**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

ДОПУСТИТИ ДО ЗАХИСТУ:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

# ПОЯСНЮВАЛЬНА ЗАПИСКА

**дипломної роботи**
***бакалавра***
(назва ступеня)

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

**спеціальність** 125 Кібербезпека
(код і назва спеціальності)

**освітня програма** Кібербезпека
(назва освітньої програми)

**на тему:** «Засоби захисту розподіленої інформаційної системи державного підприємства»

**Виконавець:** студент IV курсу, групи КБ-42

_____ **Валерія СОЛОДОВНИК.**
(підпис) (ім'я прізвище)

| | **Прізвище, ініціали** | **Підпис** |
|---|---|---|
| **Керівник** | Андрій Фесенко | |

| | | |
|---|---|---|
| **Нормоконтроль** | Сергій Даков | |

**Київ 2022**

**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО:**
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

# ЗАВДАННЯ
## на виконання дипломної роботи

**спеціальності** 125 Кібербезпека
(код і назва спеціальності)

**освітньої програми** Кібербезпека
(назва освітньої програми)

**Студентові** **КБ-42** **Валерія СОЛОДОВНИК**
(група) (ім'я прізвище)

**Тема дипломної роботи** Засоби захисту розподіленої інформаційної системи державного підприємства

### 1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

### 2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Структури, архітектури, апаратні засоби функціонування систем, набір програмних рішень для підвищення рівня безпеки, розробки інформаційних систем

### 3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Нормативно-правова база у сфері захисту інформації, структура інформаційної системи, архітектурний стиль побудови системи, основні вразливості інформаційних систем, апаратний та програмний захист систем, топологія системи Державного відприємства, рекомендації для розробки архітектури

### 4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

**Практична цінність** створення топології інформаційної системи з впровадженням засобів захисту і моніторингу та рекомендації з їх розробки.

**5. ДАТА ВИДАЧІ ЗАВДАННЯ**

Дата видачі завдання: 29.10.2021 року

Завдання видав _____ (підпис) Андрій ФЕСЕНКО (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Валерія Солодовник (ім'я, прізвище)

**КАЛЕНДАРНИЙ ПЛАН**

| № п/п | Найменування етапів робіт | Строки виконання робіт (початок-кінець) | Відмітка про виконання |
|---|---|---|---|
| 1 | Уточнення постановки задачі | 29.10.2022 – 27.01.2022 | *виконано* |
| 2 | Аналіз літератури | 28.01.2022 – 11.02.2022 | *виконано* |
| 3 | Розгляд структури інформаційних систем | 12.02.2022 – 24.02.2022 | *виконано* |
| 4 | Дослідження основних вразливостей | 25.02.2022 – 24.03.2022 | *виконано* |
| 5 | Дослідження недоліків проектування інформаційних систем | 25.03.2022 – 07.04.2022 | *виконано* |
| 6 | Відбір та аналіз актуальних технічних рішень | 08.04.2022 – 20.04.2022 | *виконано* |
| 7 | Пошук та розгляд необхідного програмного забезпечення | 21.04.2022 – 05.05.2022 | *виконано* |
| 8 | Розробка архітектури інформаційної системи для державного підприємства | 06.05.2022 – 20.05.2022 | *виконано* |
| 9 | Обгрунтування впровадження засобів захисту для інформаційної системи | 21.05.2022 – 04.06.2022 | *виконано* |
| 10 | Оформлення пояснювальної записки | 05.06.2022 – 08.06.2022 | *виконано* |
| 11 | Підготовка до захисту | 08.06.2022 – 13.06.2022 | *виконано* |

Завдання видав _____ (підпис) Андрій ФЕСЕНКО (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Валерія СОЛОДОВНИК (ім'я, прізвище)

# РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 60 сторінок, включає в себе зміст, вступ, три розділи дипломної роботи, висновки та список джерел. Крім того, робота містить 2 додатки із загальною кількістю сторінок 3. У пояснювальній записці дипломної роботи міститься 10 рисунків.

*Метою роботи* є розробка топології розподіленої інформаційної системи для державного підприємства.

Для досягнення зазначеної мети поставлено наступні завдання:

- дослідити структуру розподіленої інформаційної системи;
- провести аналіз найбільш поширених вразливостей, для розподілених інформаційних систем;
- запропонувати актуальні програмні та апаратні рішення для побудови системи ;
- побудувати топологію інформаційної системи для державного підприємства з урахуванням підібраного програмного та апаратного забезпечення;
- виробити рекомендації для систем, стабільність роботи яких є значущою для фукціонування усієї організації.

*Об’єктом дослідження* є процес побудови тополоії та мінімізація вразливостей, притаманних розподіленим системам.

*Предметом дослідження* є методи побудови захищених розподілених інформаційних систем.

*Практичною цінністю* отриманих результатів є створення топології інформаційної системи з впровадженням засобів захисту та моніторингу для забезпечення безпеки. Внесення пропозицій щодо імплементації різного роду програмних засобів для підвищення рівня безпеки цільового об'єкту.

*Результати здійснених у дипломній роботі досліджень можуть бути використані:* як основа для подальшого розширення структури державного підприємства, базис для імплементації та оновлення програмного забезпечення для розширення функцій безпеки, підвищення відмовостійкості та продуктивності процесів у системі.

*Напрямки подальших досліджень:* покращення продуктивності інформаційнох системи, економічна доцільність впровадження новішого апаратного забезпечення, сегментація системи та практична необхідність даного рішення, розробка та налаштування політик доступу до сегментів системи, пошук оптимальних варіантів реалізації критерію підвищенної відмовостійкості для критичних вузлів системи.

*Ключові слова*: розподілена інформаційна система, вразливості, топологія, архітектура, захист інформації, безпека, міжмережний екран, функціонування системи, моніторинг, DMZ, vlan, технічний захист, програмний захист, апаратна складова, програмна складова, інфраструктура, відмовостійкість, структурний підрозділ, реплікація, система сховищ, сервери, комутаційне обладнання.

# СКОРОЧЕННЯ

| | | |
|---|---|---|
| OSI | – | Open Systems Interconnection |
| VPN | – | Virtual Private Network |
| NAT | – | Network Address Translation |
| IT | – | Information Technology |
| ASIC | – | Application-specific integrated circuit |
| ICMP | – | Internet Control Message Protocol |
| TCP | – | Transmission Control Protocol |
| UDP | – | User Datagram Protocol |
| IGMP | – | Internet Group Management Protocol |
| DNS | – | Domain Name System |
| KVM | – | Kernel-based Virtual Machine |
| SSH | – | Secure Shell |
| API | – | Application Programming Interface |
| ACL | – | Access Control List |
| NFIPS | – | Next Generation Intrusion Prevention Systems |
| AMP | – | Advanced Malware Protection |
| FTP | – | File Transfer Protocol |
| DNS | – | Domain Name System |
| IP | – | Internet Protocol |
| SIEM | – | Security information and event management |
| ADC | – | Application Deliver Controllers |
| CFW | – | Thunder Convergent Firewalls |
| DMZ | – | Demilitarized Zone |
| VLAN | – | Virtual Local Area Network |
| FTD | – | First Time Deposit |
| DDoS | – | Distributed denial-of-service attack |
| MITM | – | Man in the middle |
| WAF | – | Web Application Firewall |
| SDWAN | – | Software-defined networking |
| NFV | – | Network Functions Virtualization |
| ІС | – | Інформаційна система |
| РІС | – | Розподілена інформаційна система |
| ЗІ | – | Захист інформації |
| ПЗ | – | Програмне забезпечення |

# ЗМІСТ

# ВСТУП

Разом зі стрімким розвитком інформаційних технологій, а з ним й інформаційних систем, зростає не тільки кількість та складність атак але і ускладнюється процес визначення алгоритму побудови інформаційної системи з дотриманням основних правил та кращих практик .

На поточний момент вишуканість та кількість витончених комбінацій атак на державні информаційні системи вражає. На фоні нестабільного геополітичного стану в Європі, українські ресуси дедалі частіше стають жертвами атак з метою дестабілізації спокою всередині країни [10].

Сьогодні більший відсоток зусиль спрямовано на розробку якісних алгоритмів та механізми захисту. Набагато менше уваги приділяється дослідженню саме того, якиою повинна бути топологія системи, які мають бути застосовані засоби захисту, їх характер та кількість. Фактично, на поточний момент, важко віднайти єдиний алгоритм створення ієрархії інформаційної системи, особливо, якщо мова іде про державну структуру. Це відбувається переважно через різноманіття функцій, що покладені на об’єкт захисту та вразливість поточної архітектури до різних видів атак. Проте застосування найефективніших практик розробки топології ІС, є позитивним вектором розвитку підходів до їх проектування.

Практична необхідність проведення дослідження обумовлена наступними причинами:

По-перше, фахівцям із захисту інформаційних систем необхідно чітко розуміти, який характер загроз притаманний ІС різного призначення.

По-друге, базуючись на попередньому твердженні можна створювати ІС з застосуванням найкращого апаратного та програмного забезпечення для мінімізації цих загроз поряд із загальними засобами забезпечення безпеки.

Таким чином проектування архітектури інформаційної системи, використовуючи новітні технічні засоби та сучасне програмне забезпечення, є актуальним завданням.

# РОЗДІЛ 1
# АНАЛІЗ ІНФОРМАЦІЙНИХ СИСТЕМ, ЇХНЬОЇ СТРУКТУРИ ТА ВРАЗЛИВОСТЕЙ

Сучасна IT-індустрія характеризується стрімким зростанням кількості інформаційних систем, побудованих з використанням різноманітних підходів і технологій. Цю тенденцію легко пояснити прогресивним розвитком комп'ютерних структур і компонентів цих систем. Проте існують і проблемні ситуації, коли державні організації, навіть маючи найсучасніше обладнання, можуть гальмувати цей розвиток. Основна відмінність розподілених систем від централізованих - це, безумовно, підхід до їх побудови [1].

## 1.1 Види та структури інформаційних систем

У сучасному світі комп’ютери рідко працюють ізольовано. Метою їхньої співпраці є зв’язок, обробка, зберігання та передача інформації. Найбільш зручним форматом даної взаємодії є розробка та створення інформаційних систем. Таким чином, під терміном інформаційна система (ІС), будемо розуміти організаційно-технічну систему, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів [11].

Коли розкидані різними географічними континентами системи взаємодіють одна з одною, такий формат взаємодії називається розподіленими системами. Для того, щоб окреслити дане поняття різноманітні дослідники використовували увесь спектр доступних визначень. Кулуріс та інші визначили розподілену систему, як «систему, де апаратні та програмні компоненти встановлені в географічно розосереджених комп’ютерах, які координують та співпрацюють між собою, передаючи повідомлення між ними [2].

Таненбаум і Ван Стін визначили розподілену систему як «сукупність систем, яка представляється користувачам як єдина система» [3]. З визначення Таненбаума

можна уявити, що розподілена система відноситься до програмної системи, а не до апаратних засобів, які беруть участь у створенні системи. Об’єднавши ці визначення, можна стверджувати, що розподілена система – це програма, яка зв’язується з кількома розсіяними апаратними та програмними засобами для координації дій багатьох процесів, що виконуються на різних автономних комп’ютерах через мережу зв’язку, так що всі компоненти апаратного та програмного забезпечення співпрацювати разом для виконання набору суміжних завдань, спрямованих на досягнення спільної мети.

Більшість людей вважає розподілену систему і мережу комп’ютерів однаковими. Але ці два терміни означають дві різні, але пов’язані речі. Комп’ютерна мережа – це взаємопов’язана сукупність автономних комп’ютерів, які спілкуються між собою. Користувач, який використовує комп’ютерну мережу, розуміє, що він використовує різні ресурси, що лежать на різних комп’ютерах, оскільки комп’ютерна мережа не приховує існування кількох комп’ютерів.

Але розподілена система, з іншого боку, створює відчуття, що користувач працює на одному однорідному більш потужному комп’ютері з більшими ресурсами. Існування кількох автономних комп’ютерів є прозорим для користувача, оскільки програма розподіленої системи, яка працює на комп’ютерах, вибирає відповідні комп’ютери та розподіляє робочі місця без спеціального втручання користувача [3].

Окрім надійності, метою побудови розподілених ІС є:

- прозорість;
- відкритість;
- продуктивність;
- масштабованість.

На рисунку 1 схематично показано структура розподіленої архітектури.

Основними елементами архітектури, показаними на рисунку 1, є:

Головний центр обробки даних - відповідає за зберігання та обробку всіх даних інформаційної системи

Центр обробки резервних даних - відповідає за відмовостійкість.

Користувачі - клієнтське програмне забезпечення (ПЗ) за технологією «товстий клієнт».

Сервер баз даних, сервер додатків у вузлі - займається зберіганням, обробкою всіх даних у конкретному вузлі (локальна база даних у вузлі).

Необхідні компоненти системи розподіленої архітектури також включають:

Телекомунікаційна мережа - забезпечує підключення та обмін даними між різними вузлами. Наприклад, Інтернет або корпоративна мережа.

Система інформаційної безпеки - відповідає за захист кожного вузла системи.

Сервери обміну даними - займаються реалізацією обміну даними між вузлами системи [1, 2].

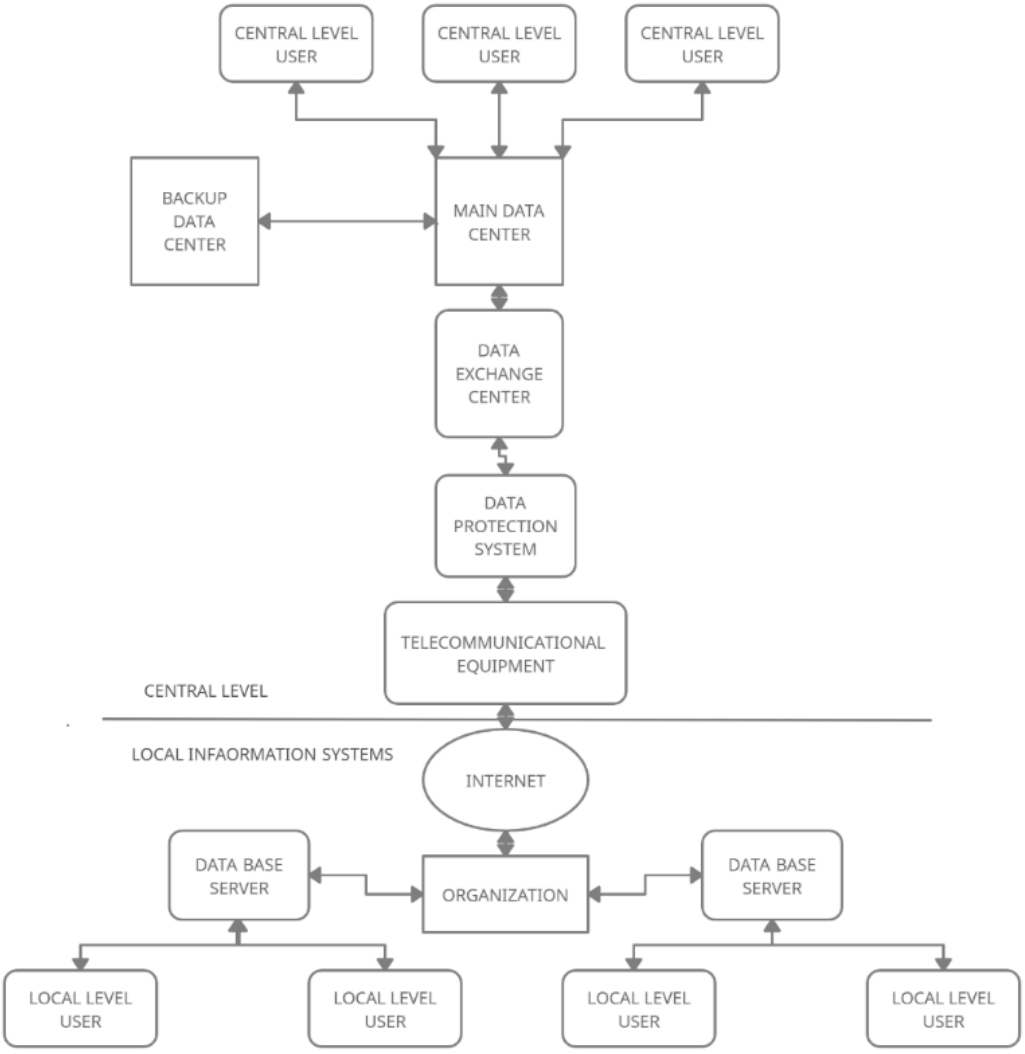



Рис. 1. Схема розподіленої архітектури інформаційної системи.

Очевидними перевагами цієї моделі є те, що їй не потрібно мати постійне телекомунікаційне обладнання для зв’язку з центральним рівнем. Ми вміємо передавати пакети не тільки по телекомунікаційній мережі, а й по зовнішніх носіях. Також інтерфейс «товстого клієнта» більш ергономічний, ніж веб-інтерфейс, особливо під час масових операцій введення даних через інтерфейс користувача, хоча зараз ця перевага не є значною.

Поряд з позитивними характеристиками використання розподіленої архітектури є негативні. Першим недоліком є те, що кожен вузол системи має локальні бази даних, що ускладнює обмін інформацією між ними. Проте проблема не лише в обміні даними, а й в оновленні та технічному забезпеченні експлуатованих систем.

Наявність складних програмних елементів, таких як сервери баз даних, програми, обмін і робочі станції, не полегшує процес виконання системних завдань. Слід зазначити, що для такого елемента, як система управління базами даних, яка є однією зі складових системи, існують варіанти, як безкоштовні, так і постачальники, що в свою чергу, при виборі другого варіанту тягне за собою значні фінансові витрати на впровадження, підтримка та обслуговування.

Необхідно йти в ногу з постійним оновленням версій усіх компонентів, що в порівнянні з централізованою архітектурою є значною статтею фінансових і тимчасових витрат. Це одне з найскладніших завдань, особливо під час надзвичайних ситуацій, і мало залежить від алгоритмів обміну даними. Інша проблема полягає в тому, що розподілена архітектура має меншу гнучкість та ефективність під час створення нових вузлів у своїй архітектурі або їх переміщення.

Всі ці аспекти впливають на можливість забезпечення необхідного рівня інформаційної безпеки системи, оскільки на кожному вузлі все залежить від системного адміністратора або менеджера, який може не мати достатнього рівня відповідальності за правила роботи систем безпеки. Також виникають проблеми, коли виникає потреба розгорнути системну точку поза фізичними межами організації. Крім того, підтримання актуальності інформації, що поширюється на центральному рівні, є складною концепцією для виконавців.

Тому на даний момент виділимо такі недоліки архітектури:

- У кожному вузлі є потреба в кваліфікованих системних адміністраторах;
- Надзвичайно висока вартість обладнання та ліцензування програмного забезпечення;
- Комплексна організаційна схема підтримки та адміністрування кожного елемента системи;
- Середні можливості для якісної інформаційної безпеки.

Таким чином, говорячи про новітні підходи до розробки інформаційних систем, слід торкнутися питання централізації системних архітектур. Архітектура централізованої інформаційної системи є логічним наслідком розвитку телекомунікаційних послуг, підвищення їх надійності та пропускної здатності, зниження вартості послуг передачі даних, широкого проникнення як у географічному сенсі, так і серед різних верств населення, бізнесу.

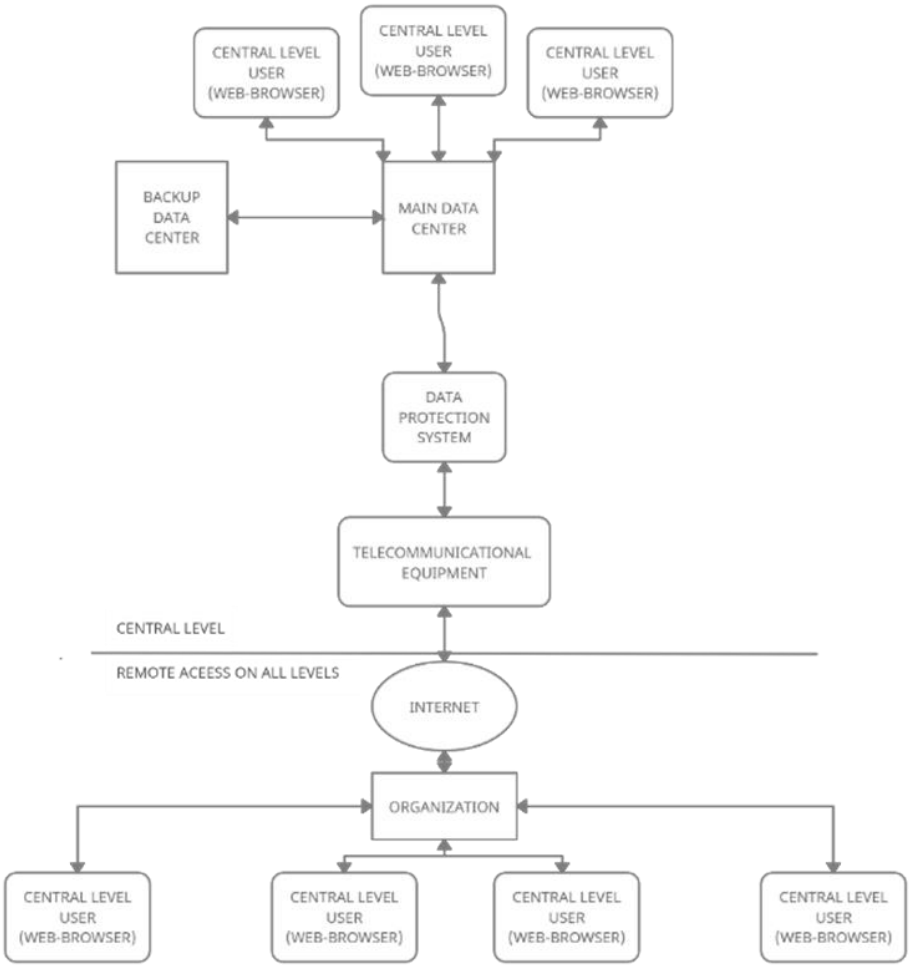



Рис. 2. Схема централізованої архітектури інформаційної системи.

На другому малюнку схематично показано архітектуру централізованої системи. Таким чином ми бачимо, що цей тип архітектури складається з потужного дата-центру, використання трирівневої архітектури та web-технологій.

Основними елементами централізованої архітектури є:

- Базовий центр обробки даних – відповідає за зберігання та обробку всіх даних інформаційної системи та взаємодію з віддаленими користувачами. Є критичним елементом.
- Центр резервного копіювання даних той самий. що стосується розподіленої архітектури. забезпечує відмовостійкість, резервне зберігання даних всієї системи на центральному рівні.
- Користувачі – це клієнтський інтерфейс, який забезпечує візуалізацію даних і взаємодію користувача з системою.
- Також необхідні елементи:
- Телекомунікаційна система, але тут вона вже забезпечує підключення до системи та обмін даними між віддаленими клієнтами;
- Система захисту інформації, яка є критичним елементом в архітектурі центрального рівня системи [1].

Щоб краще зрозуміти переваги цієї загальної архітектури, ось список, який найбільш повно їх описує:

- У централізованій архітектурі є одна база даних, з якою взаємодіють усі користувачі системи.
- На стороні клієнта немає складного програмно-апаратного комплексу. Тому, відповідно, значних фінансових витрат на їх обслуговування немає, оскільки єдиними необхідними елементами системи є операційна система та web-браузер. Зменшено перелік робіт з адміністрування станції та кількість кваліфікованих системних адміністраторів.
- Вищезгадана трирівнева архітектура – «сервер баз даних – сервер додатків – клієнт», дозволяє використовувати сучасні системи управління базами даних, web-браузер як середовище виконання програмного забезпечення. Відсутня також прямий доступ до центральної бази даних, що

значно знижує ризики її несанкціонованого зміни. Набагато простіше створювати нові вузли системи та реалізовувати віддалений доступ із клієнтських робочих станцій.

- Використовуючи єдиний набір програмного забезпечення для всіх користувачів незалежно від рівня, ми можемо говорити про єдиний спосіб доступу до системи, контроль прав, якими користується користувач на доступ і, відповідно, зниження витрат на розробку програмного забезпечення для системи.
- Централізована архітектура характеризується широким діапазоном масштабованості під час критичного навантаження системи.
- Слід також відзначити більшу керованість порівняно із розподіленою системою, оскільки забезпечити надійні організаційні процедури в одному центрі набагато простіше, ніж виконати всю процедуру на всіх рівнях системи.

Таким чином, централізована модель може значно спростити організаційно-технічні складові створення, впровадження, функціонування системи, а також інформаційну безпеку.

Слід зазначити, що наявність як розподіленої, так і централізованої архітектури, одним з найбільш ефективних варіантів захисту інформаційних систем є введення штату спеціаліста з комп'ютерної безпеки або створення спеціальних служб, як приватних, так і централізованих, на основі ситуації. Він зможе ознайомити працівників і зокрема спеціалістів департаменту інформаційної безпеки з минулими порушеннями та залучити їх до впровадження ефективних практик захисту даних.

Співробітників слід навчити основним правилам безпечної обробки даних та безпеки в Інтернеті, оскільки більшість зловмисників активно використовують соціальну інженерію як засіб атаки на систему.

З вищесказаного випливає, що використання двофакторної аутентифікації має бути передумовою для надання доступу користувачеві, незалежно від типу

архітектури. У той же час політика доступу на основі ролей до певних частин систем може бути ефективно реалізована.

Для цих типів архітектури варто звернути увагу на таку технологію, як мікросегментація мережі за допомогою vlan. Йдеться про ізоляцію ресурсів від решти організації. Це дуже ефективний інструмент для відстеження дій в системі. Іншою гарною практикою може бути реєстрація дій, а потім їх надсилання до SIEM. Це допоможе адміністратору побачити, в який час, з якої частини системи були надіслані ті чи інші інструкції чи інформація та як це вплинуло на роботу системи [4, 5].

## 1.2 Вразливості інформаційних систем

Вразливості відносяться до конструктивних або експлуатаційних недоліків, які дають змогу зловмиснику потенційно скомпрометувати систему. Також, загроза відображає потенціал або імовірність того, що зловмисник завдасть шкоди або поставить під загрозу систему. Таким чином, слід відзначити, що вразливості розподіленої системи в цілому групуються на основі функціональних блоків, що визначають структуру розподіленої системи.

На високому рівні абстрагування атаки можуть бути пов'язані з компрометацією фізичних ресурсів, схеми зв'язку, механізмів координації, самих послуг, що надаються, і політик використання даних, що лежать в основі послуг.

1. Контроль доступу та управління посвідченнями особи.

Управління доступом або допуском визначає авторизовану участь ресурсу, користувача або служби в розподіленій системі. Це може включати в себе джерело даних і права доступу на читання / запис і використання даних протягом терміну використання служби. Потенційні загрози і наступні атаки включають в себе маскування або підробку ідентифікаційних даних для отримання прав доступу до даних. Вони також можуть включати атаки типу "відмова в обслуговуванні"(DoS), що призводить до недоступності розподілених ресурсів/служб. Варто підкреслити, що розподіл ресурсів часто тягне за собою більшу кількість точок для контролю

доступу, а також більше інформації, що передається в системі для підтримки контролю доступу, що збільшує поверхню атаки системи.

Об'єкт розподіленої системи (ресурс, служба, користувач або елемент даних) бере участь у розподіленій системі з фізичним або логічним ідентифікатором. Ідентифікатор, статично або динамічно виділяється, може бути ідентифікатором ресурсу, таким як ім'я ідентифікатора або число. Таким чином, діяльність, пов'язана з підробкою ідентифікаційних даних, являє собою ймовірну загрозу.

2. Передача даних

Загрози мережевого рівня охоплюють маршрутизацію, передачу повідомлень, способи взаємодії ресурсів, ініціювання відповіді на основі подій і загрози в стеку проміжного програмного забезпечення. Більш того, це можуть бути пасивні (підслуховування) або активні атаки (модифікація даних).

Типовим прикладом є атака "людина посередині" (MITM), при якій зловмисник вставляє себе між браузером жертви і веб-сервером, щоб встановити два окремих з'єднання між ними. Це дозволяє зловмиснику активно записувати всі повідомлення і вибірково змінювати дані, не викликаючи тривоги про підозрілу активність, якщо система не застосовує перевірку автентичності кінцевої точки.

3. Управління ресурсами системи

Ця критична група охоплює спектр загроз механізмам (зазвичай протоколам проміжного програмного забезпечення), які забезпечують координацію ресурсів. Це включає в себе, серед іншого, аспекти синхронізації, управління реплікацією, змін подання, упорядкування часу/подій, лінеаризованості, консенсусу і фіксації транзакцій.

4. Безпека даних

Оскільки розподілена система по суті оперує даними (в стані спокою або в русі) по всіх аспектах: пошуку даних, розподілу даних, зберігання даних або використання даних в сервісах, класичні властивості CIA (конфіденційність, цілісність і доступність) безпосередньо застосовуються до кожного елементу цієї системи.

Загрози конфіденційності включають загрози витоку інформації, такі як атаки по побічних каналах або атаки по прихованих каналах. Будь-яка затримка або відмова в доступі до даних є загрозою доступності. Аспекти цілісності стосуються будь-якого порушення коректності даних, такого як порушення узгодженості даних, що спостерігається розподіленими учасниками. Отже, вирішення проблеми безпеки елементів даних розподіленої системи вимагає прискіпливої уваги до згаданих вище загроз для ресурсів, служб контролю доступу, передачі даних, а також загроз для даних у вигляді шкідливих додатків, коду і вірусів.

### 1.3 Проектні вимоги до розподілених інформаційних систем

При створенні складних, розподілених інформаційних систем, проектуванні їх архітектури, інфраструктури, виборі компонентів і зв'язків між ними слід враховувати крім загальних (відкритість, масштабованість, переносимість, мобільність, захист інвестицій тощо) ряд специфічних концептуальних вимог, спрямованих на забезпечення безпеки функціонування [13]. Такими вимогами є зокрема те, що:

- системна архітектура повинна бути достатньо гнучкою для того, аби допусти просте, без кардинальних змін у структурі, розширення інфраструктури, оновлення конфігурації залучених до функціонування системи засобів, нарощування функціональних можливостей та ресурсів інформаційної системи відповідно до змін напрямку роботи та розширенням спектра завдань на виконання;
- є необхідність у забезпеченні безпечного функціонування системи під час різних загроз, актуальний та надійний захист даних від помилок проектування, руйнації або ж інформаційних втрат, а також авторизація користувачів, процес резервування даних та обчислювальних ресурсів, максимально швидке відновлення функціонування ІС;

- необхідно забезпечити вдосконалений, максимально простий доступ користувачів до сервісів і результатів роботи ІС базуючись на актуальних засобах графічного відображення та наочних користувацьких інтерфейсах;
- система повинна перебувати у постійному супроводі актуальної, максимально повної та деталізованої документації, що робить можливим та кваліфікованим експлуатацію і можливість розширення ІС.

Важливо наголосити, що системи безпеки, якими б потужними вони не були, самі собою не можуть гарантувати надійність програмно-технічного рівня захисту. Виключно перевірена архітектура здатна створити ефективне об'єднання сервісів, забезпечити керованість інформаційної системи, її здатність до розвитку і протистояння новим загрозам при цьому зберігаючи такі властивості, як висока продуктивність, простота і зручність використання [13].

На рисунку 3 можемо спостерігати архітектуру головного офісу підприємства, яке має в собі низку недоліків, що в подальшому можуть призвести до припинення або некоректного функціонування всієї системи або певних її складових. Слід зазначити, що мова зараз піде переважно про недалекоглядність архітектурного проекту, недостатня довершеність технічних компонентів, а саме таких пунктів, як відсутність демілітаризованої зони та недостатня кількість обладнання на певних рівнях функціонування системи.

До технічних характеристик системи слід відносити наступні:

- системна архітектура;
- масштабованість;
- надійність, особливо коли мова іде про роботу критичних бізнес додатків;
- можливість відновлення під час збоїв устаткування;
- присутність інструментів для резервного копіювання та архівування даних;
- наявність засобів захисту від навмисних і ненавмисних технічних атак.

Вищезазначені характеристики мають вплив на такі параметри системи, як можливість нарощування функціональних властивостей за необхідністю і збільшення кількості користувачів.

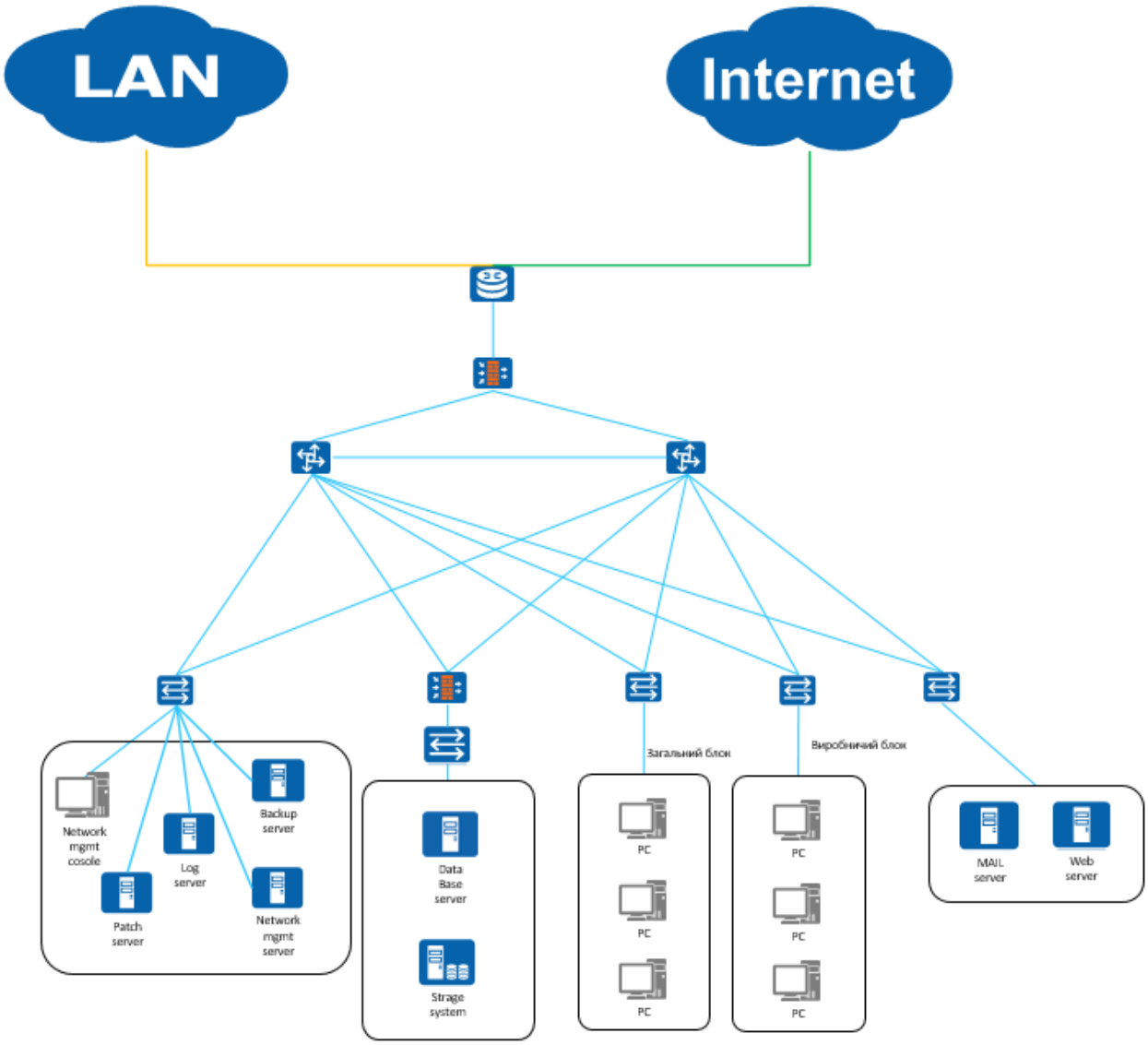



Рис. 3 Архітектура головного офісу

У даному прикладі (рис.3) відсутні демілітаризована зона для тих ресурсів, до яких повинен бути доступ як і з мережі інтернет так і з локального середовища. Немає також рішення для відмовостійкості, що забезечується дублювання критичних вузлів (комутаторів, файерволів). Відсутнє розподілення кінцевих пристроїв по віртуальним локальним мережам (vlan). Наступними недоліками є відсутність спеціального захисту для web-вузлів (WAF) та застарілість обладнання.

Додатковою умовою до інформаційної системи є можливість зручного пошуку інформації та роботи користувачів. Дана умова може стати суттєвим чинником при виборі та побудові системи. Також даний факор побічно свідчить про кваліфікацію

компанії-розробника. В той самий час гнучкість архітектури є важливим критерієм її вибору у випадку, якщо підприємство не збирається використовувати першопочатковий варіант імплементації, тобто якщо воно планує прогресувати, удосконалювати свою діяльність або просто працює в умовах постійної зміни зовнішніх умов (наприклад, державного законодавства). Відсутність системної гнучкості кінець кінцем приводить до необхідності постійного залучення коштовних фахівців фірми-розробника або інтеграційної компанії для налаштування системи автоматизації управління підприємством під постійно змінювані потреби діяльності [12].

## Висновки за розділом 1

Для того аби будувати ефективний захист необхідно розумітися на тому, що саме є об’єктом і які методи застосовуватимуться. Саме для цього у вище описаному розділі, було розглянуто архітектуру розподіленої системи її відмінності від централізованої системи, переваги, недоліки, вразливості та атаки, які можуть призвести до негативних наслідків роботи системи.

З огляду на те, що ІС в державних установах повинні обслуговувати велику кількість клієнтів, їх апаратне забезпечення, персональні обчислювальні потужності, дані є об’єктами захисту з боку адміністраторів.

# РОЗДІЛ 2
# ОСНОВНІ ТЕХНІЧНІ СКЛАДОВІ РОЗПОДІЛЕНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Для подальшого проектування безпечної розподіленої системи слід провести аналіз компонентів, що увійдуть до її складу. Серед низки необхідних системних елементів можна виділити ключові. Ними в свою чергу є:

- маршрутизатори
- комутатори;
- міжмережеві екрани;
- блейд шасі;
- сервери.

Залежно від призначення організації та послуг, які вона надає, елементи технічної складової можуть відрізнятися. Проте, якщо окреслити підготовку до побудови архітектури для штаб-квартири державної організації, слід зупинитися на ідеї про те, що обладнання повинно бути не тільки функціонально необхідним, але водночас і актуальним з точки зору можливості підтримки його постачальником. Тож, у даному розділі розглянемо необхідну апаратну частину, яка застосовуватиметься в майбутній топології.

## 2.1 Маршрутизатори

Маршрутизатор - це пристрій, який з'єднує дві або більше мереж або підмереж з комутацією пакетів. Він виконує дві основні функції: керує трафіком між цими мережами шляхом пересилання пакетів даних на призначені для них IP-адреси та дозволяє декільком пристроям використовувати те саме підключення до Інтернету.

Маршрутизатор Cisco 4461 Integrated Services Router об'єднує багато необхідних IT-функцій, включаючи мережеві, обчислювальні та ресурси зберігання. Високопродуктивні інтегровані маршрутизатори виконують кілька одночасних

служб, включаючи шифрування, управління трафіком і оптимізацію глобальної мережі, не знижуючи пропускної здатності даних. Таким чином є можливість активації нових послугг на вимогу за допомогою простої зміни ліцензії.

За останні кілька років відбулася швидка трансформація і впровадження цифрових технологій. Це створює навантаження на мережеві команди, що підтримують цю мінливу інфраструктуру, особливо при підготовці, управлінні, моніторингу та усуненні неполадок цих різноманітних пристроїв. Крім того, такі інновації, як програмно-визначена глобальна мережа (SDWAN), віртуалізація мережевих функцій (NFV), відкриті API і управління хмарою, показують великі перспективи в перетворенні IT-мереж організацій. Ця трансформація піднімає додаткові питання і проблеми перед IT-командами.


Рис. 4 Cisco 4461 Integrated Services Router

Архітектура цифрової мережі Cisco (cisco DNA) - це відкрита, розширювана, програмно-керована архітектура, яка забезпечує більш швидкі інновації, допомагає генерувати більш глибокі ідеї та забезпечує винятковий досвід у багатьох різних додатках. Cisco DNA спирається на мережу, засновану на намірах, - революційного підходу до створення мереж, який допомагає організаціям автоматизувати, спростити і убезпечити мережу.

Мережа Cisco DNA, заснована на намірах, і є мережею яка:

- Інтерпретує кожен байт даних, що проходять через неї, що забезпечує кращу безпеку, більш персоналізований інтерфейс і більш швидку роботу.
- Перетворює цільові наміри в правильну конфігурацію мережі, дозволяючи управляти і надавати доступ до кількох пристроїв і речей за лічені хвилини.
- Постійно вчиться з величезних обсягів даних, що проходять через нього, і перетворює ці дані в корисну інформацію. Допомагає вам вирішувати проблеми, перш ніж вони стануть проблемами, і уроки з кожного інциденту.

Cisco DNA Center надає централізовану панель управління всією мережею-філією, кампусом, центром обробки даних і хмарою. Замість того, щоб покладатися на покрокове управління, можна розробляти, надавати і встановлювати наскрізні політики за допомогою єдиного інтерфейсу Cisco DNA Center. Це дозволяє швидше реагувати на потреби організації і спрощувати повсякденні операції. Cisco DNA Analytics and Assurance і Cisco Network Data Platform (NDP) допоможуть отримати максимальну віддачу від мережі, постійно збираючи і застосовуючи інформацію в дії. Cisco DNA є відкритою, розширюваною і програмованою на кожному рівні. Вона об'єднує технології Cisco і сторонніх виробників, відкриті API і платформу для розробників для підтримки багатої екосистеми мережевих додатків [14].

## 2.2 Комутатори

Мережевий комутатор — це елемент мережевого обладнання, який поєднує пристрої в комп’ютерній мережі використовуючи комутацію пакетів для отримання та пересилання даних на пристрій цільового призначення.

Мережевий комутатор використовує MAC-адреси для пересилання даних на канальний рівень (L2) моделі OSI. Деякі комутатори можуть також пересилати дані на мережевий рівень (L3), додатково включаючи функції маршрутизації. Такі

комутатори широко відомі як комутатори L3 [15]. В даному розділі будуть розглянуті, як комутатори другого так і третього рівнів.

### 2.2.1 Cisco Catalyst 9500

Комутатор Catalyst 9500 (рис. 5) інноваційне апаратне забезпечення, яке допомагає переосмислити архітектуру з'єднання, посилити безпеку та вдосконалити систему організації.

Рис. 5 Cisco Catalyst 9500

Комутатор Cisco Catalyst 9500 (рис.5) побудований на основі інтегральної схеми (ASIC) Cisco Unified AccessData Plane (UADP) є провідною платформою перемикання ядра та агрегації Cisco для фіксованого підприємства.

Комутатор Cisco c9500 підтримує:

- розширені послуги маршрутизації та інфраструктури (наприклад Multiprotocol Label Switching [MPLS], VPN рівня 2 і рівня 3, багатоадресна VPN [MVPN] і трансляція мережевих адрес [NAT]);
- можливості програмно-визначеного доступу Cisco (такі як база даних відстеження хостів, міждоменне з'єднання та протокол VPN-маршрутизації та пересилання [VRF];
- віртуалізацію мережевої системи за допомогою технології Cisco StackWise Virtual2;

- основні можливості високої доступності, такі як виправлення, безперервне пересилання Cisco з перемиканням стану, резервні джерела живлення та вентилятори, підтримуючи при цьому широкий спектр оптики.

C9500 – це представник наступного покоління комутаторів ядра та рівня агрегації корпоративного класу, які підтримують повну програмованість та зручність обслуговування. Серія Cisco Catalyst 9500, заснована на процесорі x86, є провідною спеціально створеною платформою комутації Cisco з фіксованим ядром і агрегацією. Перемикачі оснащені 4-ядерним процесором x86, 2,4-ГГц, 16-ГБ пам'яті DDR4 і 16-ГБ внутрішньої пам'яті [17].

Серед особливостей даного рішення можна виділити наступні:

- можливість сегментації та мікросегментації стала легшою, з передбачуваною продуктивністю та масштабованістю;
- швидший запуск нових бізнес-сервісів і суттєво зменшений час вирішення проблем;
- підтримка подвійного стека для IPv4/IPv6 та динамічного розподілу таблиць пересилання обладнання для спрощення міграції з IPv4 на IPv6;
- підтримка як статичного, так і динамічного NAT і трансляції адреси порту (PAT).

Серед функцій захисту c9500 надає низку можливостей:

- Аналітика зашифрованого трафіку (ETA): отримуємо переваги від можливостей машинного навчання для виявлення загроз або аномалій у мережі та вжиття заходів щодо них, зокрема виявлення зловмисного програмного забезпечення в зашифрованому трафіку та розподіленого виявлення аномалій. Крім того, ETA може виявляти вразливі реалізації в зашифрованому трафіку;
- Підтримка AES-256 з 256-бітним алгоритмом шифрування MACsec, доступним на всіх моделях;
- Надійні системи: підтримка безпечної унікальної ідентифікації пристрою (SUDI) для Plug and Play, що забезпечує захист від несанкціонованого доступу до ідентифікації пристрою, який в свою чергу забезпечує zero-touch доступ,

зобов’язуючи пристрій показувати сертифікат серверу, щоб мати можливість отримати доступ до мережі [17].

### 2.2.2 Cisco Catalyst 9200

Cisco Catalyst 9200 - основа для архітектури цифрової мережі, комутатори серії Catalyst 9200 допомагають користувачам спростити складність, оптимізувати IT та знизити експлуатаційні витрати за рахунок використання інтелекту, автоматизації та людського досвіду, які жоден інший аналог не може надати, незалежно від того, де ви перебуваєте.

Вони забезпечують функції безпеки, які захищають цілісність апаратного забезпечення, а також програмного забезпечення та всіх даних, які проходять через комутатор. Catalyst 9200 забезпечує стійкість, яка забезпечує безперебійну роботу бізнесу. У поєднанні з відкритими API-інтерфейсами Cisco IOS XE і програмованістю технології UADP ASIC комутатори серії Catalyst 9200 дають те, що потрібно зараз, із захистом інвестицій.

Рис. 6 Cisco Catalyst 9200

Програмне забезпечення Cisco IOS XE застосовує абсолютно нову парадигму в конфігурації, експлуатації та моніторингу мережі за допомогою її автоматизації. Нижче наведено різні механізми автоматизації:

- Автоматизоване надання пристроїв — це можливість автоматизувати процес оновлення образів програмного забезпечення та встановлення файлів конфігурації на комутатори Cisco Catalyst, коли вони вперше розгортаються в мережі;
- Конфігурація на основі API доступна для сучасних мережевих комутаторів, таких як комутатори серії Cisco Catalyst 9200. Він підтримує широкий спектр функцій автоматизації та надає надійні відкриті API через NETCONF і RESTCONF, використовуючи моделі даних для зовнішніх інструментів, як готових, так і спеціально створених, для автоматичного надання мережевих ресурсів;
- Детальна видимість дає змогу телеметрії, передавати дані від комутатора до вузла призначення. Cisco IOS XE підтримує модель push. Вона забезпечує моніторинг мережі майже в реальному часі, що призводить до швидкого виявлення та усунення збоїв;
- Безперебійне оновлення програмного забезпечення та виправлення підтримують стійкість ОС. На комутаторах Cisco Catalyst серії 9200 Cisco IOS XE підтримує холодне виправлення з перезавантаженням, що забезпечує виправлення критичних помилок і вразливостей безпеки між регулярними випусками технічного обслуговування. Ця підтримка дозволяє додавати виправлення, не чекаючи наступного випуску обслуговування. Для холодного виправлення потрібно перезавантажити комутатор після встановлення виправлення, щоб зміни увійшли в силу;
- Надійні рішення, створені за допомогою технологій Cisco Catalyst License Trust Anchor Technologies, забезпечують безпечну основу для продуктів Cisco. Завдяки комутаторам Cisco Catalyst 9200 ці технології забезпечують автентичність апаратного та програмного забезпечення для довіри до ланцюга поставок і надійного пом’якшення від атак «людина посередині», які компрометують

програмне забезпечення та мікропрограму. Можливості Trust Anchor включають підписання зображень, безпечне завантаження та модуль Cisco Trust Anchor [18].

Висока доступність, одна з найбільш суттєвих характеристик комутаторів Cisco Catalyst серії 9200 підтримує зокрема такі функції:

- Cross-stack EtherChannel надає можливість конфігурувати технологію Cisco EtherChannel для різних членів стека для високої стійкості.
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) забезпечує швидку конвергенцію охоплюваного дерева незалежно від таймерів дерева, а також пропонує переваги балансування навантаження рівня 2 та розподіленої обробки.
- Швидке зв’язне дерево для кожної VLAN (PVRST+) забезпечує швидку реконвергенцію зв’язного дерева (IEEE 802.1w) на основі комплексного дерева для кожної VLAN, забезпечуючи простішу конфігурацію, ніж MSTP. Як в режимах MSTP, так і в PVRST+, одиниці з стек поводяться як один вузол охоплюючого дерева.
- Автоматичне відновлення через порт комутатора (відновлення «err-disable») автоматично намагається повторно активувати посилання, яке вимкнено через помилку мережі.

### 2.3 Міжмережеві екрани

Cisco Firepower 4110 (рис.7) – обраний міжмережевий екран, який належить до лінійки 4100. Загальна характеристика даних програмних рішень полягає у тому, що Cisco Firepower 4100 являє орієнтований на загрози.

Рис. 7 Cisco Firepower 4110

Діапазон пропускної здатності підходить для використання в центрах обробки даних. Вони забезпечують чудовий захист від загроз на вищих швидкостях при менших габаритах.

Cisco 4100 можуть запускати програмне забезпечення Cisco Secure Firewall ASA або Cisco Secure Firewall Threat Defense (FTD). Разом із цим Firepower 4110:

- забезпечує систему запобігання вторгнень нового покоління (ngips) для забезпечення кращого в галузі захисту від загроз;
- включає в себе повністю інтегроване рішення advanced malware protection( amp), яке усуває як відомі, так і невідомі загрози, а також інтегроване ізольоване середовище;
- дає можливість відстежувати і стримувати зараження шкідливими програмами;
- автоматично зіставляє події загроз з вразливостями мережі, щоб адміністратори могли зосередити свої ресурси на найбільш важливих загрозах;
- аналізує слабкі місця мережі і рекомендує найкращі політики безпеки для впровадження;
- інтегрується з низкою продуктів cisco network security, щоб забезпечити більш надійний захист [19].

Пом'якшення DdoS є гострою проблемою, отже і увага до захисту системи від даної атаки повинна бути на відповідному рівні. Firepower DDoS Mitigation забезпечує Radware Virtual DefensePro (vDP), доступний і підтримується безпосередньо від Cisco на таких пристроях Cisco Firepower серії 9200 і 4100.

В свою чергу Radware vDP – це рішення для пом’якшення поведінкових атак DDoS в реальному часі, яке захищає організації від безлічі загроз DDoS. Пом’якшення DDoS-атак Firepower захищає інфраструктуру додатків від деградації та відключення мережі та додатків [20].

Пом’якшення DDoS-атак складається з захищеної патентом адаптивної технології сигнатур реального часу на основі поведінки, яка виявляє та пом’якшує DDoS-атаки нульового дня на мережі та програми в режимі реального часу. Це

усуває необхідність втручання людини і не блокує легальний трафік користувачів під час атаки.

Виявлені та пом’якшені такі атаки:

- Атаки flooding SYN
- Мережні DDoS-атаки, включаючи IP-флуд, ICMP-флуд, TCP-флуд, UDP-флуд та IGMP-флуд
- DDoS-атаки додатків, включаючи потоки HTTP та потоки запитів DNS
- Аномальні атаки flood, такі як атаки нестандартних пакетів і атаки із неправильним форматом

Для підвищення рівня безпеки застовуються також технології Cisco Trust Anchor. Вони забезпечують безпечну основу для продуктів Cisco. Cisco Trust Anchor забезпечує автентичність апаратного та програмного забезпечення для довіри до ланцюга поставок [21].

Можливості Trust Anchor включають:

- Підписування зображень: криптографічно підписані зображення дають гарантію того, що мікропрограмне забезпечення, BIOS та інше програмне забезпечення є справжніми та незмінними. Під час завантаження системи програмні сигнатури системи перевіряються на цілісність;
- Безпечне завантаження: безпечне завантаження прив’язує ланцюг довіри послідовності завантаження до незмінного обладнання, пом’якшуючи загрози для основного стану системи та програмного забезпечення, яке має бути завантажено, незалежно від рівня привілеїв користувача. Він забезпечує багатошаровий захист від збереження незаконно зміненого мікропрограмного забезпечення;
- Модуль Trust Anchor: одночіпове рішення, стійке до несанкціонованого доступу, надійне криптографічне рішення забезпечує гарантію автентичності апаратного забезпечення для однозначної ідентифікації продукту, щоб можна було підтвердити його походження для Cisco, забезпечуючи гарантію, що продукт є справжнім [22].

## 2.4 Блейд шасі

PowerEdge M1000e (рис.8) інноваційна розробка Dell, яка забезпечує максимальну гнучкість, енергоефективність і теплову ефективність, загальносистемну доступність, продуктивність і керованість.

Шасі об'єднує новітні технології управління, введення-виведення, живлення та охолодження в модульному, простому у використанні корпусі. Розроблений з нуля для підтримки поточного і майбутніх поколінь серверів, систем зберігання даних, мережевих технологій і технологій управління, PowerEdge M1000e володіє запасом, необхідним для масштабування в майбутньому [23].

Dell оптимізували модульний серверний корпус PowerEdge M1000e і серверні модулі для:

- Максимальної гнучкості - модульна архітектура вводу-виводу, живлення, охолодження та управління;
- Максимальної довговічності - оптимізована конструкція живлення і охолодження підтримує поточне і майбутні покоління серверних модулів і введення-виведення; пропускна здатність введення-виведення для підтримки не тільки сучасного покоління;
- Нижчої вартості володіння - нижча вартість, ніж у стоєчних серверів з аналогічними функціями і відповідно краща в своєму класі потужність і ефективність охолодження;

Практично необмежена масштабованість шасі PowerEdge M1000e забезпечує максимальну гнучкість в архітектурі серверних процесорів і чіпсетів. Інфраструктура може одночасно підтримувати серверні архітектури Intel і AMD, в той час як передові визначення механічних, електричних і програмних інтерфейсів забезпечують підтримку і розширення серверів декількох поколінь.

До особливостей шасі відносяться наступні:

- Високошвидкісна пасивна середня плата, яка з'єднує серверні модулі спереду і з інфраструктурою живлення;

- Широкі можливості управління живленням, включаючи надання загального живлення для забезпечення повної потужності джерел живлення, доступних для всіх серверних модулів;
- Широкі можливості управління, включаючи приватні Ethernet, послідовні, USB і низькорівневі можливості управління між комутатором CMC, клавіатурою, відео і мишею (KVM) і серверними модулями.

Рис. 8 PowerEdge M1000e

До двох контролерів управління шасі (CMC - 1: стандартний; CMC-2: забезпечує додаткове резервування) і один додатковий вбудований комутатор KVM (iKVM)

До шести резервних джерел живлення з можливістю гарячого підключення і дев'яти резервних вентиляторних модулів з можливістю гарячого підключення N+1
Передня панель управління системою з РК-панеллю, двома USB-підключеннями до клавіатури і миші і одним підключенням до відеореєстратора

Підтримка блейд-масиву Dell EqualLogic ™ PS-M4110 з безшовною інтеграцією в шасі M1000e [23].

Не можливо оминути і функції безпеки, які пропонує дане рішення. M1000e пропонує безліч функцій безпеки, включаючи можливість:

- Призначення одного адміністратора для кожного блейда або одного адміністратора для декількох блейдів;
- Надання дозволів деяким блейдам на виконання(не всім);
- Налаштування адміністративного доступу для CMC - Chassis Management Controller, iDRAC - Integrated Dell Remote Access Controller з контролером життєвого циклу та вводу-виводу;

Більшість функцій безпеки керовані CMC, який забезпечує централізоване налаштування параметрів безпеки корпусу M1000e і доступ користувачів, а також захищений змінним користувачем паролем. Функції безпеки CMC включають в себе:

- Автентифікацію користувача за допомогою додаткових служб Active Directory і LDAP або збережених на обладнанні ідентифікаторів користувачів і паролів;
- Розподілення повноважень на основі ролей, які дозволяють адміністратору налаштовувати певні привілеї для кожного ідентифікатора користувача та налаштування пароля через веб-інтерфейс, що підтримує 128-розрядне шифрування SSL 3.0 та 40-розрядне шифрування SSL 3.0 (для країн, де 128-розрядне шифрування неприйнятне);
- Налаштовувані IP-порти;
- Обмеження на відмову входу в систему для кожного IP-адреси з блокуванням входу з IP-адреси при перевищенні межі;
- Налаштовуваний тайм-аут автоматичного сеансу і кількість одночасних сеансів;
- Обмежений діапазон IP-адрес для клієнтів, що підключаються до CMC;
- Захищена оболонка (SSH), яка використовує зашифрований рівень для підвищення безпеки ;

- Єдиний вхід, двофакторна аутентифікація та аутентифікація з відкритим ключем;
- Доступ до передньої панелі, який може бути відключений;

M1000e розроблений таким чином, щоб забезпечити гнучкість для підтримки різних рішень для зберігання даних в залежності від вимог організації [24].

### 2.5 Сервери

Сервер Dell EMC PowerEdge XR12 (рис.9) оснащений масштабованими процесорами Intel Xeon 3-го покоління і призначений для роботи в складних умовах, включаючи телекомунікації, військові, роздрібну торгівлю, що згідно майбутнього розташування є перевагою.


Рис. 9 Dell EMC PowerEdge XR12

З боку безпеки даний сервер надає такі можливості:

- Прошивка з криптографічним підписом
- Безпечне завантаження
- Безпечне стирання
- Блокування системи
- Підвищення ефективності та прискорення операцій завдяки автономній співпраці.

Портфель рішень Dell EMC OpenManage systems management дозволяє знизити складність управління IT-інфраструктурою і забезпечити її безпекою. Використовуючи інтуїтивно зрозумілі комплексні інструменти Dell Technologies, IT-

відділ може забезпечити безпечну та інтегровану роботу за рахунок скорочення розрізненості процесів та інформації, щоб зосередитися на розвитку бізнесу. Інструменти і засоби автоматизації, допоможуть масштабувати, управляти і захищати технологічне середовище [25].

Dell EMC PowerEdge XR12 має такі переваги:

- Вбудована потокова передача телеметрії, управління температурою і RESTful API з Redfish забезпечують оптимізовану видимість і контроль для кращого управління сервером;
- Інтелектуальна автоматизація дозволяє забезпечити взаємодію між діями людини і можливостями системи для підвищення продуктивності;
- Інтегровані можливості управління змінами для планування оновлень і безшовної настройки і впровадження з нульовим дотиком;
- Повна інтеграція управління стеком з Microsoft, VMware, ServiceNow, Ansible і багатьма іншими інструментами.

**Висновки за розділом 2**

У даному розділі було наведено основні апаратні рішення, які використовуватимуться під час проектування топології для державного підприємства.

Описано загальні принципи функціонування продуктів, їх технічні характеристики, вбудовані заходи безпеки та зазначена можливість гнучого керування з боку системних адміністраторів та адміністраторів безпеки. Усі продукти є сучасними і активно використовуваними на ринку, що безумовно підтверджується описами наданими у розділі для кожної одиниці.

# РОЗДІЛ 3
# ПЛАНУВАННЯ ТОПОЛОГІЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ШТАБ-КВАРТИРИ ДЕРЖАВНОГО ПІДПРИЄМСТВА

## 3.1 Проектування архітектури системи державного підприємства

Для спроектованої схеми (рис.10) додано наступні структурні засоби захисту, кожен з яких буде розглянуто в цьому розділі:

- DMZ
- VLAN
- NFIPS + AMP
- ACL

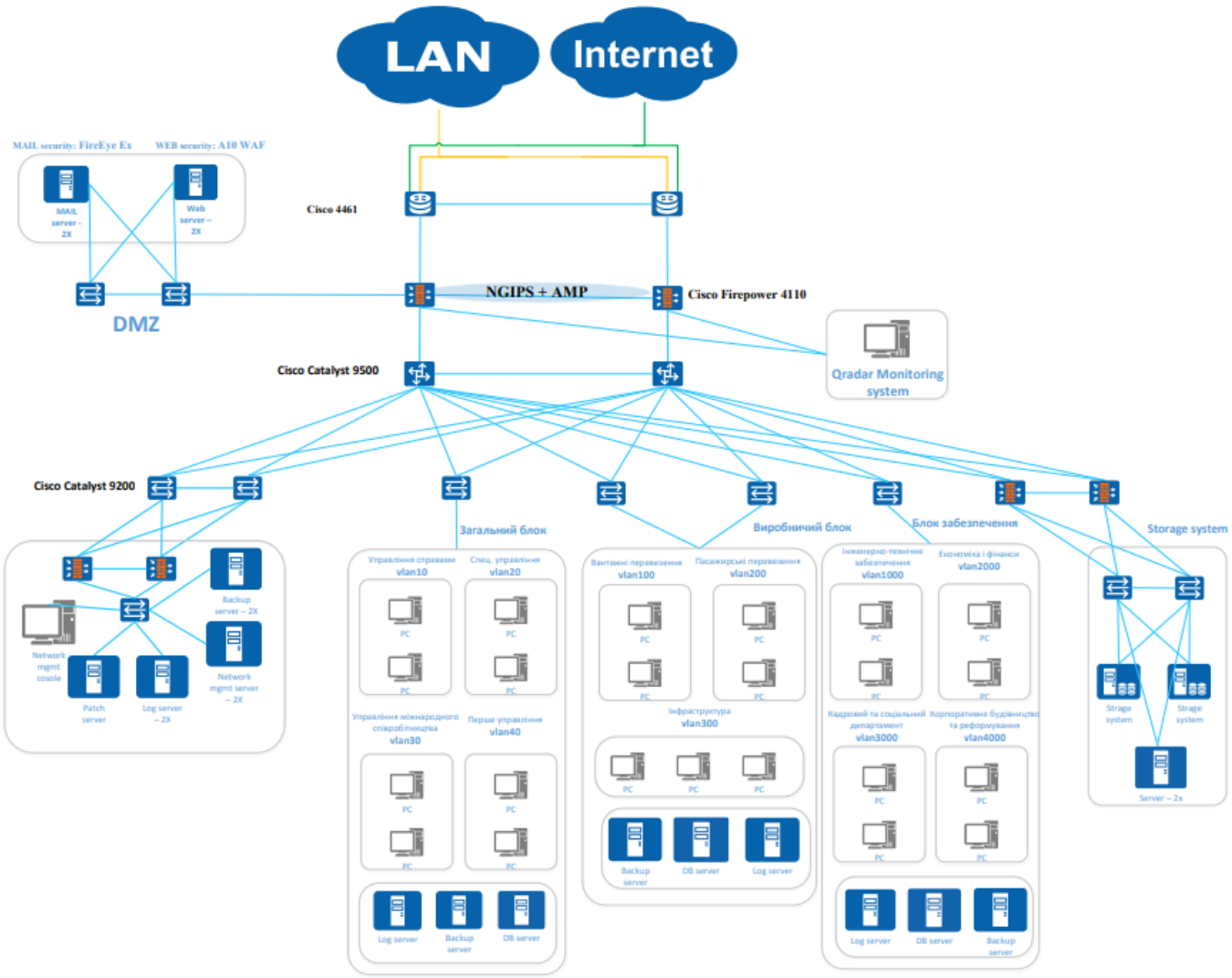



Рис. 10 Топологія штаб-квартири державного підприємства

DMZ — (demilitarized zone – демілітаризована зона) — це підмережа, яка знаходиться між Інтернетом та приватними мережами. Основна мета DMZ — дозволити організації отримати доступ до ненадійних мереж, таких як Інтернет, при цьому забезпечивши безпеку її локальної мережі. Підхід DMZ ускладнює зловмиснику отримання прямого доступу до даних організації та внутрішніх серверів через Інтернет.

Зазвичай організації зберігають зовнішні послуги та ресурси, а також сервери для системи доменних імен (DNS), протоколу передачі файлів (FTP), пошти, проксі-сервера, протоколу передачі голосу через Інтернет (VoIP) і веб-серверів у DMZ.

Організації із загальнодоступним веб-сайтом, яким користуються клієнти, повинні зробити свій веб-сервер доступним з Інтернету. Це означає піддавати всю внутрішню мережу високому ризику. Щоб запобігти цьому, організація може заплатити хостинговій фірмі за розміщення веб-сайту або їхніх загальнодоступних серверів у брандмауері, але це вплине на продуктивність. Тож натомість загальнодоступні сервери розміщуються в окремій та ізольованій мережі.

Мережа DMZ забезпечує буфер між Інтернетом і приватною мережею організації. DMZ ізольована шлюзом безпеки, таким як брандмауер, який фільтрує трафік між DMZ і локальною мережею. Сервер DMZ за замовчуванням захищений іншим шлюзом безпеки, який фільтрує трафік, що надходить із зовнішніх мереж [26].

Вона ідеально розташована між двома брандмауерами, а налаштування брандмауера DMZ гарантує, що вхідні мережеві пакети відстежуються брандмауером або іншими засобами безпеки, перш ніж вони потраплять на сервери, розміщені в DMZ. Це означає, що навіть якщо досвідчений зловмисник зможе подолати перший брандмауер, він також повинен отримати доступ до посилених служб у DMZ, перш ніж завдати шкоди організації.

Якщо зловмиснику вдається проникнути через зовнішній брандмауер і зламати систему в DMZ, він також повинен пройти внутрішній брандмауер, перш ніж отримати доступ до конфіденційних корпоративних даних.

Висококваліфікований зловмисник цілком може зламати захищену DMZ, але ресурси в ній повинні бити тривогу, яка дає низку попереджень про те, що відбувається порушення.

Основною перевагою DMZ є забезпечення для внутрішньої мережі розширеного рівня безпеки шляхом обмеження доступу до конфіденційних даних і серверів. DMZ дозволяє відвідувачам веб-сайту отримувати певні послуги, забезпечуючи буфер між ними та приватною мережею організації. В результаті DMZ також пропонує додаткові переваги безпеки, такі як:

Запобігання розвідці в мережі - забезпечуючи буфер між Інтернетом і приватною мережею, DMZ запобігає зловмисникам виконувати розвідувальну роботу, яку вони здійснюють для пошуку потенційних цілей.

Блокування підробки протоколу Інтернету (IP) - зловмисники намагаються знайти способи отримати доступ до систем, підробляючи IP-адресу та видаючи себе за легальний пристрій, що увійшов у мережу. DMZ може виявляти та зупиняти такі спроби спуфінгу. DMZ також забезпечує сегментацію мережі, щоб створити простір для організації трафіку та доступу до державних послуг далеко від внутрішньої приватної мережі.

Увімкнення контролю доступу: підприємства можуть надавати користувачам доступ до послуг за межами їхньої мережі через Інтернет. DMZ надає доступ до цих послуг, реалізуючи сегментацію мережі, щоб ускладнити доступ неавторизованого користувача до приватної мережі.

Компоненти DMZ включають:

- DNS-сервери
- FTP-сервери
- Поштові сервери
- Проксі-сервери
- Веб-сервери

На розробленій топології в межах DMZ знаходяться веб та поштові сервери. Веб-сервери є відповідальними за підтримку зв'язку з внутрішнім сервером бази даних, тому їх потрібно розмістити в DMZ. Це допомагає забезпечити безпеку внутрішньої

бази даних, яка часто зберігає конфіденційну інформацію. Окремі повідомлення електронної пошти, а також база даних користувачів, зазвичай зберігаються на серверах без прямого доступу до Інтернету.

Тобто сервер електроної пошти розміщено всередині DMZ, щоб взаємодіяти з базою даних електронної пошти та отримувати доступ до неї, не піддаючи її безпосередньо потенційно шкідливому трафіку [26].

Віртуальна локальна мережа (VLAN) — це логічна накладена мережа, яка об’єднує підмножину пристроїв, які спільно використовують фізичну локальну мережу, ізолюючи трафік для кожної групи.

LAN — це група комп’ютерів або інших пристроїв у тому самому місці, наприклад, у тій самій будівлі чи кампусі, які використовують одну фізичну мережу. LAN зазвичай асоціюється з широкомовним доменом Ethernet який являє собою набір мережевих пристроїв.

Комп’ютери в локальній мережі підключаються до одного мережевого комутатора безпосередньо, проте також можуть підключатися до одного з набору взаємопов’язаних комутаторів, наприклад набору комутаторів доступу, які під’єднуються до магістрального комутатора. Після того, як трафік перетинає маршрутизатор, він не вважається таким, що знаходиться в одній локальній мережі, навіть якщо все залишається в одній будівлі або поверсі. Як результат, місце може мати багато взаємопов’язаних локальних мереж.

VLAN, як і локальна мережа, на якій вона розташована, працює на 2 рівні мережі, на рівні Ethernet. VLAN поділяють одну комутовану мережу на набір накладених віртуальних мереж, які можуть відповідати різним функціональним вимогам і вимогам безпеки. Таке розділення дозволяє уникнути необхідності мати декілька окремих фізичних мереж для різних випадків використання [27].

Говорячи про типову конфігурацію VLAN кожен вузол даної мережі фізично підключений до комутатора Ethernet. Потім адміністратор мережі налаштовує комутатор на сегментацію певних портів для певних груп. Кожне групування називається VLAN, і з цього моменту всі члени однієї VLAN можуть спілкуватися один з одним без необхідності залучення інших мережевих пристроїв, за винятком

конкретних випадків, коли VLAN охоплює два або більше географічних місць. Тоді відповідна VLAN не має іншого вибору, окрім як обходити більше одного мережевого пристрою. Ідеї для сегментації 2 рівня різноманітні, але з точки зору безпеки це надає адміністратору мережі засіб, за допомогою якого він може захистити свою мережу від інсайдерських атак.

Наприклад, у мережі, яка не має сегментації VLAN, зловмисник на певному вузлі може запустити перевірку пакетів і почати захоплення всього мережевого трафіку, який проходить через комутатор, до якого він фізично підключений. Однак із правильно налаштованим VLAN це стає набагато складніше.

З точки зору того, як налаштувати VLAN з метою безпеки, існує кілька різних методів, але існує один, який набув значної популярності, - це VLAN на базі відділів.

Простіше кажучи, VLAN сегментується за організаційним відділом. Досягти цього можна шляхом запису всіх MAC-адрес для кожного вузла в межах даного відділу та вставлення їх у таблицю MAC комутатора. Після того, як таблиця MAC стане достатньо заповненою, адміністратор мережі налаштовує комутатор для визначення певних MAC-адрес у визначений VLAN. Якщо вищезгаданий зловмисник починає виконувати захоплення пакетів на своєму кінцевому пристрої, він захоплюватиме щонайбільше кадри Ethernet мережевого трафіку, який проходить через його відповідний VLAN. Це пояснюється тим, що комутатор, де знаходиться конфігурація VLAN, перевіряє кожен вхідний кадр Ethernet і пересилає кадри лише на основі даних у полі IEEE 802.1Q.

Проте слід розуміти, що не зважаючи на те, що VLAN забезпечують певні переваги безпеки, вони не позбавлені власного набору ризиків. Один з моментів, який фахівці з безпеки повинні мати на увазі, — це перехід між VLAN, який, є несанкціонованою практикою кінцевого використання зв’язків в межах VLAN. Цей злам найбільш ефективно виконується, коли визначений VLAN охоплює більше ніж один комутатор. Такий сценарій поширений в організаціях, де використовуються групові VLAN, і одна або кілька груп стають занадто великими для одного фізичного комутатора Ethernet. У цьому випадку може бути використана концепція,

відома як транкинг VLAN. Транкинг VLAN – це практика налаштування одного або кількох портів на комутаторі Ethernet спеціально з метою пересилання та отримання всього трафіку VLAN на/від іншого фізичного комутатора [28].

Поширена варіація застосування переходу VLAN відома як подвійне тегування. У цьому типі атаки зловмисник вставляє дублікат заголовка 802.1Q у кадр Ethernet, тим самим дозволяючи передати кадр до неавторизованої VLAN. Кадр передається, оскільки початковий перемикач перевіряє кадр, видаляє перший із двох заголовків 802.1Q і пересилає частину кадру, що залишилася. Без відома решти мережі, вторинний заголовок 802.1Q все ще приєднано до кадру; отримана логічна помилка може спричинити хаос у даній мережі. Щоб захиститися від атак із подвійними тегами, адміністратори мережі повинні бути пильними під час моніторингу мережевих журналів.

Комплекс засобів NFIPS + AMP, які присутні для міжмережевих екранів Cisco Firepower 4110, розглянутих у другому розділі дипломної роботи, є розробленими для даної лінійки засобами захисту.

Cisco Advanced Malware Protection (AMP) - розширений захист від шкідливих програм - забезпечує рівень захисту від шкідливих програм і розширених загроз для Firepower NGFW. AMP дає підприємству можливість:

- Виявляти, блокувати та аналізувати загрози зловмисного програмного забезпечення та інші спроби використання безпеки, щоб забезпечити повний захист критичних активів у мережі;
- Виявляти та блокувати загрози та спроби несанкціонованого використання;
- Ретроспективний аналіз безпеки;
- Постійний аналіз трафіку та файлів;
- Пісочниця файлів.

Забезпечуючи функціональні можливості запобігання вторгненню для Cisco Firepower NGFW, система запобігання вторгненню нового покоління (NGIPS) — побудована на відкритій технології Snort — надає організаціям детальну видимість і уявлення про виявлені загрози. Така видимість і контекст дозволяють командам

безпеки реагувати за допомогою необхідних ресурсів і успішно пом’якшувати вторгнення. Ключові можливості NFIPS можна охарактеризувати наступним переліком, до якого відносяться:

- Наявність методів виявлення аномалій;
- Контекстна обізнаність у режимі реального часу;
- Автоматика безпеки;
- Розширений захист від загроз;
- Контроль програм і фільтрація URL-адрес;

Пристрої з NGIPS забезпечують видимість мережі, аналіз безпеки, автоматизацію та розширений захист від загроз. Він використовує провідні в галузі можливості запобігання вторгненню та різноманітні методи, щоб виявити навіть найскладніші мережеві атаки та захистити вас від них [29].

NGIPS постійно знаходить інформацію про мережеве середовище, включаючи дані про операційні системи, мобільні пристрої, файли, програми та користувачів. Потім він використовує цю інформацію для створення мережевих карт і профілів хостів. Це дає контекстну інформацію, необхідну для прийняття кращих рішень щодо подій вторгнення. Ця інформація також може бути використана як вхідна інформація для кращої автоматизації ключових функцій захисту від загроз.

Функції Cisco Firepower NGIPS забезпечують провідну в галузі ефективність детектування відомих і невідомих загроз. Особливості роботи рішення включають:

- Правила IPS, які визначають і блокують трафік атак, спрямований на вразливості у вашій мережі;
- Тісно інтегрований захист від передового зловмисного програмного забезпечення, що включає розширений аналіз активності мережі та кінцевої точки;
- Технологія пісочниці, яка використовує сотні поведінкових індикаторів для виявлення атак нульового дня та атак, що ухиляються;

Список контролю доступу до мережі (ACL) складається з правил, які або надають доступ до комп’ютерного середовища, або забороняють його. Це дає змогу

адміністраторам гарантувати, що пристрій не зможе отримати доступ, якщо він не надасть належні облікові дані.

Існує два основних типи ACL - ACL файлової системи та мережеві ACL. Перший працює як фільтр, який володіє доступом до каталогів або файлів. ACL файлової системи дає інструкції для операційної системи щодо користувачів, яким дозволено доступ до системи, а також привілеї, на які вони мають право, коли вони знаходяться всередині.

Другий тип списків керує доступом до мережі. Для цього вони надають комутаторам та маршрутизаторам інструкції щодо видів трафіку, яким дозволено взаємодіяти з мережею. Вони також визначають, що кожен користувач або пристрій може робити, перебуваючи всередині.

Принцип роботи ACL не є складним. З ACL файлової системи є таблиця, яка повідомляє операційній системі комп'ютера, які користувачі мають які права доступу. Таблиця визначає користувачів, яким дозволено доступ до певних об'єктів, таких як каталоги або файли в системі. У списку є інформація для кожного користувача, який має необхідні права доступу до системи [30].

Наприклад, є певні об'єкти, доступ до яких може отримати лише адміністратор. Тобто, якщо користувач заходить не як адміністратор, доступу до виконання файлу він не матиме, проте, зробивши вхід з облікового запису адміністратора доступ до файлу буде надано.

У момент, коли користувач робить запит на доступ до об'єкта, операційна система комп'ютера перевіряє ACL, щоб побачити, чи повинен користувач мати потрібний доступ. Якщо список говорить, що користувачеві не можна дозволяти відкривати, використовувати або змінювати цей конкретний об'єкт, доступ буде відмовлено.

Особливість мережевих ACL є те, що вони встановлюються в комутатори і маршрутизатори. Фактично, вони є фільтром трафіку. Для фільтрації трафіку мережевий ACL використовує правила, попередньо визначені адміністратором або виробником. Ці правила перевіряють вміст пакетів з таблицями, які керують

параметрами доступу. Залежно від того, чи вийшов користувач, його доступ надається або забороняється.

Таким чином, комутатори та маршрутизатори, які мають списки керування доступом, виконують функцію фільтрів пакетів. Вони перевіряють адреси Інтернет-протоколу (IP) джерел і призначення, портів джерела і призначення, а також офіційну процедуру пакету, яка визначає, як він повинен рухатися по мережі.

За допомогою цього інструмента спрощується ідентифікація локальних користувачів, віддалених користувачів і віддалених хостів. Це робиться за допомогою бази даних аутентифікації, налаштованої для забезпечення доступу до пристрою лише затвердженим користувачам [30].

Список доступу також дозволяє запобігти небажаним користувачам і трафіку. Якщо провести налаштування адреси джерела або призначення і яким користувачам дозволено отримати доступ до мережі, можна запобігти сторонньому втручанню. Одночасно з цим є можливість проведення класифікацію типу трафіка. Наприклад, можна розробити політику, яка дозволяє всьому трафіку електронної пошти проходити в мережу, але блокувати трафік, який містить виконувані файли.

## 3.2 Огляд використовуваних програмних засобів захисту

### *IBM QRadar Security Information and Event Management (SIEM)*

IBM QRadar — це засіб корпоративної безпеки та управління подіями (SIEM). Він збирає дані журналів підприємства, його мережевих пристроїв, активів хоста та операційних систем, програм, вразливостей, а також діяльності та поведінки користувачів. Потім IBM QRadar виконує аналіз даних журналів і мережевих потоків у режимі реального часу для виявлення зловмисної активності, щоб її можна було швидко зупинити, запобігаючи або мінімізуючи шкоду організації.

QRadar створено, щоб надати фахівцям з безпеки централізований доступ до даних безпеки в масштабі організації та оперативне уявлення про найбільш пріоритетні загрози. Узагальнивши, можна виділити три етапи роботи засобу захисту:

- Перший етап - рішення поглинає величезну кількість даних зі всього підприємства, для забезпечення вичерпного уявлення про діяльність у локальних і хмарних середовищах.
- Другий етап – після надходження даних, QRadar застосовує в режимі реального часу автоматизований аналіз безпеки для швидкого та точного виявлення та визначення пріоритету загроз.
- Третій етап - попередження, які діють, забезпечують більший контекст потенційних інцидентів, а це в свою чергу дає змогу аналітикам з безпеки швидко реагувати, щоб обмежити вплив зловмисників [30].

QRadar SIEM інтелектуально зіставляє і аналізує різноманітну інформацію, таку як:

- Події безпеки, до яких відноситься інформація від брандмауерів, віртуальних приватних мереж, систем виявлення вторгнень, систем запобігання вторгнень, баз даних;
- Мережеві події такі як дані від комутаторів, маршрутизаторів, серверів, хостів;
- Хмарна активність: з середовищ SaaS та інфраструктури як послуги ((IaaS), таких як Office 365, SalesForce.com , Amazon Web Services( AWS), Azure і Google Cloud;
- Контекст користувача і активів, а саме контекстуальні дані з продуктів управління ідентифікацією і доступом та сканерів вразливостей;
- Події кінцевих точок, тобто інформацію з журналу подій Windows, Sysmon, рішень EDR та інших;
- Опціонально можна використовувати QRadar Network Insights як частину розгортання SIEM. В результаті підприємство може отримати уявлення про те, які системи спілкувалися одна з одною, які програми були задіяні та якою інформацією обмінювалися в пакетах. Порівнюючи цю інформацію з іншими мережевими, журнальними та користувацькими записами, аналітики з безпеки можуть виявити ненормальну мережеву активність, яка може свідчити про

скомпрометовані хости, скомпрометованих користувачів або спроби ексфільтрації даних [31].

Хоча QRadar постачається з численними правилами виявлення аномалій і поведінки як налаштуваннями за замовчуванням, команди безпеки також можуть створювати власні правила, налаштовувати параметри виявлення аномалій і завантажувати 160 попередньо створених програм із IBM Security App Exchange, щоб розширити їхнє розгортання.

***A10 Web Application Firewall***

Для захисту веб-додатків організаціям необхідно рішення, яке може пом'якшувати атаки, не блокуючи законних користувачів і не знижуючи продуктивність додатків. Їм потрібно просте в налаштуванні рішення, що підтримує докладне ведення журналу і графічну звітність. З цим досить продуктивно працює A10 WAF. До його функцій входить:

Забезпечення безпеки білих та чорних списку з автоматизованим навчанням.

Щоб зупинити веб-атаки, WAF повинен розпізнати відомі хороші поведінки, а також відомі атаки. Thunder WAF автоматично вивчає структуру захищених програм для виявлення незвичайних запитів і атак. Підтримуючи декілька одночасних шаблонів WAF, пристрої Thunder ADC і CFW можуть вивчати нові URL-адреси та одночасно захищати трафік.

Списки визначення атак для ін'єкції SQL, міжсайтових сценаріїв та іншого виявлення відомих атак. Адміністратори можуть легко переглядати та редагувати визначення як чорного, так і білого списків за допомогою веб-інтерфейсу користувача або інтерфейсу командної команди [32].

1. Захист JSON та

Thunder WAF може перевіряти трафік JSON на наявність атак, таких як ін'єкція SQL або XSS, і може обмежувати елементи JSON, такі як довжина масиву або глибина структури. Thunder WAF також може аналізувати та перевіряти файли XML та застосовувати схеми мови опису веб-служб (WSDL), щоб гарантувати, що файли XML правильно відформатовані

2. Використання геолокації для блокування трафіку за локацією

Елементи керування дозволяють A10 зупиняти DDoS-атаки, ініційовані з певних країн, і відповідати вимогам експортної відповідності.

Політики геолокації A10 дозволяють легко застосовувати елементи керування геолокацією. Імпортуючи сторонні списки геолокації з бажаних геолокаційних служб клієнтів, користувачі A10 можуть сповіщати або блокувати трафік, що надходить із певних регіонів.

3. Балансування навантаження, аутентифікація та захист DDOS Thunder ADC (Application Deliver Controllers) і CFW (Thunder Convergent Firewalls) балансують навантаження веб-трафіку, відстежують стан сервера за допомогою розширених перевірок і прискорюють роботу за допомогою кешування, стиснення та оптимізації TCP. Управління доступом до додатків (Application Access Management - AAM) забезпечує аутентифікацію та авторизацію, а захист від DDoS зупиняє програми та об'ємні DDoS-атаки – відбувається масштабування для блокування понад 200 мільйонів пакетів SYN в секунду на одному пристрої.

4. Комплексне та масштабоване управління

Для оптимізації та автоматизації керування пристрої Thunder включають промисловий стандарт CLI, веб-інтерфейс користувача та RESTful API який можна інтегрувати із сторонніми або користувацькими консолями керування. Для більших розгортань централізована система управління A10 Networks гарантує, що рутинні завдання можуть виконуватися кількома пристроями Thunder, незалежно від фізичного розташування [31].

5. Логізація та звітність

Рішення підтримує високошвидкісне ведення системного журналу, а також сповіщення електронною поштою для аналізу трафіку. Графічні звіти документують події безпеки для аналізу атак, а інформаційна панель у режимі реального часу відображає системну інформацію, використання пам'яті та ЦП, а також стан мережі.

***FireEye Ex***

Електронна пошта є найбільш вузлом, який є вразливим полем для кібератак, оскільки це точка надходження даних з найбільшим обсягом. Підприємство

стикається з постійно зростаючим числом проблем безпеки, пов'язаних з передовими загрозами на основі електронної пошти. Більшість просунутих загроз використовують електронну пошту для доставки URL-адрес, пов'язаних з фішинговими сайтами з обліковими даними і вкладеннями файлів, використовуваними в якості зброї. Електронна пошта є основним засобом кіберзлочинності, оскільки вона легко піддається таргетуванню та налаштуванню.

Обраний продукт проводить захист такими напрямками:

- Забезпечує комплексний захист електронної пошти від адресного фішингу та інших передових, багатостепових атак та атак нульового дня;
- Технологія Bursting (надсилання більшої кількості кадрів за той самий часовий інтервал) забезпечує додаткову можливість аналізу розпізнавання в періоди максимальної пропускної спроможності повідомлень;
- Підтримує аналіз зображень на операційних системах Microsoft Windows та Apple Mac OS X;
- Аналізує електронну пошту на приховані у файлах загрози, включаючи захищені паролем та зашифровані вкладення, а також шкідливі URL-адреси;
- Автоматично виявляє та зменшує або повністю запобігає фішингу даних облікових записів користувачів;
- Надає контекстні висновки з обробки даних про оповіщення для встановлення пріоритетів та стримування загроз;
- Інтегрується з різними технологіями FireEye;
- Розгортання відбувається локально в режимах активного захисту або тільки відстеження;
- Забезпечує видимість, відстеження та керування повідомленнями та оповіщеннями.

***Trend Micro Enterprise Security for Endpoints***

Державне підприємство, є складною установою, де співробітники використовують як ноутбуки, так і ПК, як в офісі так і віддалено. У багатьох випадках організації використовують файлові сервери на різних операційних

системах. Тож постає очевидна необхідність імплементації захисту для кінцевих користувачів від загроз.

Trend Micro Enterprise Security for Endpoints захищає кінцеві точки як у мережі, так і поза нею від шкідливого програмного забезпечення, вторгнень на хост (HIP) та шкідливих веб-сайтів. Цей комплекс безпеки кінцевої точки забезпечується хмарною системою безпеки Trend Micro Smart Protection Network, яка забезпечує глобальний аналіз загроз і швидшу продуктивність [33].

Під об'єктами захисту будемо розглядати:

- Персональні коп'ютери з ОС Windows/ Linux;
- Сервери Microsoft;
- Файлові, веб-сервери та сервери програм Linux.

З переваг захисту кінцевих пристроїв можна виділити такі:

- Забезпечується миттєвий захист кінцевих точок у мережі чи поза нею;
- Блокуються шкідливі файли та веб-сайти та автоматично видаляються шкідливі програми;
- Зменшується вплив на продуктивність і ресурси кінцевих точок;
- Є можливість додавання нових політик безпеки за допомогою модулів плагінів, усуваючи необхідність повторного розгортання повного рішення;
- Зменшується складність управління та загальні витрати;
- Хости захищаються від втрати даних та пошкодження репутації за допомогою додаткового DLP, шифрування та мобільної безпеки.

***TrendMicro SafeLock***

Рішення TrendMicro SafeLock призначене для захисту промислових систем управління та вбудованих пристроїв, що потребують високого рівня доступності, а також спеціалізованих пристроїв у замкнених середовищах. Обмежуючи використання системи певними функціями, рішення ефективно запобігає вторгненню та виконання шкідливих програм, надаючи мінімальний вплив на продуктивність системи та не вимагаючи регулярного оновлення антивірусної бази даних. Також рішення має простий та інтуїтивно зрозумілий користувацький інтерфейс, що полегшує роботу з даним засобом захисту [34].

Основні опції, які містить в собі SafeLock:

1. Захист від експлойтів

Заходи проти зловмисного програмного забезпечення та мережевих вірусів, а також запобігання ін’єкції DLL, запобігання підключенню API та рандомізації пам’яті зменшують ризик несанкціонованого виконання та вірусної передачі

2. Адміністрування на основі ролей

Для цієї політики доступні два типи облікових записів: обліковий запис адміністратора та обліковий запис користувача з обмеженими можливостями. Обмежений обліковий запис користувача може бути обмежений щодо функцій, для яких його можна використовувати.

3. Журнал

Перелік усіх дій цього продукту заноситься в журнал подій Windows. Оскільки він не відображається на екрані сповіщень під час роботи, це не перешкоджає використанню системи.

4. Інтерфейси

На додаток до CLI (інтерфейсу командного рядка), доступний графічний інтерфейс з хорошою функціональністю та видимістю.

### 3.3 Формування рекомендацій при побудові топології інформаційної системи для державного підприємства

Першим і найголовнішим завданням є визначення типу архітектури, яка в подальшому буде розроблятися для підприємства (державного/приватного).
Надалі починається процес пропрацювання структурних підрозділів та найголовніше постає питання резервування окремих сервісів та частин системи для підвищення відмовостійкості усієї системи підприємства.

Повинне відбуватися дублювання ключових елементів архітектури. Такими елементами є роутери, комутатори, міжмережеві екрани, сервери та системи зберігання даних. Тому на розробленій схемі чітко прослідковується ця тенденція. Наприклад для підприємства окремо винесено систему зберігання, яка має відповідно свого двійника. Обидві системи підключені до двох комутаторів зметою

уникнути єдиної точки відмови з боку комутаційного устаткування. На рівні ядра системи ми маємо два роутера, міжмережеві екрани та комутатори рівня ядра. Таким чином підвищуємо відмовостійкість та знижуємо імовірність відмови роботи сервісів, коли один з ключових елементів перестає працювати. Навіть якщо виникає така ситуація, увесь трафік з інформаційної системи буде протікати через резервний вузол такого ж рівня.

Наступним важливим пунктом при проектуванні системи є обов'язковість виокремлення певних сервісів у демілітаризовану зону. Вона потрібна через можливість ізоляції загальнодоступних сервісів.

DMZ - дозволить організації отримати доступ до ненадійної частини мережі, такої як Інтернет, при цьому забезпечивши безпеку нашої локальної мережі. В нашому випадку DMZ містить в собі два веб-сервери та два поштові сервери. В цю зону винесені саме ці два типи серверів, адже саме на них спрямована переважна більшість атак.

З точки зору організаційних підрозділів, кожен із них повинен мати власні обчислювальні ресурси та сервери резервних копій. Проте виділення окремої підмережі виключно для налаштування мережевої взаємодії, встановлення оновлень, збору журналів подій та зберігання резервних копій є необхідним через те, що звичайні користувачі структурних підрозділів (юристи, бухгалтери, працівники терміналів) не повинні мати доступ до тієї інформації, що виходить за межі їх компетенцій.

Окрім налаштування правильних політик доступу та створення віртуальних локальних мереж необхідно імплементувати також систему запобігання вторгнень. Вона надає адміністраторам системи можливість детальної видимості та визначення характеру загроз. Такі видимість та контекстуальна належність дозволяють командам безпеки реагувати за допомогою необхідних ресурсів і успішно мінімізувати наслідки вторгнення.

Ще однією достатньо практично обґрунтованою рекомендацією є впровадження системи моніторингу. Дана система збирає дані з журналів підприємства, мережевих пристроїв, активів хоста та операційних систем, програм,

вразливостей, а також діяльності та поведінки користувачів. Потім виконується аналіз у режимі реального часу, щоб можна було виявити шкідливу активність та швидко її зупинити мінімізувавши наслідки вторгнення.

### Висновки за розділом 3

У третьому розділі було розглянуто особливості побудови інформаційних систем. Створено топологію інформаційної системи державного підприємства. Описано необхідність впровадження низки засобів захисту. Проаналізовано та підібрано програмні засоби, які повинні бути імплементовані в систему для підвищення рівня безпеки. На основі двох підрозділів сформовано третій, метою якого є надання рекомендацій для розробки більш безпечних інформаційних систем на підприємствах, стабільність роботи яких має критично важливе значення.

# ВИСНОВКИ

Безпека та стабільність роботи інформаційної системи державного підприємства є одними з основних характеристик, на які спрямовано фокус адміністраторів та розробників даних систем. Їхня комплексність та кількість надаваних сервісів ускладнюють процес побудови, проте не тільки це є проблемними точками у розробці.

У дипломній роботі розв’язано актуальне питання стосовно забезпечення безпеки складових частин інформаційної системи, беручи до уваги особливості роботи обраної архітектури. Проте основна увага в роботі була сфокусована не тільки на забезпечення безпеки необхідних компонентів, але і на місце їх розташування в системі та забезпечення відмвостійкості.

У ході розв’язання поставлених задач були отримані наступні наукові та практичні результати:

1. Проведено огляд процесу побудови інформаційних систем, їхньої архітектури та структурних особливостей. В якості схеми для розбудови власного прикладу обрано – розподілений тип інформаційних систем.
2. Проведено аналіз вразливостей функціонування розподілених інформаційних систем, які базуються переважно на конструктивних та експлуатаційних недоліках. Безпосередньо ці недоліки дають можливість зловмисникам провести дії для компрометації системи.
3. Формалізовано вимоги до проектування розподілених інформаційних систем з огляду на необхідність побудови захищеної системи. Розглянуто потенційні помилки розробки топології та основні технічні характеристики відповідність яким обов’язково повинна дотримуватися під час роботи системи.
4. Проведено аналіз апаратного забезпечення. Наведено приклади високоякісних, продуктивних та сучасних технічних компонентів, які є основними одиницями в топології підприємства.

5. Запропоновано топологію інформаційної системи. Пояснено необхідність імплементації певних архітектурних рішень з огляду на те, який вплив вони матимуть на продуктивність, рівень безпеки та відмовостійкість усієї системи.

6. Запропоновані програмні продукти для впровадження на різних рівнях функціонування системи. Визначено їхні можливості та вплив на загальний рівень безпеки.

7. Сформульовано рекомендації до розробки топології розподіленої інформаційної системи. Визначено обов’язковість винесення певних ресурсів у DMZ та імплементацію системи моніторингу на підприємстві.

Всі поставлені задачі було виконано в повному обсязі.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. RESEARCH OF METHODS AND MEANS OF PROTECTION OF CENTRALIZED AND DISTRIBUTED INFORMATION SYSTEMS - Access: http://www.engineerxxi.ath.eu/wp-content/uploads/2021/12/engineerxxi_2021_vol4_23.pdf

2. G. F. Coulouris, J. Dollimore, and T. Kindberg, Distributed Systems Concepts and Design, 4th ed. London, England: Addison - Wesley, 2005.

3. T. S. Andrew and M. V. Steen, Distributed Systems: Principles and Paradigms, 2nd ed. Upper Saddle River, NJ, USA: Pearson Higher Education, 2007.

4. Segmentation strategies. Access: https://docs.microsoft.com/ru-ru/azure/architecture/framework/security/design-segmentation

5. How To Protect Your Business From A Data Breach: Seven Key Steps. Access: https://www.forbes.com/sites/forbesfinancecouncil/2018/03/08/how-to-protect-your-business-from-a-data-breach-seven-key-steps/?sh=397caf5e6b68

6. Distributed Systems Security Knowledge Area. Access: https://www.cybok.org/media/downloads/Distributed_Systems_Security_issue_1.0.pdf

7. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д–ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.

8. Про основні засади забезпечення кібербезпеки України [Електронний ресурс]: Закон України №2163-VIII від 15.12.2021. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

9. Проект Стратегії забезпечення кібернетичної безпеки України [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf

10. Щодо кібератак на сайти державних органів [Електронний ресурс] - Режим доступу: https://cip.gov.ua/ua/news/shodo-kiberatak-na-saiti-derzhavnikh-organiv

11. Про захист інформації в інформаційно-комунікаційних системах

[Електронний ресурс]: Закон України № 1089-IX від 16.12.2020. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

12. Технічні та економічні вимоги до інформаційних систем [Електронний ресурс] – Режим доступу: http://www.rusnauka.com/11_EISN_2010/Economics/63505.doc.htm

13. Вимоги до архітектури інформаційної системи для забезпечення безпеки її функціонування [Електронний ресурс] – Режим доступу: https://studme.com.ua/118004088880/informatika/trebovaniya_arhitekture_informatsionnoy_sistemy_dlya_obespecheniya_bezopasnosti_funktsionirovaniya.htm

14. Cisco 4000 Series Routers Data Sheet. Access: https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/data_sheet-c78-732542.html

15. Network switch. Access: https://en.wikipedia.org/wiki/Network_switch#Role_in_a_network

16. Чим відрізняється комутатор L3 від маршрутизатора? [Електронний ресурс] – Режим доступу: https://community.fs.com/ru/blog/layer-3-switch-vs-router-what-is-your-best-bet.html

17. Cisco Catalyst 9500 Series Switches Data Sheet. Access: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html

18. Cisco Catalyst 9200 Switch. Access: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html

19. Cisco Firepower 4110 NGFW Appliance. Access: https://www.secureitstore.com/Firepower-4110.asp

20. Cisco Secure Firewall Management Center. Access: https://www.cisco.com/site/us/en/products/security/firewalls/firewall-management-center/index.html

21. Cisco Firepower 4100 Series Data Sheet. Access: https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html#CiscoFirepower4100Seriesappliances

22. Міжмережевий екран нового покоління Firepower [Електронний ресурс] – Режим доступу: https://www.vtkt.ru/upload/iblock/b20/Cisco%20FirePower_DS.pdf

23. PowerEdge M1000e Technical Guide Access: https://i.dell.com/sites/content/business/solutions/engineering-docs/en/Documents/server-poweredge-m1000e-tech-guidebook.pdf

24. QuickSpecs HP BladeSystem c7000 Enclosure Access: https://www.karma-group.ru/upload/iblock/906/HP_BladeSystem_c7000_Enclosure.91eaf58d81f4e436dab4309acf1c9e691c.pdf

25. Dell EMC PowerEdge XR12 Access: https://i.dell.com/sites/csdocuments/Product_Docs/en/xr12-spec-sheet.pdf

26. DMZ Access: https://www.fortinet.com/resources/cyberglossary/what-is-dmz

27. VLAN (virtual LAN) Access: https://www.techtarget.com/searchnetworking/definition/virtual-LAN

28. How to configure a VLAN to achieve the benefits of VLAN security Access: https://www.techtarget.com/searchsecurity/tip/How-to-configure-a-VLAN-to-achieve-the-benefits-of-VLAN-security

29. Cisco Firepower: Next-Generation Firewall Access: https://www.datashieldprotect.com/tools/cisco-firepower-ngfw

30. Network Access Control List Access: https://www.fortinet.com/resources/cyberglossary/network-access-control-list

31. IBM QRadar SIEM Access: https://www.ibm.com/downloads/cas/RLXJNX2G

32. THUNDER WEB APPLICATION FIREWALL Access: https://www.a10networks.com/wp-content/uploads/A10-SB-19128-EN.pdf

33. Enterprise Security for Endpoints Access: https://www.optrics.com/downloads/trend-micro/ds_enterprise-security-endpoints.pdf

34. Are you giving up on security measures because of their impact on performance and of having to update pattern files? Access: https://www.karma-group.ru/upload/iblock/3ca/safe-lock-datasheet-en.pdf

35. Comparative characteristics of distributed and centralized architecture in the context of creating modern information systems. Access: http://www.medirent.com.ua/presscenter/publications/information_systems_construction.html.

36. Top 15 ways to prevent data and security breaches. Access: https://bigdatamadesimple.com/15-ways-to-prevent-data-security-breaches/

37. TANENBAUM A.S., VAN STEEN M.: Distributed systems principles and paradigms 3rd ed., distributed-systems.net, 2017.

38. Major Centralized Systems are Hacked Multiple Times a Year. Access: https://medium.com/@AxelUnlimited/major-centralized-systems-are-hackedmultiple-times-a-year-9c2ad612462b

39. Distributed Systems. Access: https://komputasi.files.wordpress.com/2018/03/mvsteen-distributed-systems-3rd-preliminary-version-3-01pre-2017-170215.pdf

40. A Guide to Building Dependable Distributed Systems Second Edition Ross J. Anderson. Access: https://terrorgum.com/tfox/books/security_engineering_a_guide_to_building_dependable_distributed_systems.pdf

41. National Security Agency Network Infrastructure Security Guidance. Access: https://media.defense.gov/2022/Mar/01/2002947139/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDANCE_20220301.PDF

# ДОДАТКИ

# ДОДАТОК А

### Тези наукових доповідей

1. IX International Conference of Students, PhD Students and Young Scientists "Engineer of XXI Century" 10th December 2021 - "Research of methods and means of protection of centralized and distributed information systems"
   Valeriia Solodovnyk, Yuliia Stepanenko, Larysa Myrytenko, Andrii Fesenko, Natalia Lukova-Chuiko

### Статті в іноземних виданнях

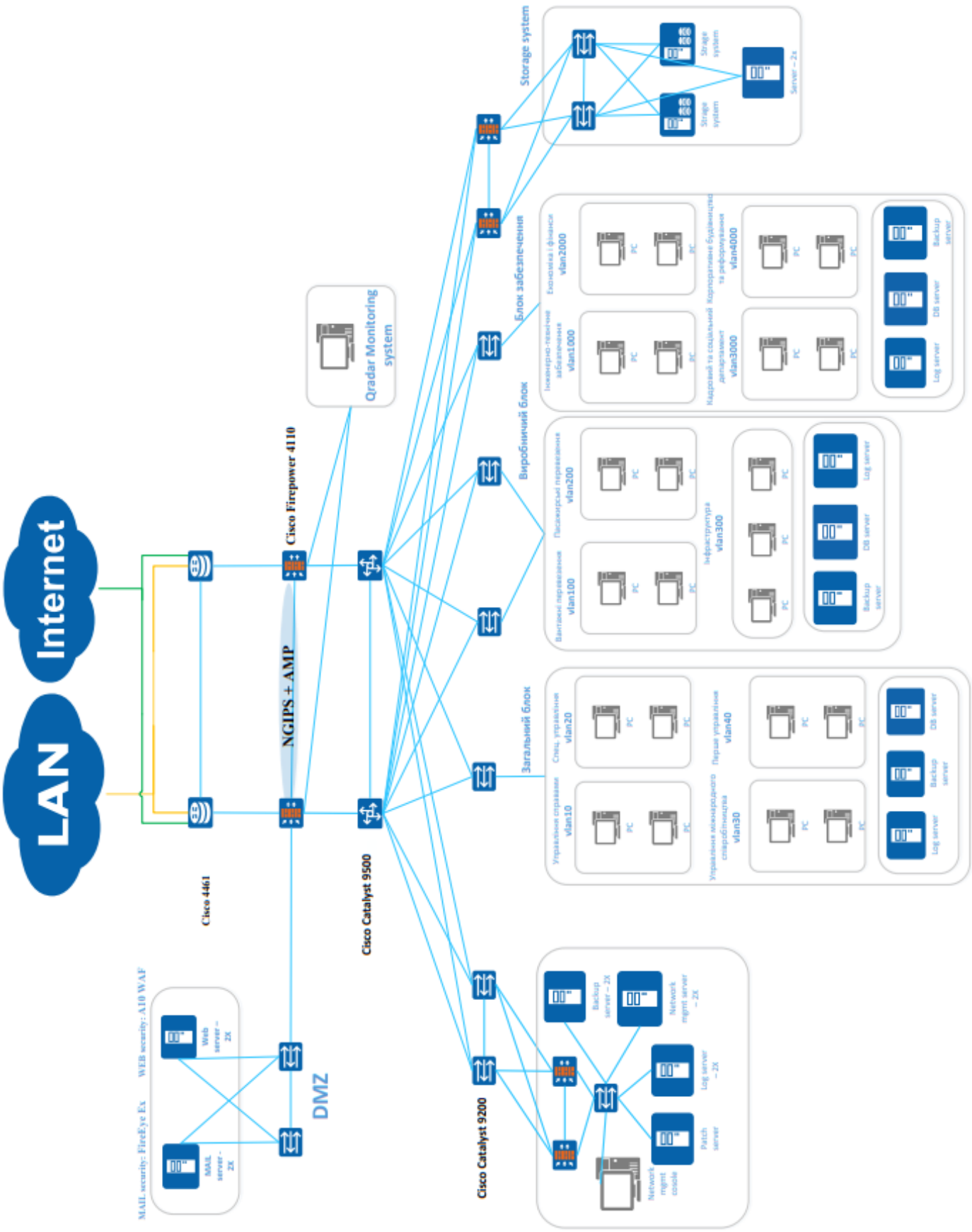
2. IX International Conference of Students, PhD Students and Young Scientists "Engineer of XXI Century" 6th December 2019 - "Analysis of SDN network management by software"  Dakov Serhiy, Valeriia Solodovnyk
3. 2nd International Conference of Cuber Hygiene & Conflict Management in Global Information Networks - "Assessment of the introduction of agents to detect the impact of system level cyber attacs on increasing the data processing center security level«Serhii Toliupa, Yanina Shestak, Ogbu James Onyigwang, Valeriia Solodovnyk
4. "IT&I 2020 Information Technology and Interactions". Тема: "RF Signals Encryption with AES in WDID96-105 Serhii Toliupa, Volodymyr Nakonechnyi, Maksym Kotov, Valeriia Solodovnyk".
5. IX International Conference of Students, PhD Students and Young Scientists "Engineer of XXI Century" 11th December 2020 - "Algorithm of load Balance optimization on hardware resources of information systems«
6. Larysa Murytenko, Valeriia Solodovnyk, Yanina Shestak
   IX International Conference of Students, PhD Students and Young Scientists

"Engineer of XXI Century" 10th December 2021 - "Secure password storage with cryptographic hash function"Yuliia Stepanenko, Valeriia Solodovnyk, Andrii Fesenko, Larysa Myrytenko

**Статті в індексованих міжнарожних виданнях**

1. Scopus indexed publication: "RF signals encryption with AES in WDID Toliupa, S., Nakonechnyi, V., Kotov, M., Solodovnyk, V. CEUR Workshop Proceedingsthis link is disabled, 2021, 2845, pp. 96–105".

# ДОДАТОК Б


Internet
LAN
Cisco 4461
Cisco Firepower 4110
NGIPS + AMP
Cisco Catalyst 9500
Cisco Catalyst 9200
Qradar Monitoring system
DMZ
MAIL security: FireEye Ex
WEB security: A10 WAF
Web server – 2x
MAIL server - 2x
Storage system
Server – 2x
Блок забезпечення
Виробничий блок
Загальний блок
Інженерно-панічне забезпечення vlan1000
Економіка і фінанси vlan2000
Кадровий та соціальний департамент vlan3000
Корпоративне будівництво та реформування vlan4000
Вантажні перевезення vlan100
Пасажирські перевезення vlan200
Інфраструктура vlan300
Управління справами vlan10
Стиль управління vlan20
Управління міжнародного співробітництва vlan30
Перше управління vlan40
PC
Backup server
DB server
Log server
Network mgmt server – 2x
Patch server
Network mgmt console