторів атаки, що дозволяють зловмисникам і ШПЗ проникати в корпоративну IT-інфраструктуру, ймовірність порушення інформаційної безпеки є вкрай високою і, як правило, це питання часу.

Довірена внутрішня мережа сьогодні є застарілим поняттям. Звичні методи захисту корпоративних мереж зараз є недостатніми. Саме тому одним з варіантів ускладнення захисту без додавання додаткових пристроїв є сегментація мережі. Початковою дією є розробка плану поділу користувачів на логічні групи, регуляція доступу для кожної з цих груп, створення віртуальних підмереж для роботи груп користувачів, а також розробка документації та опис політик безпеки для кожної з груп. Залежно від останнього вирішується питання інформаційної взаємодії користувачів з різних ланок, тобто інформаційний обмін або встановлюється обмежено, або блокується.

Логіка поділу користувачів розробляється залежно від функціональних обов’язків та необхідності в доступі до ресурсів мережі. Як типовий варіант розділення груп можна виділити наступні категорії користувачів та пристроїв: співробітники, гості, тимчасово найнятий персонал, пристрої, що не відповідають вимогам політик безпеки (ізольована зона), датчики та інженерні підсистеми і далі за списком. Окрім того, користувачі можуть також бути розділені за їх місцем в

ієрархії компанії. Це може бути як поділ за відділами, так і поділ за посадами, наприклад топ-менеджмент, бухгалтерія, керівництво, звичайні співробітники тощо.

Завданням сегментації є спрощення адміністрування локальної мережі за рахунок адміністрування груп користувачів замість присвоєння правил кожному користувачу окремо, а також зниження ризиків інформаційної безпеки за рахунок обмеження можливостей зловмисників, утворивши зони стримування в разі проникнення неавторизованих користувачів всередину локальної мережі.

Підхід до поділу користувачів на групи варто розглядати найперше з точки зору інформаційної безпеки для захисту бізнес-процесів, персональних даних та конфіденційної інформації. Згідно з розробленими політиками безпеки, співробітникам кожної з логічних груп може бути доступним лише частина корпоративних та загальних ресурсів, які необхідні для виконання покладених на них обов’язків та задач. Прикладом може стати доступ до ERP-системи з інформацією конфіденційного рівня лише для керівництва компанії, а доступ до бази даних персоналу – для співробітників профільного відділу і, за необхідності, керівництву. Більшість звичайних та тимчасово найнятих працівників можуть мати доступ лише до обмежено загальних ресурсів, наприклад, CRM та електронна пошта, але при цьому доступ до усіх інших ресурсів та застосунків мережі буде закритий.

Вплив підходу сегментації найбільше відчутний в сфері інформаційної безпеки. Інциденти в даній області часто призводять до порушення доступності окремих ресурсів, втрати або крадіжки інформації. Тому підхід сегментації сприяє підвищенню загальної безпеки мережі та доступності ресурсів, а також безперебійності усіх бізнес-процесів організації.

Окрім того є досить велика кількість випадків, за яких використання поділу на сегменти є вкрай необхідним. Як приклад, згаданий раніше гостьовий доступ. Адже доступ до мережі Інтернет без обмежень (окрім законодавчих) має бути в окремому логічному каналі з метою захисту усієї іншої інфраструктури. Також можна згадати такі випадки, як підключення до мережі пристроїв, що належать іншим організаціям, доступ аудиторів та багато іншого. Також рекомендовано

виконувати сегментацію за умови роботи в одній фізичній мережі співробітників сумісних організацій та структур з метою недопущення співробітників однієї служби до серверів баз даних іншої організації.

Варіанти застосування можна перераховувати нескінченно, але всі варіанти призводять до реалізації на практиці системи сегментування.

Основними завданнями в реалізації процесу сегментації є:

- визначення приналежності користувача до необхідної групи в момент підключення до мережі / входу в мережу (задача 1);
- відмежування трафіку користувача однієї групи від користувачів з інших груп під час передачі даних мережею (задача 2);
- забезпечити доступ користувача до чітко визначених ресурсів мережі та, як зазвичай буває, блокувати доступ до усього іншого. Це можна сформувати як «Заборонити все, що не дозволено» (завдання 3).

Зазвичай перше з завдань вирішується за допомогою автентифікації та авторизації на RADIUS-сервері (часто з використанням даних з корпоративної служби каталогів, наприклад Active Directory). Однак можливо використання й інших методів присвоєнні групи, таких як статичне присвоєння групи залежно від порту підключення, VLAN, IP-мережі, авторизація за MAC-адресою та інші. Незалежно від обраного методу сегментації реалізація залежить від можливостей сервера AAA і обладнання, що використовується.

Друге завдання традиційно вирішується шляхом створення окремих віртуальних каналів для кожної групи користувачів. Зазвичай це робиться з використанням засобів віртуалізації мережі. У випадку з невеликими мережами інженери використовують VLAN'и і транки стандарту IEEE 802.1Q. Також часто використовуються технології рівня 3, наприклад Multi-VRF CE (VRF-Lite). Великі мережі характеризуються використанням MPLS VPN з протоколами LDP та OSPF.

Третє завдання спеціалісти вирішують за допомогою фільтрації пакетів на основі IP-адреси хоста. Контроль доступу при цьому здійснюється двома можливими способами. Перший – створення списків контролю доступу (access-list) на кожному елементі мережевої інфраструктури. Однак це вважається доволі «грубим» способом фільтрації. Більш «тонким» та точним є фільтрація на системах

захисту нового покоління (NGFW, NGIPS). Незалежно від способу, головним критерієм перевірки та допуску є IP-адреса. Перевірка та фільтрація трафіку здійснюється в одному або декількох точках обміну трафіком між логічними групами користувачів.

Часто фільтрацію пакетів використовують навіть без утворення віртуальних каналів. Тому можна вважати, що в такому випадку фільтри пакетів здійснюють дві задачі одночасно.

3.3 Технологія Cisco TrustSec

Cisco TrustSec –технологія сегментації, що розроблена компанією Cisco і дозволяє автоматизувати вирішення питань, що розглянуто вище. На рис. 3.3 показано спрощений приклад мережі Cisco TrustSec.

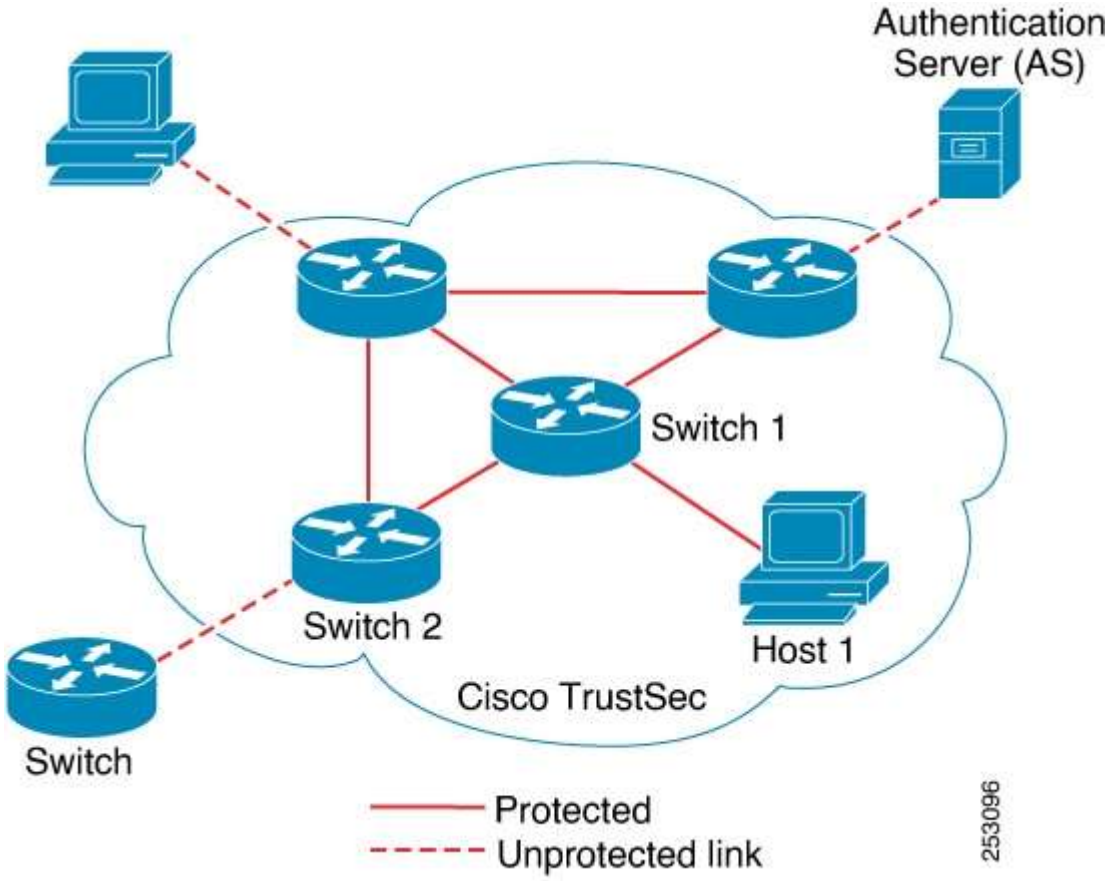

Рисунок 3.3 – Приклад мережі Cisco TrustSec [25]

Як і при використанні звичайних методів сегментування, домен Cisco TrustSec передбачає розміщення користувачів до визначених логічних груп шляхом автентифікації та авторизації користувача за допомогою виділеного AAA сервера,

яким в даній технології виступає Cisco Identity Services Engine (Cisco ISE). Сервер Cisco ISE здатен провести автентифікацію та авторизацію користувача за допомогою як внутрішньої бази даних, так і використовуючи зовнішні каталоги, наприклад, Microsoft Active Directory. TrustSec здатен працювати з різноманітними типами облікових даних, серед яких можна назвати MSCHAPv2, Generic Token Card (GTC), одноразовий пароль RSA і далі за списком. Альтернативними методами автентифікації є MAC Authentication Bypass, Web Authentication, Passive Identity (Easy Connect) на основі Active Directory та ін. Також технологія дозволяє застосовувати статичні методи, що сегментують на основі VLAN, IP-адреси, інтерфейсу підключення тощо.

На цьому подібність з іншими системами закінчується. Cisco TrustSec має механізм призначення кожній окремій групі користувачів 16-бітної мітки безпеки (Security Group Tag, SGT) під час підключення до мережі. Зазвичай подібна процедура проходить або на обладнанні периметру мережі, або на комутаторі доступу всередині корпоративної локальної мережі.

Широкий вибір варіантів класифікації та присвоєння міток користувачам, можливість роботи з дротовими та бездротовими підключеннями, підключеннями серверного рівня, VPN та багато іншого надає можливість створити на основі Cisco TrustSec єдину політику доступу для всіх типів пристроїв і підключень. Мітка SGT призначається сервером Cisco ISE в автоматичному режимі або статично елементом мережевої інфраструктури, а далі система TrustSec працює з мітками.

Саме тому сегментація та контроль трафіку за допомогою TrustSec є більш простим та ефективним рішенням. За звичайного підходу варто розробити віртуальну топологію з поділом користувачів. Рішення від Cisco дозволяє спростити цю роботу саме завдяки присвоєнню міток груп. Таким чином необхідність створення топології відпадає і користувачі можуть працювати на базі єдиної фізично-логічної топології.

Для рішення питання контролю доступу технологія TrustSec має просте та ефективне рішення. Як було сказано вище, звичайний підхід засновано на контролі доступу за IP-адресою. Cisco TrustSec передбачає роботу з списками доступу, де критерієм є саме мітка SGT. Ці списки називаються Cisco TrustSec Security Group

ACL (SGACL). Використання SGACL дає можливість серйозного спрощення роботи: взамін великій кількості списків доступу, що засновані на IP-адресах, мережеві адміністратори працюють з більш зручними SGACL, що, в свою чергу, мають в основі для роботи лише мітки груп і не вимагають ні віртуальної топології, ні фізичних чи мережевих адрес.

Концепція роботи системи реалізується в матриці TrustSec Policy сервера Cisco ISE. На заміну спискам доступу на окремих розрізнених вузлах мережі адміністратор використовує централізовану матрицю, що розміщена на окремо виділеному засобі. Приклад матриці зображено на рисунку 3.4. В даному прикладі колонками матриці є групи адресатів, рядами – адресантів або джерел трафіку. Сама політика задається в місцях перетину адресатів та адресантів, певних «комірках» матриці. Такий підхід може застосовувати як найпростіші правила (дозволити/заборонити), так і прописувати для кожної пари більш складні значення, застосувавши деталізацію трафіку або джерела портів. Різниця тут лише в умові перевірці, тобто мітка SGT.

	Destinations			
Sources	Company Database	Public Cloud	External Partner	Internet
Guest	Deny	Deny	Deny	Permit
Employee BYOD	Permit	Define Access	Deny	Web Apps
Building Mgmt.	Permit	Deny	Deny	Deny
Employee	Permit	Permit	Define Access	Permit

Рисунок 3.4 – Приклад матриці Cisco TrustSec Policy Management Matrix

Не є обов'язковою умовою для роботи заповнення усіх комірок матриці. Пусті пари будуть оброблятися стандартною політикою, будь то дозволити весь трафік або заборонити. Клітинки, де присутні введені умови, слідують налаштованим в SGACL правилам. Якщо умови для виконання заданої політики не виконуються в повному обсязі, тоді застосовується стандартна політика.

Варіант матриці доступу замість списків та динамічне призначення міток дає можливість реалізовувати політики безпеки централізовано, зручно та зменшує можливі механічні помилки операторів. Механізми TrustSec поширюють мережею в автоматичному режимі як мітки SGT, так і правила SGACL.

Мітки SGT розсилаються мережею декількома способами: безпосередньо від вузла до вузла, додаючись до заголовку фрейму або пакету трафіка, з допомогою окремого спеціалізованого протоколу SGT Exchange Protocol, що працює поверх протоколу TCP, за допомогою власної технології Cisco – Platform Exchange Grid (або скорочено pxGrid).

Перший спосіб є найбільш орієнтованим на масштабованість та зручність застосування, оскільки мітки передаються разом з потоком трафіку. Недоліком цього є те, що пристрій має бути спроможним працювати з доданими в трафік мітками. Таку можливість підтримують не всі пристрої, особливо якщо мережа працює з кадрами Ethernet, що вимагає впровадження в апаратну складову інтегральних мікросхем відповідних механізмів. Також TrustSec може не бути реалізовано в частині пристроїв локальної мережі. В такому випадку перед інженерами постане проблема об’єднання окремих ізольованих областей інфраструктури TrustSec між собою. Для таких випадків існує другий з запропонованих варіантів – протокол SXP. Варіант з застосуванням Cisco pxGrid рекомендовано застосовувати для інтеграції в систему TrustSec інших рішень від Cisco та її партнерів в сфері інформаційної безпеки.

На сьогодні Cisco TrustSec реалізована в багатьох пристроях, що знаходяться в портфоліо компанії. Серед них можна виділити комутатори та маршрутизатори корпоративного та промислового рівнів, обладнання для ЦОД, міжмережеві екрани і багато інших. Незважаючи на те, що TrustSec є фірмовою розробкою Cisco, в 2014 р компанія опублікувала інформаційний драфт IETF, в якому описано механізм протоколу Source-group tag eXchange Protocol (SXP), чим дали доступ до функціоналу TrustSec іншим виробникам обладнання зв’язку.

Стосовно поширення правил SGACL, то кожен активний пристрій локальної мережі автоматично завантажує їх з сервера Cisco ISE. Зміни, що внесено до матриці TrustSec, можуть бути негайно поширені в мережі за допомогою

відповідної консольної команди інтерфейсу Cisco ISE. Також передбачено можливість оновлення політики TrustSec локально на пристрої за допомогою необхідної команди в CLI. Кожен пристрій також може автоматично дати запит серверу на оновлення політики безпеки у зв'язку з обмеженим часом дії.

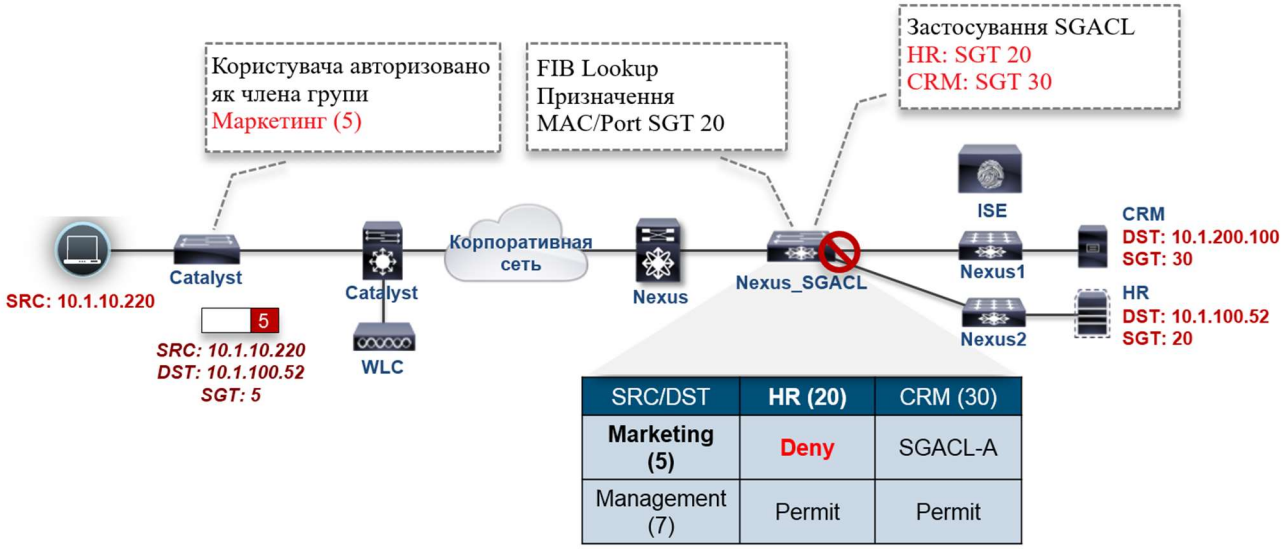

Рисунок 3.5 – Приклад застосування TrustSec

Розглянемо роботу технології TrustSec на прикладі (рис. 3.5). Користувач, що підключився до мережі, пройшов процедуру автентифікації та авторизації в мережі за допомогою сервера Cisco ISE. Результатом стало призначення цьому користувачу мітку групи 5 Маркетинг. Комутатор рівня доступу призначає кожному пакету, що надходить на його порт від цього пристрою, мітку SGT 5. Для спрощення приймемо, що уся мережа є доменом TrustSec, а політики застосовуються лише на інтерфейсах серверного комутатора Nexus_SGACL, до якого підключено комутатори Nexus1 і Nexus2 (однак зауважимо, що використання політик в цілому може не бути обмежено лише одним пристроєм чи групою пристроїв). Адміністратор створив на сервері Cisco ISE і розповсюдив в домені TrustSec політику доступу, зображену в таблиці на рисунку 3.5.

Допустимо, що користувач надіслав пакет, де отримувачем є адреса серверу групи менеджменту персоналу (HR), якому присвоєну мітку відповідної групи. Дані проходять через мережу і потрапляють на порти комутатора Nexus_SGACL, що перевіряє трафік та застосовує політики безпеки, що завчасно завантажено з сервера Cisco ISE. За правилами, матриці прийнято читати зліва направо та згори донизу. Робота обладнання не є виключенням, тому комутатор застосовує правило

заборони для будь-якого трафіку з групи Маркетинг до групи HR. Під час застосування правила пакет видаляється, виконуючи вимогу політики безпеки, а користувач або отримує повідомлення про недоступність ресурсу, або відповідне повідомлення про розірвання/заборону з’єднання.

SGACL застосовується обладнанням апаратно зі швидкістю роботи інтерфейсів та каналу в цілому. Саме тому технологія TrustSec, яка використовує мітки, не впливає на якість та продуктивність каналів зв’язку.

Таким чином, Cisco TrustSec надає механізми динамічного розподілу політик безпеки та контролю доступу усій мережі, в тому числі дозволяє застосування централізованої політики для усіх можливих видів доступу до мережі, включно з VPN.

Нагадаємо, що Cisco TrustSec працює не лиже з мережевими рішеннями компанії і сервером Cisco ISE. Інтерфейс pxGrid TrustSec дозволяє інтеграцію технології до інших рішень від Cisco та її партнерів. Зокрема можна виділити інтеграцію з Cisco Firepower, Cisco Web Security Appliance (WSA), Cisco Stealthwatch і т.д. Такий механізм дозволяє створення досить точних політик доступу до додатків, що працюють на прикладному рівні моделі OSI за допомогою цілого арсеналу можливостей міжмережевих екранів Cisco Firepower. Або ж створити привілейований доступ до веб-ресурсів, використовуючи можливості Cisco WSA. Чи розробити політики Stealthwatch з метою боротьби з загрозами, враховуючи приналежність користувача до тої чи іншої групи. Найцікавішою можливістю є автоматизація використання Cisco Rapid Threat Containment. Тут Cisco Stealthwatch або Cisco Advanced Malware Protection виявляють загрозу ІБ (наприклад, інфікований комп'ютер) і передають на сервер Cisco ISE запит обмеження доступу окремому вузлу або групі вузлів з допомогою функціоналу TrustSec (динамічне приміщення в карантин).

Також TrustSec, фактично існуючи як технологія програмної сегментації, легко інтегрується з архітектурою програмно-описаного ЦОД Cisco Application Centric Infrastructure (ACI). Подібний тип інтеграції описує відповідність між групами користувачів та компонентами серверних додатків, що поділені на групи

Endpoint Groups (EPG) технології ACI. Результатом є створення наскрізних політик безпеки для охоплення як мережної, так і серверної частин корпоративної системи.

Обидві технології – TrustSec і ACI – спрямовані на оптимізацію та автоматизацію процесів в областях безпеки і ЦОД. В даному застосуванні технології працюють в симбіозі, доповнюючи одна одну і пропонуючи додаткові вигоди від застосування їх разом.

Розглянемо декілька типових завдань відділів ІТ та ІБ та порівняємо результати рішення завдань у випадках, коли сегментація зроблена традиційними методами та за допомогою технології TrustSec.

Для подібності рішень припустимо, що в обох випадках процедури авторизації проходили з застосуванням виділеного серверу, де застосовується служба Microsoft Active Directory.

Ізоляція трафіку для прикладу виконується створенням віртуальних топологій та розробки списків доступу для традиційного варіанту мережі, а для мережі домену TrustSec використовуються стандартні для технології мітки SGT.

Завдання контролю доступу для традиційної мережі вирішується лише списками доступу. Мережа з використанням TrustSec використовує можливості списків доступу на базі міток, що поширюється мережу з виділеного сервера Cisco ISE.

Обумовимо, що для даного прикладу традиційна мережа підтримує можливості віртуалізації, утворення VLAN, підмереж і т.д., а сценарій з доменом має весь доступний функціонал TrustSec.

Виходячи з заданих умов та функціональних можливостей обох описаних технологій, можна виділити наступні переваги TrustSec:

- значне зниження часу та праці на внесення змін;
- зниження ймовірності простою мережі, недоступності ресурсів, пов’язаних з цим збоїв бізнес-процесів та можливих інцидентів ІБ, що виникають по причині механічних помилок інженера;
- вступ в силу нових політик доступу без необхідності очікування;
- зміна статичного контролю доступу на динамічний;
- автоматизована сегментація мережі;

- непряма оптимізація шляхів передачі трафіку між групами користувачів.

Ефект від впровадження TrustSec тим більше, чим більше динаміки в конфігурації закритих груп користувачів компанії, тому що TrustSec автоматизує ці зміни замість трудомісткої ручної роботи.

Також TrustSec дозволяє вирішити проблеми сфери кібербезпеки, що виникають в процесі сегментації мережі традиційними способами. Для більш чіткого розмежування груп користувачів та пристроїв за допомогою традиційних методів необхідно створити таку кількість топологій, яка покриватиме запити кожного користувача. Але чим більше груп, тим більша кількість топологій, відповідно зростає трудомісткість процесів налаштування та адміністрування. Результатом стане утворення такої кількості віртуальних груп та підмереж, яка буде неоптимальною з точки зору інформаційної безпеки. Спрощення топології мережі може дійти компромісу між безпекою та кількістю топологій. Але такий варіант не йде на користь безпеці мережі. На противагу цьому мережа TrustSec дозволяє уникнути подібних обмежень, утворюючи поділ на оптимальну кількість логічних груп користувачів, не наносячи шкоди безпеці.

Крім того, технологія TrustSec підвищує рівень безпеки за рахунок суворої взаємної автентифікації елементів мережевої інфраструктури та надає можливість шифрування трафіку на канальному рівні.

Перераховані та описані вище переваги Cisco TrustSec, порівняно з традиційними підходами, забезпечують значне зниження збитків, що пов’язані з інцидентами ІБ, та ймовірність виникнення самих інцидентів.

Оскільки TrustSec дозволяє більш точний розподіл груп, то в разі виникнення інцидентів ІБ очікуваний збиток буде набагато меншим, порівняно з мережею, де використано традиційні підходи. З цієї ж причини технологія заощаджує час на дослідження та усунення наслідків події інформаційної безпеки.

З цього можна виділити ще одну перевагу використання домену TrustSec. Спеціалісти можуть усунути наслідки події без переривання доступу до ресурсів мережі. Особливо важливо та затребувано це буде для, наприклад, привілейованих користувачів. Умовно, при зараженні ПК відділу бухгалтерії зберігається

можливість їх роботи за рахунок присвоєння їм мітки карантинної зони, при цьому ризик зараження пристроїв інших відділів зводиться до мінімуму.

Перевагою сегментації користувачів інструментами TrustSec також є те, що при виникненні події ІБ для розслідування та звітності необхідно дослідити та проаналізувати меншу кількість робочих станцій, що прискорить та полегшить роботу відповідного підрозділу та зменшить час простою техніки та підрозділу, що постраждав від атаки.

ВИСНОВКИ

В дипломній роботі проаналізовано одного з лідерів ринку телекомунікацій Cisco Systems, а також розроблено варіант топології мережі з застосуванням рішень цього виробника. Як окремий важливий елемент створення локально-обчислювальної мережі підприємства розглянуто підхід до сегментації на основі Cisco TrustSec. Розглянуто типові завдання сегментування мережі, завдання IT та ІБ. Розглянуто також варіант топології мережі стандартного типу з захистом на периметрі мережі та його недоліки. Докладно аналізуються нові можливості та переваги для бізнесу, які пропонує Cisco TrustSec.

Для сучасного бізнесу характерна дедалі більша динаміка. Мережа, а також реалізовані в ній політики, повинні оперативно підлаштовуватися під вимоги бізнесу, що змінюються. Критично важлива і належна робота бізнес-процесів, що спираються на мережу та залежать від вибору обладнання мережі, сегментації LAN та організації захисту. Будь-які зміни політики мають бути реалізовані не лише швидко, а й надійно. Тому традиційні засоби сегментації, розглянуті у роботі, вже не відповідають запитам бізнесу сьогоднішнього та завтрашнього днів. Підтримувати ці запити можна за допомогою сучасної технології сегментації мережі Cisco TrustSec.

TrustSec відповідає сучасним вимогам бізнесу та пропонує інструментарій, що реалізує зміни середовища сегментації швидко та надійно за рахунок автоматизації та зведення до мінімуму «людського фактору». Окремо варто звернути увагу, що дана технологія є частиною екосистеми Cisco, що ставить вимогу до монобрендовості мережевої інфраструктури в її критичних вузлах.

У результаті Cisco TrustSec пропонує бізнесу виграш, як мінімум, у трьох областях:

Зниження витрат. Ефект Expected Value за рахунок зниження ризиків ІБ та зниження ризиків простоїв бізнес-процесів. Розглядати цей фактор варто лише в контексті дистанції, оскільки миттєві фінансові витрати будуть вище, ніж подібні рішення конкурентів.

Зменшення робочого часу. Виражений у людино-годинах виграш робочого дня персоналу з допомогою зниження обсягів рутинної роботи. З'являється можливість зосередитись на вирішенні стратегічних, творчих завдань, які часто відкладаються або взагалі не виконуються.

Оптимізація часу. Виражене у тижнях чи днях загальне прискорення запуску нових сервісів/додатків та отримання бізнес-результатів, які тією чи іншою мірою спираються на сегментацію мережі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Gartner. Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure. 6 March 2024. Tim Zimmerman, Christian Canales, Nauman Raja, Mike Leibovitz [Електронний ресурс] – Режим доступу: https://www.exclusive-networks.com/ro/wp-content/uploads/sites/44/2024/03/Gartner-Reprint.pdf

2. Committee on National Security Systems (CNSS). Glossary. CNSSI No. 4009. April 6, 2015 [Електронний ресурс] – Режим доступу: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

3. Про внесення змін до Закону України "Про захист інформації в автоматизованих системах" [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2594-15#Text

4. Gartner. Gartner Information Technology Glossary [Електронний ресурс] – Режим доступу: https://www.gartner.com/en/information-technology/glossary

5. Що таке ERP системи, кому вони потрібні і навіщо? [Електронний ресурс] – Режим доступу: https://ua.ifsukraine.com/chto-takoe-erp-sistemy-komu-oni-nuzhny-i-zachem/

6. CRM (електронний словник компанії SendPulse) [Електронний ресурс] – Режим доступу: https://sendpulse.ua/support/glossary/crm

7. Клієнт-серверна архітектура [Електронний ресурс] – Режим доступу: https://training.qatestlab.com/blog/technical-articles/client-server-architecture/

8. Ivan Zmerzlyi. Клієнт-серверна архітектура та ролі серверів [Електронний ресурс] – Режим доступу: https://medium.com/@IvanZmerzlyi/клієнт-серверна-архітектура-та-ролі-серверів-9893d8048229

9. IP телефонія: що це, та як вона відрізняється від звичайної телефонії? [Електронний ресурс] – Режим доступу: https://blog.globalbilgi.com.ua/ip-telefoniia-shcho-tse-ta-vidminnosti-vid-zvychainoi-telefonii/

10. Що таке локальна мережа і навіщо вона потрібна? [Електронний ресурс] – Режим доступу:

https://itedu.center/ua/blog/articles/lan_wan_man/?srsltid=AfmBOooU53U_8SI2gKUW6vOLbIWJA_GhoeT-Jt_d09Icz_19fV_JVi85

11. Ethernet. Енциклопедія LanMarket. [Електронний ресурс] – Режим доступу: https://lanmarket.ua/ua/entsiklopediya/telekommunikatsionnye-tekhnologii/ethernet.html

12. Wi-Fi. Матеріал з Вікіпедії — вільної енциклопедії. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Wi-Fi

13. Industrial and outdoor wireless solutions [Електронний ресурс] – Режим доступу: https://www.cisco.com/site/us/en/products/networking/industrial-wireless/index.html

14. Secure Wireless LAN [Електронний ресурс] – Режим доступу: https://www.fortinet.com/solutions/small-business/wireless

15. White Paper: Internal Segmentation Firewall: Security Where You Need It, When You Need It [Електронний ресурс] – Режим доступу: https://lansys.com.ua/wp-content/uploads/2019/01/Fortinet_ISFW_overview_en.pdf

16. Cisco Secure Firewall At-a-Glance [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/at-a-glance-c45-736624.html

17. Cisco Secure Firewall Management Center (formerly Firepower Management Center) Data Sheet [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html

18. Discover the Benefits of Pre-Owned HPE Aruba Networking [Електронний ресурс] – Режим доступу: https://www.curvature.com/resources/blog/discover-the-benefits-of-preowned-hpe-aruba-networking/

19. Wireless Access Points and Edge [Електронний ресурс] – Режим доступу: https://www.juniper.net/us/en/products/access-points.html

20. Switch on the power of your network [Електронний ресурс] – Режим доступу: https://www.cisco.com/site/us/en/products/networking/switches/index.html

21. Cisco 1000 Series Integrated Services Routers Data Sheet [Електронний ресурс] – Режим доступу:

https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-integrated-services-routers-isr/datasheet-c78-739512.html

22. Cisco Wireless 9176 Series Access Points Data Sheet [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/wireless-9176-series-acc-point-ds.html

23. Desk Phone 9800 Series Data Sheet [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/ip-phones/desk-phone-9800-series-ds.html

24. Alex Samonte. Network Security Reference Architecture [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/document-library/ra-network-security-reference-architecture.pdf

25. Cisco TrustSec Configuration Guide [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/configuration_guide/cts/b_179_cts_9300_cg/cisco_TrustSec_overview.html

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)