Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: **Дослідження мережевих архітектур для критичних інфраструктур**

Виконав(ла): студент(ка) 6 курсу, група СНнм-61
спеціальності 122 «Комп'ютерні науки»
(шифр і назва спеціальності)
(підпис) Петрик О.М.
(прізвище та ініціали)

Керівник (підпис) Марценко С.В.
(прізвище та ініціали)
Нормоконтроль (підпис) Мацюк О.В.
(прізвище та ініціали)
Завідувач кафедри (підпис) Боднарчук І.О.
(прізвище та ініціали)
Рецензент (підпис) Яцишин В.В.
(прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
« » 20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня МАГІСТР
(назва освітнього ступеня)

за спеціальністю 122 «Комп'ютерні науки»
(шифр і назва спеціальності)

студенту Петрику Олегу Михайловичу
(прізвище, ім'я, по батькові)

1. Тема роботи **Дослідження мережевих архітектур для критичних інфраструктур**

Керівник роботи **Марценко Сергій Володимирович, к.т.н., доц.**
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 22 » листопада 2022 року № 4/7 950 .

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи технічне завдання на дослідження мережевих архітектур для критичних інфраструктур

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1 Аналіз предметної області; 2 Дослідження мережевих архітектур для критичних інфраструктур; 3 Охорона праці та безпека в надзвичайних ситуаціях; Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Мета, об'єкт предмет дослідження; Завдання дослідження; Основні кроки аналізу критичних інфраструктур; Основні кроки ідентифікації критичних інфраструктур; Хмарні архітектури для критичних інфраструктур; Технологія SDN для критичних інфраструктур; Архітектура мереж для критичних інфраструктур; Моделі архітектур мереж для критичних інфраструктур; Розподілена архітектура; Реалізація різних архітектур для мобільного зв'язку; Реалізація мереж з надлишковими шляхами; Реалізація мережі Juniper на основі віртуалізації; Реалізація мережі VMware для критичної інфраструктури; Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Мацюк О.В., доц. каф. КН		
Безпека в надзвичайних ситуаціях	Клепчик В.М., ст.викл.		

7. Дата видачі завдання _____

1.1 КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	**1.2** Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	14.11.22-15.11.22	*Виконано*
2.	Підбір наукових джерел щодо дослідження	16.11.22-27.11.22	*Виконано*
	мережевих архітектур для критичних інфраструктур		
3.	Переклад та опрацювання наукових джерел щодо	28.11.22-25.12.22	*Виконано*
	мережевих архітектур для критичних інфраструктур		
4.	Виконання дослідження мережевих архітектур для	09.01.23-12.03.23	*Виконано*
	критичних інфраструктур		
5.	Оформлення розділу «Аналіз предметної області»	13.03.23-19.03.23	*Виконано*
6.	Оформлення розділу «Дослідження мережевих	20.03.23-26.03.23	*Виконано*
	архітектур для критичних інфраструктур»		
	Виконання завдання до підрозділу «Охорона праці»	10.04.23-16.04.23	*Виконано*
7.	Виконання завдання до підрозділу «Безпека в	17.04.23-23.04.23	*Виконано*
8.	надзвичайних ситуаціях»		
	Оформлення кваліфікаційної роботи	24.04.23-30.04.23	*Виконано*
9.	Нормоконтроль	01.05.23-07.05.23	*Виконано*
10.	Перевірка на плагіат	08.05.23	*Виконано*
11.	Попередній захист кваліфікаційної роботи	15.05.23	*Виконано*
12.	Захист кваліфікаційної роботи	24.05.2023	

Студент _____ Петрик О.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Марценко С.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження мережевих архітектур для критичних інфраструктур // Кваліфікаційна робота // Петрик Олег Михайлович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно–інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНнм–61 // Тернопіль, 2023 // С. 71 , рис. – 8 , табл. – , кресл. – , додат. – 4 , бібліогр. – 60 .

Ключові слова: МЕРЕЖІ, МЕРЕЖЕВІ АРХІТЕКТУРИ, КРИТИЧНА ІНФРАСТРУКТУРА, ХМАРИ, ВІРТУАЛІЗАЦІЯ.

У роботі проведено дослідження мережевих архітектур для критичних інфраструктур, що дало змогу проаналізувати наявні моделі таких мереж для задач даного класу, визначити сильні та слабкі сторони при їх використанні.

Перший розділ кваліфікаційної роботи описує типи мережевих архітектур, оцінку ризиків для мережевих систем критичних інфраструктур, аналіз заходів безпеки, хмарні архітектури та технології SDN і IBN.

Другий розділ кваліфікаційної роботи досліджує вимоги архітектури мереж критичних інфраструктур, моделі архітектур для різних випадків інфраструктур, реалізацію архітектури на основі рішень вді VMware, безпеку архітектур для критичних інфраструктур.

Метою дослідження є мережеві архітектури для критичних інфраструктур. Об'єкт дослідження – процес отримання, передавання та захисту даних в мережах критичних інфраструктур. Предмет дослідження – теорія проектування телекомунікаційних мереж, теорія передавання даних, теорія захисту інформації.

ANNOTATION

Research of Network Architectures for Critical Infrastructures // Diploma thesis Master degree // Petryk Oleh M. // Ternopil' Ivan Pul'uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science // Ternopil', 2023 // P. 71 , Tables – , Fig. – 8 , Diagrams – , Annexes. – 4 , References – 60 .

The study of network architectures for critical infrastructures was conducted, which made it possible to analyze the existing models of such networks for this class of tasks, to identify strengths and weaknesses in their use.

The first section of the qualification work describes the types of network architectures, risk assessment for critical infrastructure network systems, security analysis, cloud architectures and SDN and IBN technologies.

The second section of the qualification paper explores the requirements of critical infrastructure network architecture, architecture models for different infrastructure cases, architecture implementation based on VMware solutions, and security of architectures for critical infrastructures.

The purpose of the study is network architectures for critical infrastructures. The object of research is the process of receiving, transmitting and protecting data in critical infrastructure networks. The subject of the research is the theory of telecommunication network design, data transmission theory, information security theory.

Keywords: NETWORKS, NETWORK ARCHITECTURES, CRITICAL INFRASTRUCTURE, CLOUDS, VIRTUALIZATION.

ЗМІСТ

Вступ 8
1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ 11
1.1 Аналіз критичних інфраструктур 11
1.2 Ідентифікація критичних інфраструктур 12
1.3 Оцінка ризиків для мережевих систем критичних інфраструктур 13
1.4 Визначення вразливостей мереж для критичних інфраструктур 15
1.5 Аналіз заходів безпеки для мереж критичних інфраструктур 18
1.6 Хмарні архітектури у мережах для критичних інфраструктур 20
1.7 Використання технології SDN у мережевих архітектурах для критичної інфраструктури 26
1.8 Аналіз можливості застосування технології IBN для мережевих архітектур критичної інфраструктури 33
1.9 Висновки до першого розділу 35
2 дослідження мережевих архітектур для критичних інфраструктур 36
2.1 Вимоги архітектури мереж для критичної інфраструктури 36
2.2 Моделі архітектур мереж для критичних інфраструктур 37
2.3 Дослідження мультихмарної архітектури на основі рішень від VMware 46
2.4 Дослідження безпеки мережевих архітектур для критичних інфраструктур 53
2.5 Висновки до другого розділу 56
3 Охорона праці та безпека в надзвичайних ситуаціях 58
3.1 Охорона праці 58
3.1.1 Освітлення робочого місця 58
3.2 Безпека в надзвичайних ситуаціях 61
3.2.1 Основні принципи і способи забезпечення життєдіяльності 61
3.3 Висновки до третього розділу 62

Висновки 3
список літературних джерел 5
Додатки

ВСТУП

Архітектура мереж для критичної інфраструктури в Україні може варіюватися в залежності від конкретної галузі та потреб. Однак, в загальних рисах можна виокремити деякі ключові аспекти.

Україна має розподілену критичну інфраструктуру, що охоплює різні регіони країни. Це означає, що мережева архітектура повинна бути розподіленою, забезпечуючи зв'язок між різними локаціями та об'єктами. Критична інфраструктура потребує високої доступності, щоб забезпечити безперебійну роботу в будь-який час. Мережева архітектура повинна бути резервованою, з дублюванням мережевих шляхів та обладнанням, щоб уникнути відмов та забезпечити неперервну роботу. Забезпечення безпеки мереж є критично важливим аспектом архітектури для критичної інфраструктури. Вона повинна включати захист від кібератак, ідентифікацію та автентифікацію користувачів, шифрування даних, системи виявлення та запобігання вторгнень, а також моніторинг та аудит безпекових подій. Критична інфраструктура може включати об'єкти з великим обсягом даних, наприклад, енергетичні системи, телекомунікаційні мережі тощо. Тому мережева архітектура повинна бути спроектована з врахуванням високої пропускної здатності та швидкодії, щоб забезпечити ефективну передачу даних. Мережева архітектура повинна бути гнучкою та масштабованою, щоб враховувати зростаючі потреби та зміни в критичній інфраструктурі. Вона повинна бути легко розширюваною та здатною до інтеграції з новими технологіями та обладнанням.

Зазначені аспекти є загальними та можуть варіюватися залежно від конкретної галузі критичної інфраструктури в Україні. Крім того, враховується також регуляторне середовище та стандарти безпеки.

Актуальність теми. Дослідження мережевих архітектур для критичних інфраструктур є важливим науково-технічним завданням, оскільки

стосується питань національної безпеки, надійності та продуктивності роботи сервісів, що забезпечують критичні інфраструктури.

Мета і завдання дослідження. Метою дослідження є мережеві архітектури для критичних інфраструктур, дослідження яких дасть змогу створити передумови для вибору найбільш відповідної архітектури для конкретного випадку критичної інфраструктури. Досягнення поставленої мети передбачає виконання наступних завдань: дослідити вимоги до архітектур мереж критичних інфраструктур, моделі реалізації таких архітектур, наявні на ринку пропозиції для організації таких мереж, питання безпеки та оптимізації роботи.

Об’єкт дослідження – процес отримання, передавання та захисту даних в мережах критичних інфраструктур.

Предмет дослідження – теорія проектування телекомунікаційних мереж, теорія передавання даних, теорія захисту інформації.

Практичне значення одержаних результатів. Здійснено ідентифікацію критичних інфраструктур та подано основні кроки для її виконання. Проведено оцінку ризиків для мережевих систем критичних інфраструктур, що дало змогу подати аналіз вразливостей, оцінити ймовірності та наслідки, визначити рівень ризику та подати опис заходів менімізації ризиків. Описано визначення вразливостей мереж для критичних інфраструктур, що є важливим кроком у процесі аналізу безпеки та сітйкості систем. Проаналізовано заходи безпеки для мереж критичних інфраструктур, які слід враховувати при захисті мереж критичних інфраструктур. Проведено опис хмарних архітектурних рішень, що можуть використовуватись у мережах для критичних інфраструктур, що дасть змогу застосувати найкращі можливості різних хмарних технологій. Розглянуто можливість використання технології SDN при проектуванні мережевих архітектур критичних інфраструктур, що показало позитивні елементи у вигляді централізованого керування мережею, динамічної адаптації мережевої інфраструктури, підвищеної безпеки,

масштабованості і швидкого відновлення після відмови. Подано можливість використання технології IBN для мережевих архітектур критичних інфраструктур.

Наукова новизна розробки: визначено та описано вимоги до мережевих архітектур критичних інфраструктур, що повинні враховуватись при їх виборі та впроваджені. Проведено аналіз моделей мережевих архітектур, що дає змогу застосувати найбільш відповідну модель для конкретного випадку критичної інфраструктури. Виявлено, що серед існуючих архітектур в задачах даного класу буде ефективним застосування контернеризації, як гнучкого, швидкодійного та надійного варіанту розгортання сервісів. Здійснено дослідження конкретної реалізації мультихмарної архітектури від компанії VMware, що надає можливість впроваджувати інновації та трансформувати клієнтський досвід, масштабувати і розвивати бізнес, підвищувати залученість та продуктивність працівників. Проект Northstar від VMware базується на використанні SaaS, що для критичних інфраструктур буде надавати програмне забезпечення через хмару для гнучкої та швидкої підтримки управління критичними системами. Даний проект забезпечує узгодженість політик, операцій та автоматизацію в мультихмарних середовищах. Отримавши доступ до хмарної консолі Northstar, підприємства зможуть застосовувати мережеві політики та політики безпеки у своїх приватних хмарних, гібридних та мультихмарних середовищах. Досліджено основні аспекти Кібербезпекового каркасу NIST для критичної інфраструктури. Конкретні вимоги та рекомендації можуть варіюватись залежно від конкретної галузі інфраструктури. Рекомендується ознайомитися з офіційними документами NIST та консультуватися з експертами з безпеки для отримання детальної інформації та порад. Загальний підхід до безпеки повинен включати комплексний підхід, що враховує різні аспекти захисту, включаючи людей, процеси та технології.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз критичних інфраструктур

Аналіз критичних інфраструктур є важливим процесом для оцінки їхньої безпеки, надійності та стійкості. Цей аналіз допомагає виявляти потенційні загрози, визначати вразливості і ризики, а також розробляти заходи для запобігання небажаним подіям та забезпечення відновлення в разі виникнення непередбачуваних ситуацій [1-6].

Основні кроки аналізу критичних інфраструктур включають:

– ідентифікація критичних інфраструктур. Цей крок включає ідентифікацію систем, мереж, об’єктів або послуг, які є життєво важливими для функціонування суспільства. Це можуть бути енергетичні мережі, транспортна інфраструктура, комунікаційні системи, водопостачання, медичні установи та інші системи, які гарантують безпеку і добробут населення;

– оцінка ризиків. Після ідентифікації критичних інфраструктур проводиться оцінка потенційних ризиків, зокрема визначення загроз, які можуть впливати на ці інфраструктури. Це можуть бути природні катастрофи, техногенні аварії, кібератаки, терористичні акти тощо. Оцінка ризиків включає аналіз вірогідності виникнення загрози та можливих наслідків;

– визначення вразливостей. Проводиться аналіз критичних інфраструктур для виявлення потенційних вразливостей. Це можуть бути технічні вразливості систем, недоліки у безпеці мереж, недостатня захищеність даних, проблеми управління та інші аспекти, які можуть стати точкою входу для атак або привести до непередбачуваних ситуацій;

– розробка заходів безпеки. На основі оцінки ризиків і виявлених вразливостей розробляються заходи безпеки для захисту критичних

інфраструктур. Це можуть бути технічні заходи, такі як використання шифрування, автентифікація, контроль доступу, резервне копіювання даних тощо, а також організаційні заходи, такі як політики безпеки, навчання персоналу, реагування на інциденти тощо;

– планування надійності та відновлення. Розробляються плани надійності та відновлення для критичних інфраструктур. Ці плани включають заходи для забезпечення стійкості, швидкого відновлення та відновлення після виникнення аварійних ситуацій або атак.

Аналіз критичних інфраструктур є постійним процесом, оскільки загрози та вразливості можуть змінюватись з часом. Оновлення та перевірка заходів безпеки є важливим аспектом забезпечення надійності та безпеки критичних систем.

1.2 Ідентифікація критичних інфраструктур

Ідентифікація критичних інфраструктур є першим і важливим кроком в аналізі безпеки та стійкості систем, які забезпечують життєво важливі послуги. Основна мета цього процесу полягає в тому, щоб визначити системи, мережі, об’єкти або послуги, які, якщо вони вийдуть з ладу або піддаються атакам, можуть мати серйозні наслідки для функціонування суспільства або призвести до значних втрат життя або майна [7-10].

Основні кроки ідентифікації критичних інфраструктур включають:

– визначення секторів. Спочатку встановлюються різні сектори критичних інфраструктур, такі як енергетика, транспорт, комунікації, фінанси, водопостачання, медичні послуги тощо. Цей крок допомагає організувати процес ідентифікації та фокусувати увагу на конкретних галузях;

– аналіз систем. Далі проводиться детальний аналіз кожного сектора для визначення систем, компонентів або об'єктів, які грають ключову

роль у забезпеченні безпеки та функціонування цього сектора. Наприклад, у секторі енергетики це можуть бути електростанції, підстанції, трансформатори, енергетичні мережі тощо;

– оцінка важливості. Кожна ідентифікована система або компонент оцінюється щодо її важливості для функціонування суспільства та життєвої безпеки. Це може включати оцінку потенційних наслідків в разі відмови або атаки на ці системи, визначення їхнього впливу на суспільство та інші чинники;

– встановлення пріоритетів. На основі оцінки важливості системи встановлюються пріоритети. Це допомагає визначити, які системи потребують особливої уваги та заходів безпеки, які мають високий пріоритет у відновленні після аварійних ситуацій або атак;

– консультації та співробітництво. Ідентифікація критичних інфраструктур є складним процесом, і вона вимагає взаємодії з експертами, органами управління кризовими ситуаціями, представниками сектору та іншими стейкхолдерами. Співробітництво та обмін інформацією допомагають уточнити ідентифікацію та враховувати різноманітні аспекти безпеки та стійкості.

Ідентифікація критичних інфраструктур є постійним процесом, оскільки нові системи можуть з’являтись або існуючі можуть змінюватись з часом. Цей процес допомагає краще розуміти уразливості та ризики, що дозволяє впроваджувати ефективні заходи безпеки та стійкості.

1.3 Оцінка ризиків для мережевих систем критичних інфраструктур

Оцінка ризиків критичних інфраструктур є важливим етапом у забезпеченні безпеки та стійкості систем. Цей процес допомагає виявити

потенційні загрози, визначити їх вплив та імовірність виникнення, а також встановити пріоритети для впровадження заходів безпеки [11-17].

Основні кроки оцінки ризиків критичних інфраструктур включають:

– ідентифікація загроз. Спочатку визначаються потенційні загрози, які можуть вплинути на критичні інфраструктури. Це можуть бути природні катастрофи, техногенні аварії, кібератаки, терористичні акти, соціальні та економічні загрози тощо. Важливо враховувати як загрози зовнішнього походження, так і внутрішні фактори, що можуть стати причиною виникнення аварійних ситуацій;

– аналіз вразливостей. Проводиться оцінка вразливостей критичних інфраструктур, тобто їхніх слабких місць або потенційних точок входу для загроз. Це можуть бути технічні вразливості, такі як недостатня захищеність мереж, недоліки у програмному забезпеченні, фізичні слабкі місця, а також організаційні вразливості, такі як недостатня свідомість персоналу про безпеку, неадекватні процедури управління ризиками тощо;

– оцінка імовірності та наслідків. Здійснюється оцінка імовірності виникнення загрози та можливих наслідків цієї загрози для критичних інфраструктур. Це може включати аналіз історичних даних, експертні оцінки, моделювання ризиків та імовірнісних сценаріїв. Результати оцінки можуть бути представлені у вигляді рейтингу ризиків або іншої форми категоризації;

– визначення рівня ризику. На основі оцінки імовірності та наслідків ризику встановлюється рівень загрози для критичних інфраструктур. Це допомагає визначити пріоритети для впровадження заходів безпеки та алокації ресурсів;

– розробка заходів мінімізації ризиків. На основі оцінки ризиків розробляються конкретні заходи для мінімізації ризиків. Це можуть бути технічні заходи, такі як захист мереж, шифрування, моніторинг систем, а також організаційні заходи, такі як плани надійності, політики безпеки, навчання персоналу, плани реагування на інциденти тощо.

Оцінка ризиків критичних інфраструктур є ітеративним процесом, який потребує постійного моніторингу та оновлення, оскільки загрози та умови змінюються з часом.

1.4 Визначення вразливостей мереж для критичних інфраструктур

Дослідження комп’ютерних мереж для критичної інфраструктури є важливим аспектом забезпечення безпеки та надійності систем, які забезпечують життєво важливі послуги, наприклад, електроенергію, транспортні системи, медичні установи тощо. Оскільки критична інфраструктура має велику значущість для функціонування суспільства, недостовірність або відмова в роботі може мати серйозні наслідки [18-24].

Основні аспекти дослідження комп’ютерних мереж для критичної інфраструктури включають:

– аналіз вразливостей. Дослідники вивчають різні аспекти мережі, виявляють потенційні вразливості і ризики. Це може включати аналіз можливих атак, шляхів проникнення та розвитку загроз безпеці;

– розробка заходів безпеки. На основі результатів аналізу вразливостей, дослідники розробляють та тестують різні заходи безпеки. Це можуть бути технологічні заходи, такі як шифрування даних, аутентифікація та контроль доступу, а також організаційні заходи, такі як політики безпеки та навчання персоналу;

– аналіз мережевої інфраструктури. Дослідження включає детальний аналіз мережевої інфраструктури критичних систем. Це може включати оцінку мережевих протоколів, архітектури мережі, фізичного забезпечення, резервування та механізмів відновлення;

– тестування імітацією атак. Дослідження мереж для критичної інфраструктури включає проведення тестів, які моделюють реальні атаки для

оцінки стійкості систем. Це може включати пенетраційні тести, аналіз відновлення після відмови, тестування стійкості до перенавантаження тощо;

– розробка резервних планів. Дослідники працюють над розробкою ефективних резервних планів для критичної інфраструктури в разі відмови або атаки. Це можуть бути плани відновлення, резервні мережеві маршрутизатори, механізми автоматичного відновлення тощо.

Дослідження комп'ютерних мереж для критичної інфраструктури допомагають виявляти потенційні загрози та ризики, розробляти та впроваджувати ефективні заходи безпеки та забезпечувати стійкість і надійність систем, що забезпечують життєво важливі послуги.

Визначення вразливостей мереж критичних інфраструктур є важливим кроком у процесі аналізу безпеки та стійкості систем. Цей процес допомагає ідентифікувати слабкі місця та потенційні ризики, що можуть бути використані для атак або порушення функціонування мережі.

Основні кроки визначення вразливостей мереж критичних інфраструктур включають:

– інвентаризація мережі. Спочатку проводиться інвентаризація всіх компонентів та пристроїв мережі критичної інфраструктури. Це включає сервери, комутатори, маршрутизатори, файрволи, безпроводові точки доступу та інші активні пристрої. Також варто враховувати підключені системи та залежності між ними;

– виявлення потенційних вразливостей. За допомогою спеціалізованих інструментів та методів проводиться сканування мережі для виявлення потенційних вразливостей. Це можуть бути вразливості в операційних системах, програмному забезпеченні, конфігураційні проблеми, слабкі паролі, відкриті порти тощо;

– аналіз результів сканування. Отримані результати сканування аналізуються та оцінюються. Приділяється увага критичним вразливостям, які можуть мати серйозний вплив на безпеку та функціонування мережі.

Важливо визначити потенційний вплив кожної вразливості, включаючи можливі наслідки та ймовірність зловживання;

– перевірка відповідності стандартам безпеки. Порівнюються виявлені вразливості з встановленими стандартами безпеки. Наприклад, можуть бути використані стандарти, такі як ISO 27001 або NIST Cybersecurity Framework, для оцінки безпеки мережі та визначення відповідності;

– перевірка заходів безпеки. Оцінюються наявні заходи безпеки та їх ефективність. Перевіряється, чи використовуються найкращі практики забезпечення безпеки мережі, такі як застосування патчів, використання сильних паролів, обмеження прав доступу, шифрування даних тощо;

– розробка плану заходів. На основі отриманих результатів розробляється план заходів для виправлення виявлених вразливостей. Це можуть бути технічні заходи, такі як встановлення патчів, конфігураційні зміни, удосконалення систем моніторингу та виявлення вторгнень, а також організаційні заходи, такі як навчання персоналу, усвідомлення безпеки, політики та процедури управління ризиками.

Основні елементи архітектури стандарту ISO 27001 зображено на малюнку 1.1.

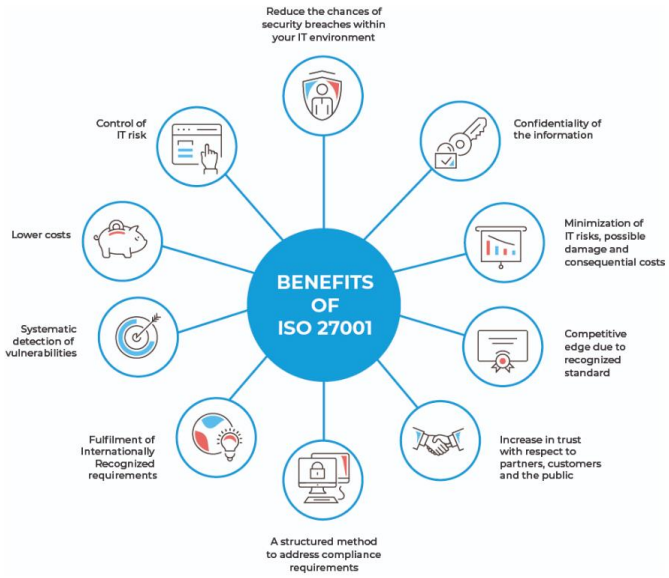

Рисунок 1.1 – Архітектура стандарту ISO 27001

Відповідність будь якої архітектури загальновизнаним стандартам надає можливість сертифікувати такі мережі, що в свою чергу уможливлює використання визначених підходів у подальшому обслуговування та експлуатації таких мереж.

Важливо зауважити, що визначення вразливостей мережі критичної інфраструктури є постійним процесом і вимагає регулярного моніторингу та оновлення, оскільки вразливості можуть змінюватись з часом або з'являтись нові загрози.

1.5 Аналіз заходів безпеки для мереж критичних інфраструктур

Заходи безпеки для мереж критичних інфраструктур включають широкий спектр заходів, що мають на меті забезпечити конфіденційність, цілісність та доступність мережі [25]. Ось декілька важливих заходів безпеки:

– періодичне оновлення програмного забезпечення. Важливо мати механізми для постійного оновлення програмного забезпечення на всіх компонентах мережі. Це включає операційні системи, програми, пристрої мережевого обладнання тощо. Оновлення включають в себе патчі безпеки та виправлення вразливостей;

– сильні аутентифікаційні механізми. Необхідно використовувати сильні аутентифікаційні механізми, такі як паролі довжиною не менше 12 символів, використання двофакторної аутентифікації, використання сертифікатів тощо. Потрібно заборонити використання слабких або загальновідомих паролів;

– контроль доступу. встановлення механізмів контролю доступу для обмеження прав доступу користувачів до ресурсів мережі. Використовуйте принцип найменших привілеїв (Principle of Least Privilege), щоб кожен користувач мав тільки ті права, які необхідні для виконання своїх обов’язків;

– моніторинг мережі. потрібно забезпечити використання системи моніторингу мережі для виявлення незвичних активностей, вторгнень або аномалій в мережевому трафіку. Це можуть бути системи виявлення вторгнень (IDS/IPS), системи журналювання подій, аналітика безпеки тощо. Встановити реагування на виявлені загрози та атаки вчасно;

– захист від зовнішніх загроз. забезпечити захисні механізми на рівні периметра мережі, такі як файрволи, системи фільтрації трафіку, системи захисту від DDoS-атак. Це допоможе зменшити вплив можливих зовнішніх загроз на мережу;

– резервне копіювання даних. Регулярно створюйте резервні копії даних мережі та забезпечуйте їх захищений зберігання. Це дозволить відновити дані в разі випадкового видалення, аварій або витоку інформації;

– конфігураційне управління. ведення систематичного контролю конфігурацій мережевого обладнання, програмного забезпечення та сервісів. Використання стандартизованих конфігураційних шаблонів та процесів для забезпечення відповідності та усунення вразливостей;

– навчання та свідомість користувачів. Забезпечення навчання користувачів про основні правила безпеки, розпізнавання фішингових атак, безпечне використання паролів та інших мережевих ресурсів. Регулярно нагадуйте про правила безпеки та оновлюйте свідомість персоналу;

– аудит безпеки. проведення регулярних аудитів безпеки мережі для виявлення потенційних вразливостей та недоліків у заходах безпеки. Аудити допоможуть ідентифікувати можливі проблеми та вжити відповідних заходів для їх вирішення.

Це лише декілька основних заходів безпеки, які слід враховувати при захисті мереж критичних інфраструктур. Залежно від конкретної інфраструктури та вимог безпеки, можуть використовуватись й інші техніки та методи.

1.6 Хмарні архітектури у мережах для критичних інфраструктур

Хмарні архітектури можуть бути використані для побудови критичних інфраструктур з метою забезпечення високої доступності, масштабованості та безпеки [26-31]. Нижче наведено декілька розглянутих хмарних архітектур для критичних інфраструктур:

– хмарні приватні мережі (Private Clouds). Приватна хмарна архітектура надає повний контроль над інфраструктурою та дозволяє виробникам керувати інфраструктурою власними силами. Це особливо важливо для критичних інфраструктур, де безпека та конфіденційність є пріоритетом. Приватні хмарні мережі можуть бути розгорнуті власними силами або використовуючи послуги провайдерів приватних хмар;

– хмарні гібридні мережі (Hybrid Clouds). Гібридна хмарна архітектура поєднує приватну і публічну хмарні інфраструктури. Критичні дані та додатки можуть бути розміщені в приватній хмарі, забезпечуючи високий рівень безпеки, тоді як менш критичні ресурси можуть бути розміщені в публічній хмарі для більшої масштабованості та гнучкості;

– мультихмарні архітектури (Multi-Clouds). Мультихмарні архітектури передбачають використання різних публічних хмарних провайдерів для розміщення критичних інфраструктурних ресурсів. Це дозволяє розподіляти ризики та забезпечувати високу доступність шляхом розміщення ресурсів на різних хмарних платформах;

– архітектура багатошарових хмар (Multi-tier Cloud Architecture). Ця архітектура передбачає розміщення різних рівнів додатків та сервісів на різних хмарних платформах. Критичні компоненти можуть бути розміщені в приватній хмарі, тоді як менш критичні компоненти можуть бути розміщені в публічній хмарі. Це забезпечує кращий контроль над безпекою та надійністю критичних ресурсів;

– резервування та відновлення (Backup and Recovery). Критичні інфраструктури повинні мати механізми резервного копіювання та відновлення даних. Хмарні платформи можуть надавати інтегровані механізми резервного копіювання та відновлення, що дозволяють швидко відновлювати дані у разі аварій або випадкового видалення;

– захист даних та конфіденційність. Хмарні архітектури повинні забезпечувати механізми шифрування даних, контролю доступу та моніторингу для забезпечення конфіденційності та захисту даних. Критичні дані мають бути шифрованими під час транзиту та зберігання.

Ці архітектури можуть бути поєднані та налаштовані відповідно до конкретних вимог критичних інфраструктур. Важливо враховувати безпеку, доступність та вимоги до даних при виборі хмарної архітектури для критичних інфраструктур.

Хмарні приватні мережі є одним із варіантів хмарних архітектур, які можуть бути використані для побудови критичних інфраструктур. Приватна хмарна мережа надає повний контроль над інфраструктурою та дозволяє забезпечити високий рівень безпеки, конфіденційності та доступності даних. Ось кілька ключових характеристик та переваг хмарних приватних мереж для критичних інфраструктур:

– безпека та конфіденційність. Хмарні приватні мережі забезпечують вищий рівень безпеки, оскільки інфраструктура контролюється власними силами організації. Критичні дані можуть бути збережені в межах приватної мережі, що дозволяє забезпечити конфіденційність та захист від несанкціонованого доступу;

– контроль над інфраструктурою. Організації мають повний контроль над конфігурацією та керуванням приватної хмарної мережі. Вони можуть визначати параметри безпеки, мережеві політики та масштабування, що дає більшу гнучкість і відповідність вимогам критичних інфраструктур;

– висока доступність та надійність. Приватні хмарні мережі можуть бути розгорнуті з використанням географічно розподілених центрів обробки даних, що забезпечує високу доступність та надійність. Резервування ресурсів, реплікація даних та механізми відновлення допомагають уникнути відмов у роботі та забезпечують безперебійну роботу критичних інфраструктур;

– вищий рівень налаштування. У приватних хмарних мережах організації можуть використовувати спеціалізоване обладнання та рішення, які відповідають їх потребам. Це дозволяє забезпечити оптимальну продуктивність, швидкість та низьку латентність для критичних додатків та сервісів;

– внутрішня комунікація та пропускна здатність. Приватні хмарні мережі дозволяють організаціям забезпечувати внутрішню комунікацію між різними компонентами і системами в межах мережі. Це полегшує інтеграцію додатків та забезпечує високу пропускну здатність для обміну даними між різними складовими критичної інфраструктури.

Хмарні приватні мережі можуть бути побудовані власними силами організації або за допомогою послуг провайдерів приватних хмар. Вибір підходящого рішення залежить від вимог безпеки, доступності та гнучкості критичної інфраструктури.

Хмарні гібридні мережі є популярним варіантом архітектури для критичних інфраструктур, оскільки поєднують переваги як приватних, так і публічних хмарних середовищ. Вони дозволяють організаціям комбінувати різні рівні безпеки, контролю та гнучкості для відповідності вимогам критичних інфраструктур. Ось деякі важливі аспекти хмарних гібридних мереж для критичних інфраструктур:

– розподіл ресурсів. Гібридна архітектура дозволяє розподіляти ресурси між приватною і публічною хмарними середовищами. Критичні компоненти та дані можуть бути розміщені в приватній хмарі, забезпечуючи

вищий рівень безпеки та контролю, тоді як менш критичні компоненти можуть бути розміщені в публічній хмарі для більшої масштабованості та гнучкості;

– гнучкість масштабування. Гібридні мережі дозволяють організаціям масштабувати ресурси в залежності від потреб. При необхідності можна розширювати потужність приватної хмари або використовувати додаткові ресурси з публічної хмари. Це дозволяє забезпечити високу доступність та продуктивність критичних систем;

– безпека та конфіденційність. В гібридних мережах організації можуть зберігати критичні дані в приватній хмарі, що дозволяє забезпечити вищий рівень безпеки та контролю над даними. В той же час, менш критичні дані можуть бути розміщені в публічній хмарі з додатковими заходами безпеки, такими як шифрування та контроль доступу;

– резервне копіювання та відновлення. Гібридні мережі дозволяють організаціям реалізувати механізми резервного копіювання та відновлення даних. Критичні дані можуть бути резервованими в приватній хмарі, забезпечуючи швидке відновлення у разі аварій або випадкового видалення;

– керування та моніторинг. Гібридні мережі вимагають ефективного керування та моніторингу для забезпечення безпеки, доступності та продуктивності. Управління може здійснюватися через централізовану систему керування, що надає організації повний контроль над інфраструктурою.

Гібридні мережі дозволяють організаціям використовувати найкращі можливості приватних і публічних хмарних середовищ для побудови критичних інфраструктур. Вони забезпечують баланс безпеки, контролю, масштабованості та гнучкості, що є важливими факторами для успішного функціонування критичних систем [32].

Мультихмарні архітектури для критичних інфраструктур використовуються для поєднання різних хмарних середовищ в одну єдину

мережу. Це дозволяє організаціям отримати переваги кількох хмарних платформ і забезпечити високий рівень безпеки, доступності та гнучкості для критичних систем. Ось деякі основні аспекти мультихмарних архітектур для критичних інфраструктур:

– гнучкість та розширюваність. Мультихмарні архітектури дозволяють організаціям використовувати різні хмарні середовища, такі як публічна хмара, приватна хмара або гібридна хмара, залежно від потреб. Це дає можливість розширювати ресурси та забезпечувати гнучкість для критичних систем, незалежно від обмежень однієї платформи;

– забезпечення високої доступності. Мультихмарні архітектури дозволяють розміщувати критичні компоненти та дані на різних хмарних платформах і географічно розподілених центрах обробки даних. Це забезпечує високу доступність та надійність, оскільки випадкові відмови або проблеми в одній платформі не призводять до повної недоступності системи;

– безпека та контроль. Мультихмарні архітектури дозволяють організаціям встановлювати власні політики безпеки, контролю доступу та шифрування для кожної хмарної платформи. Це дозволяє забезпечити вищий рівень безпеки та захисту даних для критичних систем;

– оптимізація ресурсів. Мультихмарні архітектури дозволяють розподіляти ресурси між різними хмарними платформами в залежності від їх використання та потреб. Це дозволяє оптимізувати витрати на ресурси та забезпечити ефективне використання інфраструктури;

– управління та моніторинг. Мультихмарні архітектури вимагають централізованого управління та моніторингу для забезпечення безпеки, доступності та продуктивності критичних систем. Це може включати в себе централізовану панель керування, механізми моніторингу та автоматизацію процесів управління.

Мультихмарні архітектури дозволяють організаціям використовувати найкращі можливості різних хмарних платформ для побудови критичних

інфраструктур. Вони забезпечують гнучкість, доступність та безпеку, необхідні для успішного функціонування критичних систем в сучасному цифровому середовищі.

Архітектура багатошарових хмар (Multi-tier Cloud Architecture) є популярним підходом для побудови критичних інфраструктур у хмарному середовищі. Вона використовує різні рівні абстракції та функціональні компоненти для забезпечення безпеки, масштабованості та доступності системи. Ось основні компоненти та їх характеристики в архітектурі багатошарових хмар для критичних інфраструктур:

– рівень додатків (Application Layer). Це верхній рівень архітектури, де розміщуються додатки та бізнес-логіка. Додатки можуть бути розгорнуті у віртуальних машинах або контейнерах. На цьому рівні реалізується логіка обробки даних та виконання бізнес-процесів;

– рівень сервісів (Service Layer). Цей рівень включає сервіси, які надаються додатками. Це можуть бути сервіси автентифікації, авторизації, кешування, моніторингу тощо. Сервіси на цьому рівні забезпечують додаткам додаткові функціональні можливості та підтримують вимоги до безпеки та продуктивності;

– рівень платформи (Platform Layer). Цей рівень включає середовище виконання, таке як віртуальні машини, контейнери, бази даних тощо. Він забезпечує інфраструктурну підтримку для додатків і сервісів, включаючи масштабування, управління ресурсами, моніторинг і автоматизацію;

– рівень інфраструктури (Infrastructure Layer). Цей рівень включає фізичну інфраструктуру, таку як сервери, мережеві компоненти, сховища даних тощо. Він забезпечує апаратну підтримку для верхніх рівнів і включає механізми безпеки, резервного копіювання, відновлення та забезпечення надійності;

– рівень мережі (Network Layer). Цей рівень відповідає за комунікацію між компонентами архітектури. Він включає мережеві протоколи, маршрутизацію, балансування навантаження, мережеву безпеку та інші механізми, що забезпечують з’єднання та комунікацію між різними компонентами системи.

В архітектурі багатошарових хмар кожен рівень відповідає за свою функцію і має відокремлену відповідальність, що дозволяє забезпечити модульність, масштабованість та безпеку критичних інфраструктур. Ця архітектура дозволяє гнучко налаштовувати рівні сервісів та ресурсів відповідно до вимог критичних додатків і забезпечує ефективне функціонування системи у хмарному середовищі.

1.7 Використання технології SDN у мережевих архітектурах для критичної інфраструктури

Технологія SDN (Software-Defined Networking) може бути використана в критичних інфраструктурах для поліпшення безпеки, масштабованості та керованості мережі [33-37]. Наведемо деякі способи використання технології SDN у критичних інфраструктурах:

– централізоване керування мережею. За допомогою SDN можна створити централізовану панель керування мережею, що дозволяє адміністраторам централізовано налаштовувати, керувати та моніторити мережеві пристрої і політики. Це спрощує управління мережею критичної інфраструктури та дозволяє швидко реагувати на зміни та виявляти проблеми в реальному часі;

– динамічна адаптація мережевої інфраструктури. SDN дозволяє динамічно налаштовувати мережеві ресурси в залежності від вимог критичних додатків та навантаження. Це дозволяє оптимізувати

використання ресурсів і забезпечує ефективну роботу мережі навіть при змінних умовах роботи;

– безпека мережі. SDN може забезпечити покращену безпеку мережі в критичних інфраструктурах. Це можна досягнути за допомогою централізованого контролю доступу, шифрування трафіку, моніторингу та виявлення вторгнень. SDN також дозволяє впровадження політик безпеки на рівні програмного забезпечення та швидку реакцію на загрози безпеки;

– масштабованість. SDN може допомогти забезпечити масштабованість мережі в критичних інфраструктурах. Це досягається шляхом відокремлення керування мережею від фізичної інфраструктури, що дозволяє легко масштабувати мережу, додавати нові ресурси та розширювати функціональність;

– відновлення після відмови. SDN дозволяє швидко відновлювати мережеві послуги після відмови або аварії. За допомогою централізованого керування, можна легко переключати трафік на альтернативні шляхи або резервні ресурси, забезпечуючи неперервність роботи критичних систем.

Застосування технології SDN у критичних інфраструктурах допомагає підвищити ефективність, надійність та безпеку мережі. Вона дозволяє адаптуватися до змінних умов, ефективно використовувати ресурси та швидко реагувати на проблеми.

Централізоване керування мережею SDN в критичних інфраструктурах може бути важливим елементом для забезпечення ефективності, безпеки та керованості. Основні переваги централізованого керування мережею SDN включають:

Централізований контроль: За допомогою SDN-контролера, адміністратори мережі можуть централізовано налаштовувати, керувати та моніторити всю мережеву інфраструктуру. Це дозволяє забезпечити єдиний пункт керування, спрощує управління мережею і дозволяє швидко реагувати на зміни та проблеми.

– гнучкість та адаптивність. Централізоване керування дозволяє адміністраторам легко налаштовувати політики мережі, включаючи маршрутизацію, керування пропускною здатністю, безпеку та якість обслуговування. Це дозволяє швидко адаптувати мережу до змінних вимог і забезпечувати оптимальну продуктивність;

– централізований моніторинг і аналітика. Централізоване керування дозволяє збирати дані про стан мережі з різних пристроїв і аналізувати їх для виявлення проблем, оптимізації ресурсів та прийняття управлінських рішень. Це покращує відладку, моніторинг та аналіз мережевої продуктивності в реальному часі;

– безпека. Централізоване керування дозволяє впроваджувати політики безпеки на рівні програмного забезпечення, контролювати доступ до ресурсів та виявляти аномалії в мережі. Адміністратори можуть швидко реагувати на потенційні загрози та впроваджувати заходи безпеки на всіх рівнях мережі;

– управління більшими масштабами. Централізоване керування дозволяє керувати мережевими ресурсами в розподіленому середовищі. Це особливо корисно для критичних інфраструктур, які можуть включати розподілені мережі на різних географічних об'єктах. За допомогою SDN, адміністратори можуть керувати всіма цими ресурсами з одного централізованого місця.

Централізоване керування мережею SDN забезпечує більшу гнучкість, керованість та безпеку в критичних інфраструктурах, дозволяючи адміністраторам зосередитися на стратегічних аспектах управління мережею та швидко реагувати на зміни та загрози.

Динамічна адаптація мережевої інфраструктури SDN в критичних інфраструктурах дозволяє пристосовувати мережу до змінних умов та вимог, забезпечуючи ефективну роботу систем. Ось декілька аспектів, пов'язаних з динамічною адаптацією мережевої інфраструктури SDN:

– гнучкість маршрутизації. У традиційних мережах маршрутизація часто є статичною і налаштовується вручну. За допомогою SDN, маршрутизація може бути динамічною та автоматичною. Це означає, що маршрути можуть змінюватися в реальному часі в залежності від умов мережі, трафіку та вимог додатків. SDN контролер може аналізувати стан мережі та приймати рішення щодо оптимальних маршрутів для передачі даних;

– динамічне керування пропускною здатністю. SDN дозволяє динамічно управляти пропускною здатністю мережі. За допомогою контролера SDN, можна змінювати політики керування пропускною здатністю на основі поточних потреб додатків. Наприклад, в моменти пікового навантаження можна виділяти більше пропускної здатності для критичних додатків та регулювати її в інший час. Це дозволяє ефективно використовувати ресурси мережі та забезпечувати потрібну продуктивність;

– автоматичне виявлення і відновлення. SDN може допомогти виявити проблеми в мережі та автоматично відновити роботу. Контролер SDN може моніторити стан мережевих пристроїв, з'ясовувати, чи вони працюють належним чином, та виявляти відмови. При виявленні проблеми контролер може автоматично перенаправити трафік на альтернативні шляхи або резервні ресурси, щоб забезпечити неперервну роботу системи;

– автоматизація та оркестрація. SDN дозволяє автоматизувати багато рутинних завдань управління мережею. Адміністратори можуть створювати політики та правила, що автоматично виконуються контролером SDN. Це дозволяє спростити процеси конфігурації, моніторингу та управління мережею;

– гнучкість та масштабованість. SDN надає гнучкість та масштабованість для критичних інфраструктур. За допомогою SDN, можна легко додавати нові ресурси, розширювати мережу та адаптуватися до змін

вимог. SDN дозволяє впроваджувати нові сервіси та додатки без необхідності фізичного переконфігурування мережі.

Використання технології SDN для динамічної адаптації мережевої інфраструктури у критичних інфраструктурах допомагає забезпечити ефективну роботу систем, швидку реакцію на зміни та максимальну надійність.

Безпека мереж SDN є важливим аспектом для критичних інфраструктур, оскільки вони мають високу вразливість до кібератак. Основні аспекти безпеки мереж SDN для критичних інфраструктур включають:

– аутентифікація та авторизація. Система SDN повинна мати механізми аутентифікації та авторизації, які перевіряють ідентифікацію та права доступу користувачів до мережевих ресурсів. Це дозволяє управляти доступом до контролерів SDN та мережевих пристроїв і забезпечувати, що лише авторизовані користувачі мають право керувати мережею;

– контроль доступу. Важливо мати механізми контролю доступу, які встановлюють політики доступу до мережевих ресурсів на основі ролей або правил. Такі механізми дозволяють обмежувати доступ до критичних ресурсів та застосовувати принцип найменшого дозволеного доступу (Principle of Least Privilege);

– захист комунікації. Комунікація між контролерами SDN, мережевими пристроями та додатками повинна бути захищеною. Використання шифрування та протоколів безпеки, таких як Transport Layer Security (TLS), допомагає уникнути перехоплення та зловживання даними під час передачі по мережі;

– виявлення та відповідь на загрози. Система SDN повинна мати механізми для виявлення та відповіді на потенційні кіберзагрози. Використання системи моніторингу та аналізу мережі допомагає виявляти аномалії та незвичайну активність в реальному часі. Крім того, реалізація

системи реагування на інциденти (Incident Response) дозволяє швидко реагувати на загрози та вживати відповідних заходів безпеки;

– сегментація мережі. Сегментація мережі допомагає обмежити розповсюдження атак та зменшити вплив вразливостей. Шляхом розділення мережі на логічні сегменти та застосування політик безпеки можна обмежити доступ до критичних ресурсів тільки для необхідних пристроїв та користувачів;

– аудит безпеки. Система SDN повинна мати можливість записувати журнали подій (logs) та проводити аудит безпеки. Це дозволяє відстежувати події, виявляти незвичайну активність та проводити розслідування в разі інцидентів.

Враховуючи ці аспекти безпеки, критичні інфраструктури можуть використовувати мережі SDN з високим рівнем захисту від кібератак та забезпечувати безперебійну та надійну роботу систем [38-40].

Масштабованість є важливою характеристикою для мереж SDN в критичних інфраструктурах, оскільки такі мережі повинні бути готовими впоратися з великим обсягом трафіку та змінювати розмір та склад мережі в залежності від потреб системи. Ось декілька аспектів масштабованості SDN для мереж критичних інфраструктур:

– горизонтальне масштабування. SDN дозволяє горизонтальне масштабування, що означає додавання нових фізичних або віртуальних ресурсів до мережі для забезпечення більшої пропускної здатності та обробки трафіку. За допомогою контролера SDN, можна легко додавати нові комутатори або віртуальні мережеві функції (VNF) та інтегрувати їх у загальну мережу;

– вертикальне масштабування. SDN також дозволяє вертикальне масштабування, що означає збільшення ресурсів або потужності існуючих фізичних або віртуальних ресурсів. Наприклад, можна збільшити обсяг

пам'яті або обчислювальну потужність контролера SDN для підтримки більшої кількості комутаторів або додатків;

– розділення мережі на сегменти. SDN дозволяє розділити мережу на логічні сегменти, які можуть бути масштабовані окремо. Кожен сегмент може мати власні контролери та ресурси, що дозволяє збільшувати масштаб тільки в окремих частинах мережі, які вимагають більшої потужності або пропускної здатності;

– управління мережею SDN. Централізоване управління мережею SDN дозволяє адміністраторам зосередитися на високорівневих політиках та правилах керування мережею замість окремого налаштування кожного мережевого пристрою. Це спрощує управління мережею та дозволяє швидко реагувати на зміни в мережі без необхідності фізичного переконфігурування пристроїв;

– розподілений контроль. В деяких випадках, для забезпечення високої масштабованості, може бути використана розподілена архітектура контролера SDN. В такій архітектурі контролери можуть бути розподілені на різних вузлах мережі для більшої ефективності та резервування.

Масштабованість SDN дозволяє критичним інфраструктурам змінювати свою мережеву інфраструктуру відповідно до потреб системи, забезпечуючи високий рівень продуктивності, ефективності та надійності.

Відновлення після відмови (recovery) є важливою частиною стратегії безпеки для критичних інфраструктур, які використовують мережі SDN. Основні аспекти відновлення після відмови для SDN включають:

– резервне копіювання. Регулярне резервне копіювання конфігурацій та стану мережі SDN дозволяє відновити мережу до попереднього стану у разі відмови. Резервні копії можуть бути збережені на віддалених серверах або в облакі для забезпечення доступу до них після відмови;

– резервування контролерів. Для забезпечення високої доступності мережі SDN, можна використовувати резервні контролери. У разі відмови одного контролера, резервний контролер може автоматично прийняти керування мережею. Це дозволяє знизити вплив відмови на роботу мережі та забезпечити безперебійну роботу системи;

– детекція та відновлення помилок. Механізми виявлення помилок та автоматичного відновлення (fault detection and recovery) можуть бути використані для швидкого виявлення відмов та автоматичного відновлення мережі до нормального стану. Це може включати автоматичну переконфігурацію пристроїв або перенаправлення трафіку на альтернативні шляхи;

– тестування та вправи відновлення. Важливо регулярно проводити тестування та вправи відновлення для перевірки ефективності процедур відновлення та забезпечення готовності до реальних ситуацій відмови. Це допомагає ідентифікувати потенційні проблеми та покращити процес відновлення;

– моніторинг та аналітика. Постійний моніторинг мережі SDN дозволяє вчасно виявляти проблеми та відмови. Використання аналітичних інструментів допомагає аналізувати дані про мережу та ідентифікувати потенційні загрози або слабкі місця.

Ці практики допомагають забезпечити швидке відновлення після відмови мережі SDN в критичних інфраструктурах та знизити час простою мережі, що важливо для забезпечення безперебійної роботи системи.

1.8 Аналіз можливості застосування технології IBN для мережевих архітектур критичної інфраструктури

Технологія IBN (Intent-Based Networking) є перспективним підходом до керування мережами, який може бути корисним для критичних

інфраструктур. IBN спрощує керування мережами, використовуючи високорівневі наміри (інтенти), виражені адміністраторами, замість прямого налаштування окремих мережевих пристроїв. Проаналізовано деякі можливі переваги використання технології IBN для критичних інфраструктур.

Автоматизація та швидка реакція: IBN дозволяє автоматизувати багато процесів управління мережею, що сприяє швидкій реакції на зміни та вимоги мережі. За допомогою алгоритмів машинного навчання та штучного інтелекту, система IBN може аналізувати стан мережі, прогнозувати можливі проблеми та приймати автоматичні рішення для відновлення нормальної роботи [47-51].

Політика та виконання високорівневих намірів: IBN дозволяє адміністраторам виражати високорівневі наміри для мережі, такі як "забезпечити надійну комунікацію між певними системами" або "обмежити доступ до певних ресурсів". Система IBN перетворює ці наміри в конкретні налаштування мережі та моніторить, щоб переконатися, що вони виконуються правильно.

Забезпечення безпеки: IBN може допомогти впровадженню політик безпеки на рівні всієї мережі. За допомогою аналізу мережевого трафіку та механізмів перевірки відповідності політикам безпеки, система IBN може виявляти потенційні загрози та реагувати на них, забезпечуючи високий рівень безпеки для критичних інфраструктур.

Моніторинг та аналітика: Технологія IBN може забезпечити постійний моніторинг мережі та аналітику її стану. Це дозволяє виявляти аномалії, проблеми та прогнозувати витрати на мережеві ресурси. Адміністратори можуть отримати повну картину про стан мережі та приймати відповідні рішення для забезпечення ефективної роботи критичних інфраструктур.

Загалом, використання технології IBN може поліпшити управління мережами для критичних інфраструктур, забезпечуючи автоматизацію, швидку реакцію на зміни та підвищену безпеку. Однак, важливо ретельно

планувати впровадження та враховувати специфічні вимоги і потреби критичної інфраструктури під час реалізації технології IBN.

1.9 Висновки до першого розділу

Перший розділ кваліфікаційної роботи аналізує характеристики критичних інфраструктур для визначення їх сильних та слабких якостей при розробці мережевих архітектур. Здійснено ідентифікацію критичних інфраструктур та подано основні кроки для її виконання. Проведено оцінку ризиків для мережевих систем критичних інфраструктур, що дало змогу подати аналіз вразливостей, оцінити ймовірності та наслідки, визначити рівень ризику та подати опис заходів менімізації ризиків. Описано визначення вразливостей мереж для критичних інфраструктур, що є важливим кроком у процесі аналізу безпеки та сітйкості систем. Проаналізовано заходи безпеки для мереж критичних інфраструктур, які слід враховувати при захисті мереж критичних інфраструктур. Проведено опис хмарних архітектурних рішень, що можуть використовуватись у мережах для критичних інфраструктур, що дасть змогу застосувати найкращі можливості різних хмарних технологій. Розглянуто можливість використання технології SDN при проектуванні мережевих архітектур критичних інфраструктур, що показало позитивні елементи у вигляді централізованого керування мережею, динамічної адаптації мережевої інфраструктури, підвищеної безпеки, масштабованості і швидкого відновлення після відмови. Подано можливість використання технології IBN для мережевих архітектур критичних інфраструктур.

2 ДОСЛІДЖЕННЯ МЕРЕЖЕВИХ АРХІТЕКТУР ДЛЯ КРИТИЧНИХ ІНФРАСТРУКТУР

2.1 Вимоги архітектури мереж для критичної інфраструктури

Архітектура мереж для критичних інфраструктур має бути ретельно спроектованою та розробленою з огляду на вимоги безпеки, надійності та стійкості. Основні принципи при проектуванні мереж для критичних інфраструктур включають:

– сегментація мережі. Важливо розділити мережу на логічні сегменти залежно від потреб та рівня довіри. Це допомагає унеможливити розповсюдження атаки або внутрішнього зловживання і знижує вплив можливих проблем або аварій;

– захист периметра. На рівні периметра мережі слід використовувати захисні механізми, такі як файрволи, IDS/IPS системи (системи виявлення та запобігання вторгненням) та системи фільтрації трафіку, для контролю доступу та виявлення можливих загроз зовнішнього середовища;

– захист внутрішніх сегментів. У кожному логічному сегменті мережі слід використовувати механізми безпеки для захисту від внутрішніх загроз. Це можуть бути інтранети, використання віртуальних приватних мереж (VPN), контроль доступу до ресурсів та обмеження прав доступу користувачів;

– резервування та відновлення. Мережа для критичних інфраструктур повинна мати механізми резервування та відновлення, щоб забезпечити неперервність роботи в разі виникнення аварійних ситуацій або випадків відмов. Це можуть бути дублювання мережевого обладнання, наявність резервних каналів, механізми автоматичного перемикання та відновлення послуг;

– моніторинг та аналіз. Налагодження систем моніторингу та аналізу дозволяє виявляти можливі загрози та атаки, а також реагувати на них вчасно. Це включає системи виявлення вторгнень (IDS/IPS), моніторинг мережевого трафіку, системи журналювання подій та аналітику безпеки;

– фізична безпека. Важливим аспектом архітектури мереж для критичних інфраструктур є фізична безпека. Це включає контроль доступу до приміщень з мережевим обладнанням, захист від несанкціонованого фізичного доступу, резервування енергопостачання та захист від природних лих;

– системи аутентифікації та авторизації. Використання механізмів аутентифікації та авторизації для контролю доступу до мережевих ресурсів. Це можуть бути системи одноразових паролів, системи двофакторної аутентифікації, системи керування доступом тощо.

– планування масштабування. Розробка мережі для критичних інфраструктур має передбачати можливість масштабування та розширення в разі збільшення потреб та зміни умов. Варто враховувати майбутні потреби та забезпечити гнучкість мережевої інфраструктури.

Враховуючи специфіку критичних інфраструктур, архітектура мережі має бути проектована з урахуванням максимальної надійності, стійкості до атак та здатності до відновлення в разі виникнення непередбачених ситуацій.

2.2 Моделі архітектур мереж для критичних інфраструктур

Для критичної інфраструктури можуть використовуватись різні моделі архітектур комп’ютерних мереж залежно від конкретних потреб і вимог. Наведемо кілька типових моделей, які можуть бути використані:

– централізована архітектура. У цій моделі всі мережеві ресурси і контроль зосереджені в одному центральному вузлі. Вона забезпечує

простоту керування і контролю, але може бути вразлива до відмови центрального вузла;

– розподілена архітектура. В цій моделі мережеві ресурси і керування розподілені між декількома вузлами. Це забезпечує більшу надійність і масштабованість, оскільки відмова одного вузла не спричиняє відмову всієї мережі;

– мережа з резервними шляхами. У цій моделі створюються додаткові резервні шляхи для передачі даних у випадку відмови основних шляхів. Це забезпечує високу доступність і надійність мережі;

– архітектура з використанням віртуалізації. Ця модель використовує віртуалізацію для створення віртуальних мереж та віртуальних приватних мереж (VPN). Вона забезпечує збільшення ефективності ресурсів і забезпечує високий рівень безпеки та ізоляції мережевих сегментів;

– архітектура з використанням контейнеризації. В цій моделі використовуються контейнери для розгортання ізольованих додатків і сервісів. Вона забезпечує гнучкість, швидкість розгортання та масштабованість мережевих ресурсів.

Централізована архітектура мереж для критичної інфраструктури передбачає зосередження управління та контролю над мережею в одному центральному вузлі або контролері. Основні характеристики централізованої архітектури включають:

– централізоване керування. Усі прийняття рішень і керування мережею здійснюється в одному центральному вузлі. Це дозволяє забезпечити єдиною точкою керування та зменшити складність управління;

– оптимізація ресурсів. Централізоване керування дозволяє ефективно використовувати ресурси мережі. Це може включати розподіл пропускної здатності, призначення IP-адрес, управління безпекою та інші аспекти;

– моніторинг та аналіз. Зосереджене керування дозволяє здійснювати централізований моніторинг мережі та аналізувати її стан. Це дозволяє швидко виявляти проблеми, вирішувати їх та приймати відповідні заходи;

– забезпечення безпеки. Централізована архітектура спрощує впровадження і керування системами безпеки. Всі правила безпеки можуть бути централізовано налаштовані і контрольовані, що полегшує захист мережі від загроз.

Однак, централізована архітектура також має свої обмеження та потенційні недоліки:

– одна точка відмови. Якщо центральний вузол або контролер виходить з ладу, це може спричинити відмову всієї мережі. Це робить систему вразливою до відмови та атак;

– обмежена масштабованість. Централізована архітектура може бути обмежена в масштабуваності, особливо при великому обсязі даних або широкому розподіленні мережі;

– затримки. Управління і прийняття рішень в централізованій архітектурі можуть призвести до затримок, особливо в великих мережах або при великому обсязі даних;

– витрати на мережеве обладнання. Централізована архітектура може вимагати високої вартості мережевого обладнання для забезпечення потрібного рівня продуктивності та надійності.

Вибір централізованої архітектури мережі для критичної інфраструктури повинен бути здійснений з урахуванням конкретних потреб, вимог та ризиків, а також з урахуванням можливостей комп'ютерних мереж та доступних технологій.

Розподілена архітектура мереж для критичної інфраструктури передбачає розподілення управління та контролю мережею між декількома

вузлами або контролерами. Приклад такої архітектури показано на рисунку 2.1

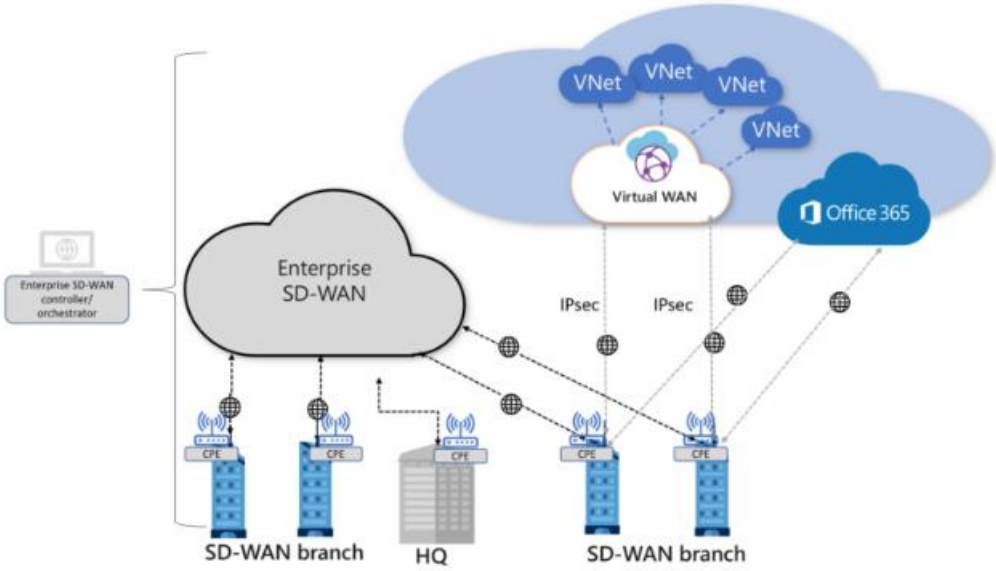

Рисунок 2.1 – Розподілена архітектура на основі SD-WAN технології

Основні характеристики розподіленої архітектури включають:

– резервність та висока доступність. Розподілена архітектура дозволяє використовувати декілька вузлів або контролерів, що забезпечує резервність та високу доступність мережі. У випадку відмови одного вузла, інші можуть продовжувати працювати, забезпечуючи неперервну роботу мережі;

– масштабованість. Розподілена архітектура дозволяє гнучко масштабувати мережу шляхом додавання нових вузлів або контролерів. Це дозволяє збільшувати мережеві ресурси і оброблювати більші обсяги даних або зростаючі вимоги мережі;

– розділення трафіку. Розподілена архітектура дозволяє розділити трафік між різними вузлами або контролерами. Це полегшує обробку трафіку, забезпечує балансування навантаження і покращує продуктивність мережі;

– зменшення затримок. Управління та прийняття рішень в розподіленій архітектурі можуть відбуватись ближче до мережевих вузлів, що зменшує затримки та покращує швидкість реакції мережі;

– висока надійність. Розподілена архітектура забезпечує високий рівень надійності, оскільки вона розподіляє функції та завдання між декількома вузлами або контролерами. Це дозволяє уникнути однієї точки відмови і забезпечити надійну роботу мережі.

Розподілена архітектура мереж добре підходить для критичних інфраструктур, оскільки вона забезпечує високу доступність, надійність і масштабованість мережі. Однак, вона також може бути складнішою в управлінні та вимагати більшої кількості ресурсів для побудови та підтримки розподілених вузлів або контролерів. Порівняння реалізації різних моделей для провайдера мобільних послуг показано на рисунку 2.2.

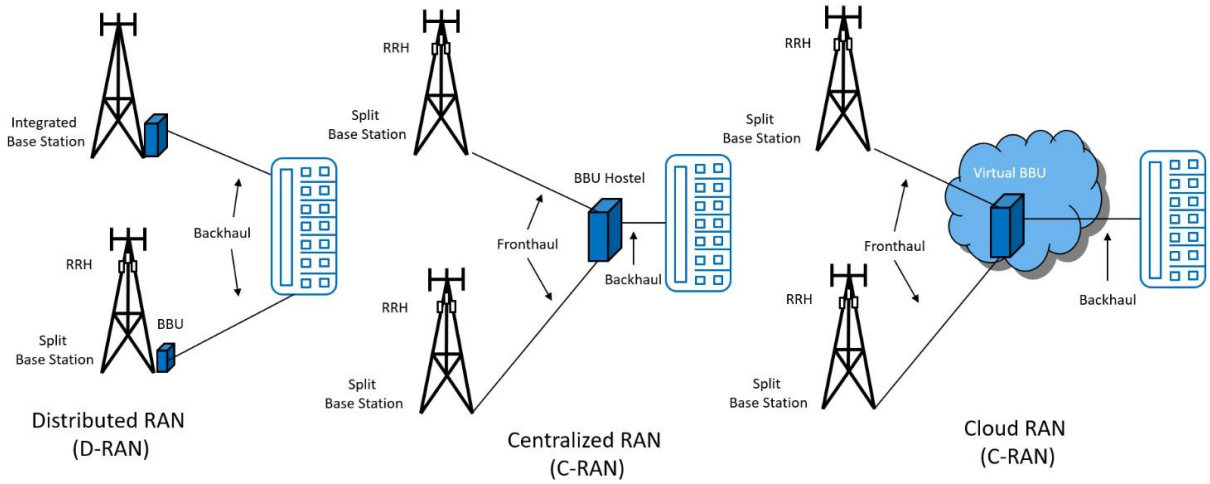

Рисунок 2.2 – Реалізація різних моделей для провайдера мобільних послуг

Мережа з резервними шляхами (redundant network) є важливою складовою критичних інфраструктур, оскільки забезпечує високу надійність і доступність мережі. Така мережа має додаткові шляхи (резервні шляхи), які можуть використовуватись в разі відмови або перешкоди на основних шляхах. Приклад реалізації такої мережі подано на рисунку 2.3.

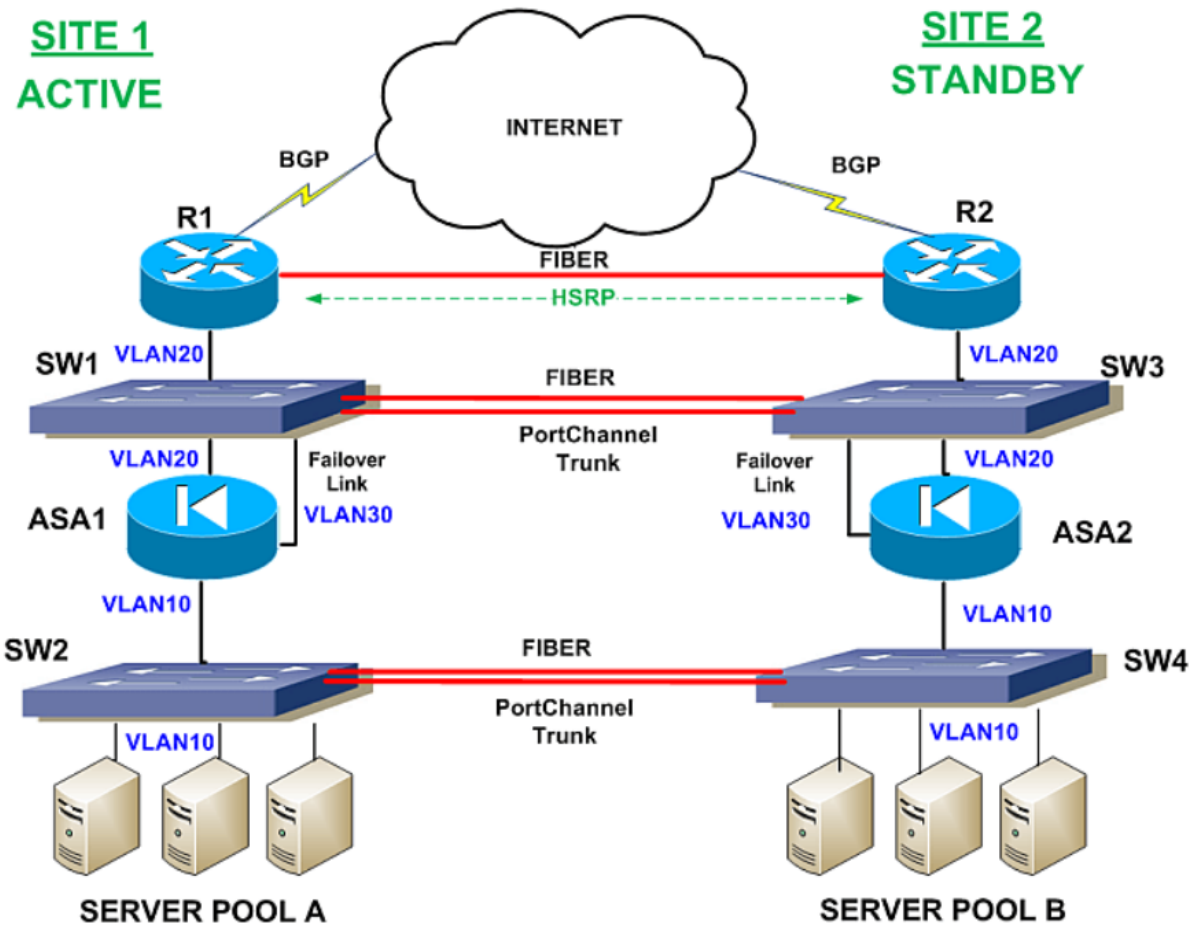

Рисунок 2.3 – Реалізація мережі з надлишковими шляхами

Основні характеристики мережі з резервними шляхами включають:

– резервні шляхи. Мережа має альтернативні шляхи, які можуть бути використані в разі відмови або перешкоди на основних шляхах. Це забезпечує неперервність зв'язку та доступ до ресурсів мережі навіть у випадку проблем з основними шляхами;

– автоматичне переключення. Резервні шляхи активуються автоматично, якщо виявляється проблема на основних шляхах. Це забезпечує швидке переключення і відновлення зв'язку без значного втручання адміністратора мережі;

– протоколи маршрутизації з резервними шляхами. Використання протоколів маршрутизації, які підтримують резервні шляхи, дозволяє мережі динамічно перебудовувати маршрути при виявленні відмови на основних

шляхах. При цьому мережа може шукати та використовувати доступні резервні шляхи;

– моніторинг та керування. Для ефективного використання резервних шляхів, мережа повинна мати механізми моніторингу та керування. Це дозволяє виявляти відмови на основних шляхах, активувати резервні шляхи і виконувати належне розподілення трафіку;

– балансування навантаження. Мережа з резервними шляхами може використовувати балансування навантаження для розподілу трафіку між основними та резервними шляхами. Це допомагає оптимізувати використання ресурсів мережі і підвищує продуктивність.

Мережа з резервними шляхами є ефективним заходом для забезпечення надійності і доступності критичних інфраструктур. Вона дозволяє мережі швидко відновитись після відмови і забезпечує неперервний доступ до важливих ресурсів.

Архітектура з використанням віртуалізації для мереж критичних інфраструктур включає використання віртуальних мереж та віртуальних пристроїв для побудови і керування мережевою інфраструктурою. Основні компоненти такої архітектури включають:

– віртуальні мережі. Віртуальні мережі (Virtual Networks) дозволяють створювати віртуальні сегменти мережі на основі фізичної інфраструктури. Кожна віртуальна мережа може мати власні незалежні параметри, політики безпеки та маршрутизацію. Це дозволяє логічно ізолювати різні частини мережі, підвищує безпеку та ефективність мережі.

– віртуальні пристрої. Віртуальні пристрої (Virtual Devices) включають віртуальні комутатори, маршрутизатори, файрволи та інші мережеві пристрої, які працюють на основі програмного забезпечення (Software-Defined Networking). Вони можуть бути запущені на фізичних серверах або в хмарному середовищі, і дозволяють гнучко керувати трафіком, маршрутизацією та безпекою мережі.

– віртуалізація мережевих ресурсів. Віртуалізація мережевих ресурсів (Network Function Virtualization, NFV) використовує віртуальні пристрої для заміни фізичних мережевих пристроїв, таких як маршрутизатори та файрволи. Це дозволяє гнучко масштабувати та керувати функціями мережі, спрощує управління та знижує вартість обладнання.

– оркестрація та автоматизація. Архітектура з використанням віртуалізації для мереж критичних інфраструктур передбачає використання оркестраторів та систем автоматизації для керування мережевими ресурсами та процесами. Це дозволяє автоматично налаштовувати та керувати мережевою інфраструктурою, швидко реагувати на зміни та забезпечувати високу доступність мережі.

Приклад реалізації функцій NFV показано для мережі Juniper на рисунку 2.4.

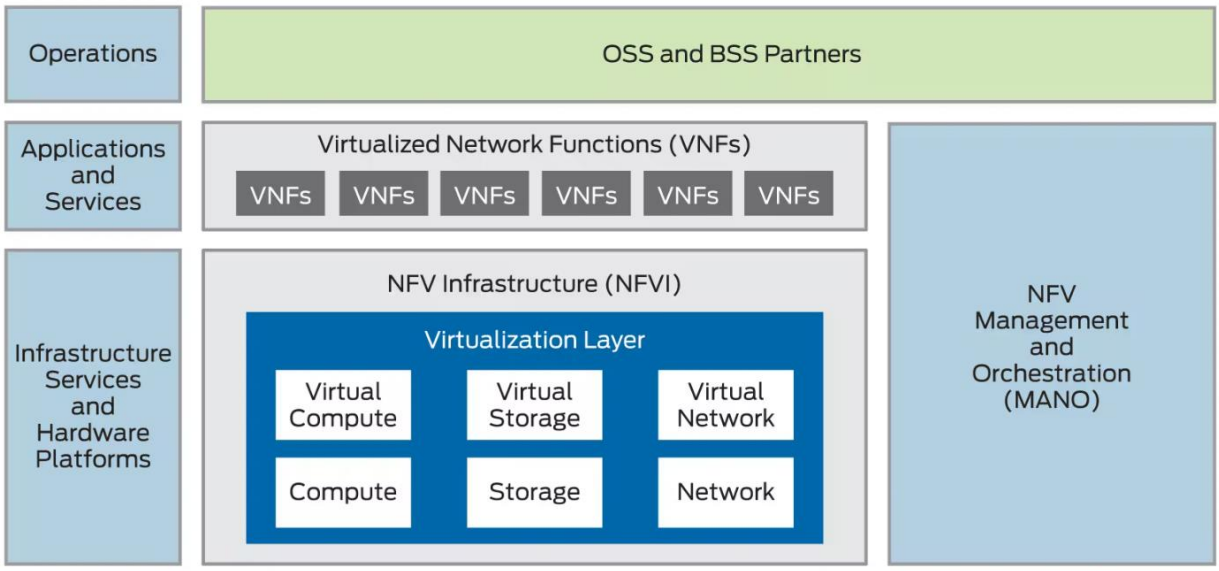

Рисунок 2.4 – Реалізація мережі Juniper

Архітектура з використанням віртуалізації дозволяє розгортати та керувати мережевою інфраструктурою критичних інфраструктур з використанням гнучкості та автоматизації. Вона сприяє підвищенню

надійності, безпеки та масштабованості мережі, що є особливо важливим для критичних застосувань.

Архітектура з використанням контейнеризації для критичних інфраструктур базується на використанні контейнерів для упаковки, розгортання та керування додатками та сервісами в мережевому середовищі. Основні складові такої архітектури включають:

– контейнери. Контейнери є стандартизованим способом упаковки додатків та їх залежностей відокремлено від хост-системи. Вони забезпечують стандартизоване середовище виконання для додатків, що спрощує розгортання, масштабування та управління ними;

– контейнерні оркестратори. Контейнерні оркестратори, такі як Kubernetes, Docker Swarm або Apache Mesos, використовуються для керування контейнерами в розподіленому середовищі. Вони дозволяють автоматично розподіляти ресурси, керувати масштабуванням, відновленням та моніторингом контейнерів;

– мікросервісна архітектура. Контейнеризація сприяє використанню мікросервісної архітектури, де додатки розбиваються на невеликі, незалежні компоненти, які можуть бути упаковані в окремі контейнери. Це дозволяє гнучко масштабувати, оновлювати та управляти окремими компонентами системи;

– безпека. Контейнеризація може забезпечувати високий рівень безпеки за допомогою використання ізольованих контейнерів, обмеження привілеїв та контролю доступу до ресурсів. Крім того, засоби моніторингу та логування можуть бути використані для виявлення та реагування на потенційні загрози безпеки;

– резервне розгортання. Контейнеризація дозволяє легко створювати резервні копії контейнерів та швидко відновлювати систему в разі відмови або неполадок. Це забезпечує високу доступність та швидке відновлення критичних інфраструктур.

Архітектура з використанням контейнеризації дозволяє забезпечити гнучкість, масштабованість, безпеку та високу доступність для критичних інфраструктур. Вона спрощує розгортання, управління та моніторинг системи, забезпечуючи ефективне використання ресурсів та швидку відмовостійкість.

Кожна з цих моделей має свої переваги і недоліки, і вибір конкретної моделі залежить від потреб і вимог критичної інфраструктури, що розглядається.

2.3 Дослідження мультихмарної архітектури на основі рішень від VMware

Мультихмарні архітектури стають дедалі важливішою частиною корпоративних стратегій, що забезпечують надійну роботу додатків. Згідно з дослідженням VMware Digital Momentum, проведеним серед осіб, відповідальних за прийняття рішень у сфері корпоративних технологій, майже 73% повідомили, що вони стандартизують роботу додатків та інфраструктури на основі мультихмарних технологій1.

Мультихмарна інфраструктура пропонує багато переваг, таких як можливість швидкого масштабування та підвищення надійності. Таким чином, розгортання мультихмарних систем може допомогти бізнесу:

- впроваджувати інновації та трансформувати клієнтський досвід;
- масштабувати та розвивати бізнес;
- підвищити залученість та продуктивність працівників.

Проте, з операційної та технологічної точки зору, мультихмарні технології становлять серйозний виклик: Складність. Швидкі інновації та зростання вимагають здатності розгортати робочі навантаження та керувати ними в будь-якій публічній хмарі, забезпечуючи при цьому необхідну доступність та масштабування сервісів. Однак управління робочими

навантаженнями та інфраструктурою в декількох хмарах одночасно значно підвищує складність мережевої архітектури, що з'єднує ці додатки і хмари. Це також вимагає від компаній розгортання складних правил безпеки для захисту мережевого трафіку, при цьому доводиться покладатися на обмежену мобільність і видимість робочих навантажень, а також на можливості виявлення загроз, які не масштабуються.

Успішне впровадження мультихмарної інфраструктури вимагає засобів приборкання складності, яка притаманна мультихмарним технологіям.

Project Northstar – це мережева та безпекова пропозиція на основі SaaS, яка надасть клієнтам NSX набір мультихмарних мережевих та безпекових послуг на вимогу, наскрізну видимість та контроль. Клієнти зможуть використовувати централізовану хмарну консоль для отримання миттєвого доступу до мережевих послуг і послуг безпеки, таких як управління мережевою політикою і політикою безпеки, мережеве виявлення і реагування (Network Detection and Response, NDR), аналітика NSX, розширене балансування навантаження (Advanced Load Balancing, ALB), брандмауер веб-додатків (Web Application Firewall, WAF) і HCX. Він підтримуватиме розгортання як у приватній хмарі, так і в хмарі VMware Cloud, що працює в публічних хмарах, і дозволить підприємствам створити гнучку мережеву інфраструктуру, яку вони зможуть розгортати і згортати за лічені хвилини.

SaaS (Software as a Service) для критичних інфраструктур використовується для надання програмного забезпечення через хмару, що є гнучким і швидким рішенням для підтримки та управління критичними системами. Основні характеристики та переваги використання SaaS для критичних інфраструктур включають:

– готове до використання програмне забезпечення. SaaS надає готові до використання програмні рішення, які можуть бути легко

впроваджені в критичні інфраструктури. Це зменшує час і зусилля, потрібні для розробки та впровадження власного програмного забезпечення;

– швидкість впровадження та масштабованість. SaaS дозволяє швидко масштабувати програмне забезпечення для відповіді на зростаючі потреби критичних систем. Ви можете легко збільшувати або зменшувати розмір ресурсів в залежності від потреб;

– висока доступність та надійність. Постачальники SaaS зазвичай забезпечують високу доступність і надійність своїх послуг, включаючи резервне копіювання даних, реплікацію та забезпечення безперебійної роботи. Це допомагає знизити ризик відмови і забезпечити неперервну роботу критичних систем;

– зниження витрат. Замість того, щоб придбати, встановлювати та управляти власним обладнанням та програмним забезпеченням, ви можете скористатися SaaS за моделью підписки. Це знижує витрати на обладнання та обслуговування, а також спрощує оновлення та підтримку;

– легке керування та моніторинг. SaaS надає централізовані засоби керування та моніторингу, які дозволяють вам ефективно керувати та контролювати критичні системи через веб-інтерфейс або API;

– безпека. Постачальники SaaS зазвичай приділяють велику увагу заходам безпеки, включаючи шифрування даних, механізми аутентифікації та авторизації, контроль доступу та інші заходи для захисту конфіденційності та цілісності даних.

Узагалі, SaaS дозволяє компаніям зосередитися на своїх основних функціях, не витрачаючи багато часу та зусиль на розробку та управління власним програмним забезпеченням. Використання SaaS для критичних інфраструктур може сприяти швидкому впровадженню, масштабованості, високій доступності та зниженню витрат.

Project Northstar забезпечить кілька ключових переваг:

– швидше повернення інвестицій. Доступність послуг на вимогу та спрощене споживання мережевих послуг і послуг безпеки означає, що клієнти зможуть миттєво отримувати доступ до мережевих послуг і послуг безпеки через обрану ними хмару. Об’єднана модель політики у всіх провідних публічних і приватних хмарах дозволить IT-спеціалістам досягти справжньої узгодженості політики при впровадженні ключових мультихмарних сценаріїв використання, таких як аварійне відновлення, мобільність робочих навантажень, відмовостійкість сервісів, розрив хмари та еластичне з’єднання між хмарами. Таким чином, вони зможуть швидше виводити додатки на ринок від концепції до реалізації, що призведе до скорочення часу на отримання прибутку. Архітектура SaaS також дозволяє VMware виводити на ринок швидкі інновації, до яких клієнти можуть отримати миттєвий доступ;

– гнучке споживання послуг. На додаток до існуючих моделей надання послуг, мережеві послуги та послуги безпеки будуть надаватися за моделлю SaaS на основі послуг на вимогу. Такий вибір моделей споживання забезпечить клієнтам VMware економічну та операційну гнучкість. Крім того, централізоване управління та контроль забезпечить узгодженість політик, робочих процесів та обслуговування платформи, а VMware виконуватиме ці завдання за допомогою моделі розподіленої відповідальності;

– масштабована латеральна безпека. Розгортаючи Northstar, підприємства зможуть краще захистити свої робочі навантаження в мультихмарних середовищах завдяки розподіленому брандмауеру, NDR та безпеці хмарної платформи, керованої VMware. NDRaaS забезпечить масштабоване виявлення загроз та реагування на них. А за допомогою NSX Intelligence as a Service підприємства отримають 360-градусний огляд своїх робочих навантажень у мультихмарних середовищах.

Проект Northstar – це редизайн і переосмислення мультихмарних архітектур та операцій. Традиційна мережева архітектура розподілена між приватною та публічною хмарами, а кілька додатків працюють у різних хмарах, кожна з яких використовує свій набір мережевих функцій, правил безпеки та політик автоматизації. Кожною хмарою також керують окремі локальні адміністратори за допомогою власних хмарних консолей, що ускладнює прийняття єдиних політик у мультихмарному середовищі. Це створює операційні проблеми та додає складнощів в управлінні гібридною та мультихмарною інфраструктурою. Коли кожна хмара працює як ізольована, операції та управління також стають ізольованими. Приклад архітектури реалізації подано на рисунку 2.5.

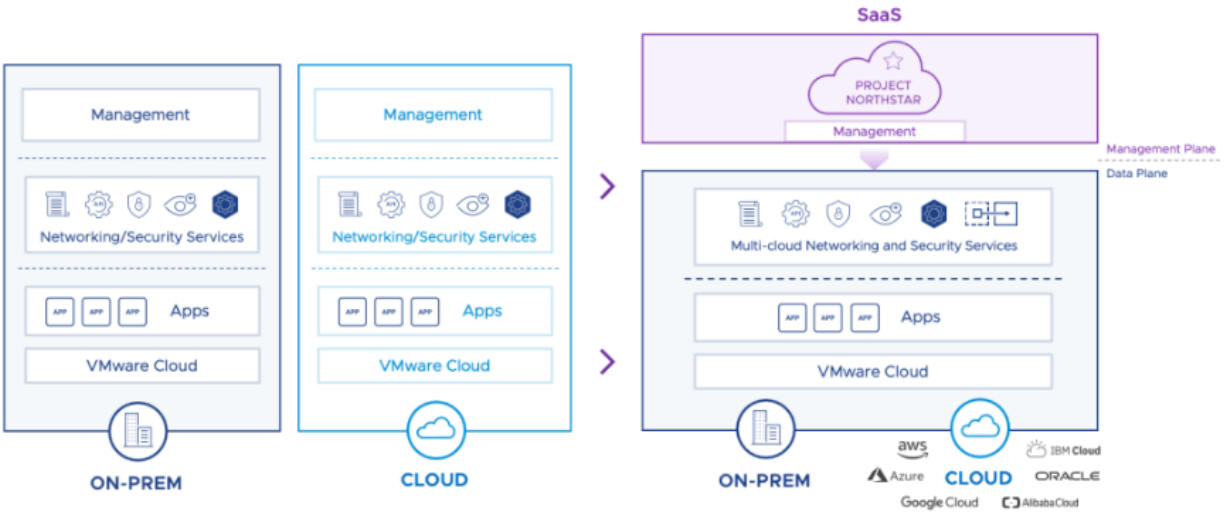

Рисунок 2.5 – Реалізація багатохмарної мережі від VMware для критичної інфраструктури

Проект Northstar вирішить ці проблеми, надаючи послугу SaaS, яка забезпечує узгодженість політик, операцій та автоматизацію в мультихмарних середовищах. Отримавши доступ до хмарної консолі Northstar, підприємства зможуть застосовувати мережеві політики та політики безпеки у своїх приватних хмарних, гібридних та мультихмарних середовищах.

Сервіси, що надаються в межах проекту NorthStar від VMware показано на рисунку 2.6.

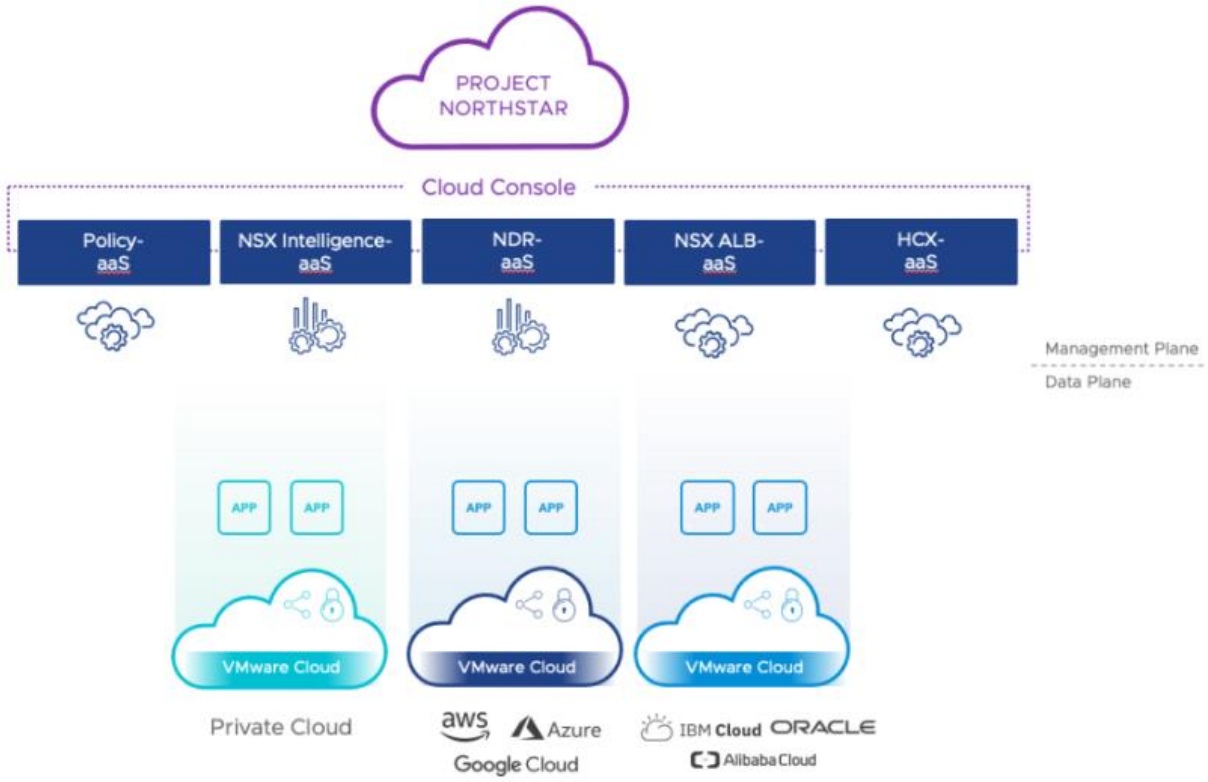

Рисунок 2.6 – Сервіси для мережевих архітектур критичних інфраструктур

Централізоване управління політиками. Завдяки Project Northstar клієнти зможуть централізовано керувати мережевими політиками та політиками безпеки у всіх своїх хмарах. Project Northstar забезпечить єдину площину для планування та розгортання узгоджених мережевих засобів управління та політик безпеки в багатосайтових та багаторегіональних розгортаннях. Пропозиція також включає в себе вбудовані засоби управління мережею та безпекою, а також усунення несправностей.

Планування безпеки і видимість. Служба NSX Intelligence забезпечує 360-градусний огляд мультихмарного середовища кожного клієнта в режимі реального часу. Він працює на основі масштабованого озера даних, керованого VMware, яке може поглинати величезні обсяги даних про потоки

трафіку і надавати рекомендації щодо мережевих політик і політик безпеки в мультихмарних розгортаннях. Інструменти візуалізації забезпечують видимість мультихмарного трафіку і безпеки в режимі реального часу. Аналіз мережевого трафіку (NTA) надасть інформацію про загрози та виявлення поведінкових аномалій.

Мережеве виявлення та реагування. Служба Network Detection and Response (NDR) забезпечить масштабоване виявлення загроз і реагування на них для робочих навантажень, розгорнутих в приватних і/або публічних хмарах. Механізм кореляції NDR аналізуватиме події IDPS, шкідливе програмне забезпечення та аномалії на основі кампаній загроз, що допоможе запобігти перевантаженню оповіщеннями та спростити процеси моніторингу SOC. Ця послуга забезпечує спрощене сортування загроз, масштабування та пошук загроз відповідно до фреймворку MITRE ATT&CK.

Розширене балансування навантаження. Хмарний сервіс розширеного балансування навантаження (ALB) та можливості розміщених контролерів підтримуються на локальному рівні, у VMware Cloud та в публічних хмарах. Послуга буде реалізовувати вдосконалений контролер балансування навантаження як керований VMware сервіс, який можна використовувати автономно або разом з іншими SaaS-сервісами Project Northstar. Клієнти зможуть отримати доступ до повнофункціонального і багатокористувацького постачальника послуг розширеного балансувальника навантаження під управлінням VMware, що спрощує роботу завдяки централізованому управлінню клієнтами. VMware SRE керує контролером, забезпечуючи високу відмовостійкість сервісів.

Мобільність робочих навантажень: Спираючись на сильні сторони VMware HCX, мобільність робочих навантажень як послуга буде повністю управлятися VMware, надаючи можливість організувати безпечне підключення та мобільність робочих навантажень на різних майданчиках. Послуга дозволить спростити введення в експлуатацію та пришвидшити

усунення несправностей за допомогою централізованої інформаційної панелі в декількох хмарах. Клієнти зможуть централізовано управляти міграцією робочих навантажень і балансуванням між декількома хмарами і знаходити першопричини за лічені хвилини, а не години, використовуючи розширену централізовану звітність.

Хоча ці послуги раніше пропонувалися клієнтам NSX з використанням середовищ, розміщених локально і в VMware Cloud на AWS, проект Northstar являє собою стратегічний перехід до надання цих послуг в локальних, гібридних і мультихмарних середовищах за допомогою моделі надання послуг SaaS.

2.4 Дослідження безпеки мережевих архітектур для критичних інфраструктур

Безпека мережевих архітектур для критичної інфраструктури є надзвичайно важливою, оскільки ці системи мають високу важливість та потребують захисту від різних видів загроз. Основні аспекти безпеки мережевих архітектур для критичної інфраструктури включають:

– аутентифікація та авторизація. Забезпечення правильної аутентифікації користувачів та пристроїв, а також належної авторизації доступу до ресурсів мережі. Використання сильних механізмів аутентифікації, таких як двофакторна аутентифікація, може забезпечити вищий рівень безпеки;

– контроль доступу. Обмеження доступу до мережевих ресурсів та функцій залежно від ролі та привілеїв користувачів. Встановлення політик контролю доступу, які враховують принцип найменшого можливого доступу, може зменшити ризик несанкціонованого доступу;

– шифрування. Використання шифрування для захисту конфіденційності та цілісності даних, які передаються по мережі.

Шифрування даних у спокої (at-rest) та під час передачі (in-transit) допомагає запобігти несанкціонованому доступу до інформації;

– моніторинг та аналіз. Реалізація систем моніторингу, які стежать за активністю в мережі та виявляють підозрілу або аномальну поведінку. Це дозволяє вчасно виявляти та реагувати на потенційні загрози або атаки;

– захист від вразливостей. Використання мережевих пристроїв та програмного забезпечення з найновішими патчами безпеки та забезпечення їх регулярного оновлення. Це допомагає запобігти використанню вразливостей в мережевих пристроях для атак та несанкціонованого доступу;

– резервне копіювання та відновлення. Регулярне створення резервних копій даних та можливість швидкого відновлення мережевих ресурсів у випадку відмови або інциденту. Це допомагає забезпечити неперервну роботу критичних систем та мінімізувати вплив на їх функціонування;

– системи виявлення та запобігання вторгнень (IDS/IPS). Використання систем виявлення та запобігання вторгнень допомагає виявляти та блокувати потенційні атаки на мережу. Ці системи аналізують мережевий трафік на наявність аномалій та небезпечних пакетів.

NIST (National Institute of Standards and Technology) розробило рамки і рекомендації з безпеки для різних галузей, включаючи критичну інфраструктуру. Одна з таких моделей безпеки, розроблених NIST – це Кібербезпековий каркас (Cybersecurity Framework, CSF).

Кібербезпековий каркас NIST визначає набір контролів та процесів, які допомагають організаціям впроваджувати та управляти безпекою своїх систем. Він базується на визнаних стандартах та рекомендаціях і містить такі основні елементи:

– керівництво. розробка політики безпеки, призначення відповідальних осіб, створення процедур управління безпекою;

– управління ризиками. виявлення, оцінка та керування ризиками, пов'язаними з безпекою інформації та критичною інфраструктурою;

– керування доступом. забезпечення контролю доступу до систем та ресурсів, ідентифікація та аутентифікація користувачів, управління привілеями;

– конфігураційне управління. управління конфігураціями систем та компонентів, включаючи контроль змін, патчі та оновлення;

– виявлення та реагування. впровадження механізмів для виявлення інцидентів, моніторингу мережі та систем, а також швидка реакція на події безпеки;

– безпека зв’язку. захист мережевого зв’язку, шифрування даних, захист від атак та перехоплення інформації;

– управління погодженістю. забезпечення відповідності з регуляторними вимогами та стандартами безпеки, а також регулярне оцінювання впроваджених заходів безпеки.

На рисунку 2.7 показано основні складові елементи даного фреймворку.

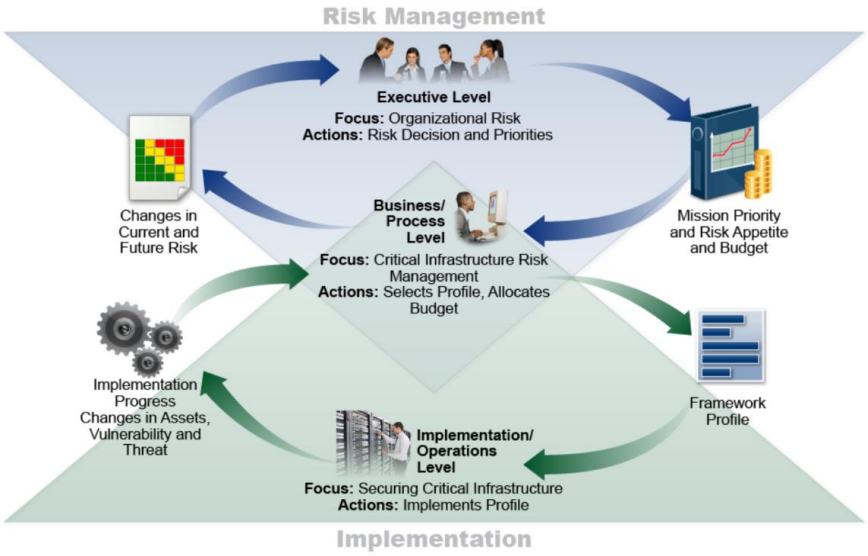

Рисунок 2.7 – NIST фреймворк безпеки

Це лише огляд основних аспектів Кібербезпекового каркасу NIST для критичної інфраструктури. Конкретні вимоги та рекомендації можуть варіюватись залежно від конкретної галузі інфраструктури. Рекомендується ознайомитися з офіційними документами NIST та консультуватися з експертами з безпеки для отримання детальної інформації та порад. Загальний підхід до безпеки повинен включати комплексний підхід, що враховує різні аспекти захисту, включаючи людей, процеси та технології.

2.5 Висновки до другого розділу

Другий розділ кваліфікаційної роботи присвячений дослідженню мережевих архітектур для критичних інфраструктур. Визначено та описано вимоги до таких архітектур, що повинні враховуватись при їх виборі та впроваджені. Проведено аналіз моделей мережевих архітектур, що дає змогу застосувати найбільш відповідну модель для конкретного випадку критичної інфраструктури. Виявлено, що серед існуючих архітектур в задачах даного класу буде ефективним застосування контернеризації, як гнучкого, швидкодійного та надійного варіанту розгортання сервісів. Здійснено дослідження конкретної реалізації мультихмарної архітектури від компанії VMware, що надає можливість впроваджувати інновації та трансформувати клієнтський досвід, масштабувати і розвивати бізнес, підвищувати залученість та продуктивність працівників. Проект Northstar від VMware базується на використанні SaaS, що для критичних інфраструктур буде надавати програмне забезпечення через хмару для гнучкої та швидкої підтримки управління критичними системами. Даний проект забезпечує узгодженість політик, операцій та автоматизацію в мультихмарних середовищах. Отримавши доступ до хмарної консолі Northstar, підприємства зможуть застосовувати мережеві політики та політики безпеки у своїх приватних хмарних, гібридних та мультихмарних середовищах. Досліджено

основні аспекти Кібербезпекового каркасу NIST для критичної інфраструктури. Конкретні вимоги та рекомендації можуть варіюватись залежно від конкретної галузі інфраструктури. Рекомендується ознайомитися з офіційними документами NIST та консультуватися з експертами з безпеки для отримання детальної інформації та порад. Загальний підхід до безпеки повинен включати комплексний підхід, що враховує різні аспекти захисту, включаючи людей, процеси та технології.

3 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

3.1 Охорона праці

3.1.1 Освітлення робочого місця

Законодавчими актами, що визначають основні положення про охорону праці є загальні закони України, а також спеціальні законодавчі акти. До загальних законів належать: Конституція України, Закони України: “Про охорону праці”, “Про охорону здоров’я”, “Про пожежну безпеку” [51-55].

Приміщення, в яких встановлені персональні комп’ютери, повинні мати природне та штучне освітлення відповідно до СНиП II-4-79.

Природне освітлення має здійснюватись через світлові прорізи, орієнтовані переважно на північ чи північний схід і забезпечувати коефіцієнт природною освітленості (КПО) не нижче ніж 1,5%. Розраховується КПО за методикою, викладеною в СНиП II-4-79.

Штучне освітлення в приміщеннях з робочими місцями має здійснюватись системою загального рівномірного освітлення. У разі переважної роботи з документами, допускається застосування системи комбінованого освітлення (крім системи загального освітлення додатково встановлюються світильники місцевого освітлення). Зазначення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300-500лк. Якщо ці значення освітленості неможливо забезпечити системою загального освітлення, допускається використовувати місцеве освітлення. При цьому світильники місцевого освітлення слід встановлювати таким чином, щоб не створювати відблисків на поверхні екрана, а освітленість екрана має не перевищувати 300лк. Як джерела світла в разі штучного освітлення мають застосовуватись переважно люмінесцентні лампи типу ЛБ. У разі влаштування відбитого освітлення у приміщеннях, де переважним чином працюють з документами, допускається застосування металогалогенних ламп потужністю

250Вт. Допускається застосування ламп розжарювання у світильниках місцевого освітлення. Система загального освітлення має становити суцільні або переривчасті лінії світильників, розташовані збоку від робочих місць (переважно ліворуч), паралельно лінії зору працюючих.

Допускається використання світильників таких класів світлорозподілу:

– прямого світла — П;
– переважно прямого світла — Н;
– переважно відбитого світла — В.

Для загального освітлення слід застосовувати світильники серії ЛПО 3б із дзеркальними гратами, що укомплектовані високочастотними пускорегулювальними апаратами (ВЧ ПРА). Допускається застосовувати світильники цієї серії без ВЧ ПРА тільки в модифікації «Кососвітло».

При відсутності світильників серії ЛПО36 з ВЧ ПРА і без ВЧ ПРА модифікації «Кососвітло» допускається застосування світильників загального освітлення серії:

– ЛПО13 — 2×40/Б — 01;
– ЛПО13 — 4×40/Б — 01;
– ЛПО13 — 2×40 — 06;
– ЛПО13 — 2×65 — 06;
– ЛСО05 — 2×40 — 001;
– ЛСО05 — 2×40 — 003;
– ЛСО04 — 2×36 — 008;
– ЛПО34 — 4×36 — 002;
– ЛПО34 — 4×58 — 002;
– ЛПО31 — 2×31 — 002,

а також їх вітчизняні та зарубіжні аналогів.

Застосування світильників без розсіювачів та екрануючих грат заборонено. Яскравість світильників загального освітлення в зоні кутів випромінювання від 50 до 90 градусів з вертикаллю в повздовжній та

поперечній площинах має становити не більше ніж 200 кд/м2, захисний кут світильників — не менше ніж 40 градусів. Світильники місцевого освітлення повинні мати відбивач, що просвічує, із захисним кутом, не меншим ніж 40 градусів.

Слід передбачити обмеження прямої блискості від джерел природного та штучного освітлення. При цьому яскравість світлих поверхонь (вікна, джерела штучного освітлення), що розташовані в полі зору повинна бути не більше ніж 200 кд/м2. Необхідно обмежувати відбиту блискість на робочих поверхнях відносно джерел природного і штучного освітлення. При цьому яскравість відблисків на екрані ВДТ має не перевищувати 40 кд/м2, а яскравість стелі в разі застосування системи відбитого освітлення – 200 кд/м2.

Показник осліплености у разі використання джерел загального штучного освітлення у виробничих приміщеннях має не перевищувати 20, а показник дискомфорту в адміністративно-громадських приміщеннях має бути не більше за 40. Необхідно обмежувати нерівномірність розподілу яскравості в полі зору працюючих з ВДТ. При цьому співвідношення яскравостей робочих поверхонь має бути не більшим ніж 3:1, а співвідношення яскравостей робочих поверхонь та поверхонь стін, обладнання тощо — 5:1. Коефіцієнт запасу для освітлювальних установок загального освітлення має дорівнювати 1,4. Коефіцієнт пульсації має не перевищувати 5%, що забезпечується застосуванням газорозрядних ламп у світильниках загального та місцевого освітлення з ВЧ ПРА для світильників будь-яких типів. Якщо не має світильників з ВЧ ПРА, то лампи багатолампових світильників або світильники загального освітлення, розташовані поруч, слід вмикати на різні фази трьохфазної мережі. Для забезпечення нормованих значень освітленості у приміщеннях з ВДТ ЕОМ та ПЕОМ слід чистити шибки і світильники принаймні двічі на рік і вчасно замінювати лампи, що перегоріли.

3.2 Безпека в надзвичайних ситуаціях

3.2.1 Основні принципи і способи забезпечення життєдіяльності

Можна виділити ряд важливих проблем, які постійно перебувають у полі зору людства для забезпечення нормальних умов життя і праці.

Дотримання параметрів середовища перебування людини в необхідних для життєдіяльності межах – це одна із складних проблем, які стоять перед світовим співтовариством. Це пов’язано з тим, що трудова діяльність людей з року в рік активізується, ускладнюється, вводяться новіші знаряддя праці і технології. Виникає проблема технологічної безпеки [56-60].

Це означає, що збільшується навантаження на всі структурні частини навколишнього середовища, є очевидною небезпека виснаження природних ресурсів, незворотних забруднень і зміни безпечних параметрів середовища, за якими створюються реальні умови для виникнення різного роду небезпек.

Отже, кожна держава повинна мати професійно придатні структури і системи захисту від наслідків імовірних небезпек. Головною метою таких систем є захист населення та зниження рівня ризику при виникненні певних небезпек шляхом запобігання, реагування і ліквідації їх наслідків. Можна навести основні принципи та способи забезпечення життєдіяльності:

– забезпечення населення всіма видами енергоресурсів (електроенергією, газом, нафтопродуктами, кам’яним вугіллям, водою тощо). Енергетична криза, що існує сьогодні, суттєво впливає на життєдіяльність людей. Це одна з найбільш актуальних проблем забезпечення безпеки будь-якої країни світу;

– забезпечення населення всіма необхідними параметрами і нормами матеріального середовища життя. Гострою проблемою для багатьох людей у різних країнах є недостатня кількість житла, комунального транспорту, суспільних закладів, спортивних комплексів, медичних закладів та інших елементів системи життєзабезпечення;

– забезпечення продуктами харчування. Продукти харчування є фізіологічною основою життєдіяльності. Із збільшенням чисельності населення ця проблема стає особливо гострою. Якщо людство не розробить нові перспективні технології вирощування продуктів харчування і своєчасно не адаптується до них, може виникнути небезпечна ситуація глобального масштабу;

– наявність і раціональне використання питної (прісної) води. Йдеться про охорону прісної води від забруднення, що може призвести до непридатності її використання для потреб населення. Звідси випливає важливість очищення води, боротьба з промисловим і побутовим забрудненням, виснаженням водойм;

– ліквідація, переробка або використання відходів виробництва. Особливо небезпечними є відходи атомних, хімічних, біологічних виробництв, кількість яких щорічно зростає і, відповідно, збільшується кількість відходів.

Дотримання основних принципів і способів забезпечення життєдіяльності є необхідною умовою для успішного функціонування людини.

3.3 Висновки до третього розділу

В даному розділі кваліфікаційної роботи розглянуто питання освітлення робочого місця. В безпеці в надзвичайних ситуаціях висвітлено питання основних принципів та способів забезпечення життєдіяльності.

ВИСНОВКИ

За результатами виконання кваліфікаційної роботи здійснено дослідження мережевих архітектур для критичних інфраструктур. Основні результати отримано у наступному вигляді:

– проаналізовано характеристики критичних інфраструктур для визначення їх сильних та слабких якостей при розробці мережевих архітектур;

– здійснено ідентифікацію критичних інфраструктур та подано основні кроки для її виконання;

– проведено оцінку ризиків для мережевих систем критичних інфраструктур, що дало змогу подати аналіз вразливостей, оцінити ймовірності та наслідки, визначити рівень ризику та подати опис заходів менімізації ризиків;

– описано визначення вразливостей мереж для критичних інфраструктур, що є важливим кроком у процесі аналізу безпеки та сітйкості систем;

– проаналізовано заходи безпеки для мереж критичних інфраструктур, які слід враховувати при захисті мереж критичних інфраструктур;

– проведено опис хмарних архітектурних рішень, що можуть використовуватись у мережах для критичних інфраструктур, що дасть змогу застосувати найкращі можливості різних хмарних технологій;

– розглянуто можливість використання технології SDN при проектуванні мережевих архітектур критичних інфраструктур, що показало позитивні елементи у вигляді централізованого керування мережею, динамічної адаптації мережевої інфраструктури, підвищеної безпеки, масштабованості і швидкого відновлення після відмови;

– подано можливість використання технології IBN для мережевих архітектур критичних інфраструктур.

– визначено та описано вимоги до архітектур мереж критичних інфраструктур, що повинні враховуватись при їх виборі та впроваджені;

– проведено аналіз моделей мережевих архітектур, що дає змогу застосувати найбільш відповідну модель для конкретного випадку критичної інфраструктури;

– виявлено, що серед існуючих архітектур в задачах даного класу буде ефективним застосування контернеризації, як гнучкого, швидкодійного та надійного варіанту розгортання сервісів;

– здійснено дослідження конкретної реалізації мультихмарної архітектури від компанії VMware, що надає можливість впроваджувати інновації та трансформувати клієнтський досвід, масштабувати і розвивати бізнес, підвищувати залученість та продуктивність працівників;

– досліджено основні аспекти Кібербезпекового каркасу NIST для критичної інфраструктури.

В розділі «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання освітлення робочого місця. В безпеці в надзвичайних ситуаціях висвітлено питання основних принципів та способів забезпечення життєдіяльності.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Critical Infrastructure Security and Resilience [Електронний ресурс]. – https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/chemical-sector – Назва з екрану. – Дата звернення: 4.05.2023.

2. Critical Infrastructure [Електронний ресурс]. – Режим доступу: https://www.techtarget.com/whatis/definition/critical-infrastructure – Назва з екрану. – Дата звернення: 4.05.2023.

3. Critical Infrastructure [Електронний ресурс]. – Режим доступу: https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en – Назва з екрану. – Дата звернення: 4.05.2023.

4. Defining critical infrastructure [Електронний ресурс]. – Режим доступу: https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/defining-critical-infrastructure – Назва з екрану. – Дата звернення: 4.05.2023.

5. What is network functions virtualization nfv [Електронний ресурс]. – Режим доступу: https://www.juniper.net/ru/ru/research-topics/what-is-network-functions-virtualization-nfv.html – Назва з екрану. – Дата звернення: 4.05.2023.

6. Announcing project northstar [Електронний ресурс]. – Режим доступу: https://blogs.vmware.com/networkvirtualization/2022/08/announcing-project-northstar.html/ – Назва з екрану. – Дата звернення: 4.05.2023.

7. Solution brief vmware cloud packs [Електронний ресурс]. – Режим доступу: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-solution-brief-vmware-cloud-packs.pdf – Назва з екрану. – Дата звернення: 5.05.2023.

8. Cloud packs [Електронний ресурс]. – Режим доступу: https://www.vmware.com/cloud-solutions/cloud-packs.html – Назва з екрану. – Дата звернення: 5.05.2023.

9. NSX [Електронний ресурс]. – Режим доступу: https://www.vmware.com/products/nsx.html – Назва з екрану. – Дата звернення: 5.05.2023.

10. Industry 5.0 – Towards a sustainable, human-centric and resilient European inustry [Електронний ресурс]. – Режим доступу: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/industry-50-towards-sustainable-human-centric-and-resilient-european-industry_en – Назва з екрану. – Дата звернення: 5.05.2023.

11. Industry 5.0, a transformative vision for Europe [Електронний ресурс]. – Режим доступу: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/industry-50-transformative-vision-europe_en – Назва з екрану. – Дата звернення: 6.05.2023.

12. Enabling Technologies for Industry 5.0 [Електронний ресурс]. – Режим доступу: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/enabling-technologies-industry-50_en – Назва з екрану. – Дата звернення: 6.05.2023.

13. A. D wankhade and P. N. Dr Chatur, “Comparison of Firewall and Intrusion Detection System,” Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 1, pp. 674–678, 2014, URL: http://ijcsit.com/docs/Volume 5/vol5issue01/ijcsit20140501145.pdf/.

14. T. King et al., “BLACKHOLE Community,” Internet Engineering Task Force (IETF), 2016. [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/rfc7999. – Назва з екрану. – Дата звернення: 6.05.2023.

15. D. S. Ms. Charjan, P. S. Ms. Bochare, and Y. R. Bhuyar, “An Overview of Secure Sockets Layer,” Int. J. Comput. Sci. Appl., vol. 6, no. 2, pp. 388–393, 2013

16. Industry 5.0 [Електронний ресурс]. – Режим доступу: https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en – Назва з екрану. – Дата звернення: 6.05.2023

17. Industry 4.0 [Електронний ресурс] – Режим доступу: https://www.quuppa.com/industry-4-0/?gclid=Cj0KCQiAm5ycBhCXARIsAPldzoWU20ocJRPYn64SA4xbl_dJgOXqvXcCHd96pTFxRRYJMibIFGEu-7EaAmzaEALw_wcB – Назва з екрану. – Дата звернення: 7.05.2023

18. Кулаков Ю.О. Комп'ютерні мережі / Ю.О. Кулаков – Юніор, 2005. – 397 с.

19. Вишневський В. М. Теоретичні основи проектування комп'ютерних мереж / В. М. Вишневський – Техносфера, 2004. – 512 с.

20. Amobile solutions [Електронний ресурс]. – Режим доступу: https://www.amobile-solutions.com/en/?gclid=Cj0KCQiAm5ycBhCXARIsAPldzoXq_gttAexROGuPD1BpFlttz_iRWPHwGHfJYkZCsHITrnzAGp00qRwaAkK_EALw_wcB – Назва з екрану. – Дата звернення: 7.05.2023

21. Digital transformation in manufacturing [Електронний ресурс]. – Режим доступу: https://blogs.cisco.com/manufacturing/how-is-digital-transformation-in-manufacturing-bridging-the-gap-to-productivity-security-resiliency-and-sustainability – Назва з екрану. – Дата звернення: 7.05.2023

22. Internet of Things [Електронний ресурс]. – Режим доступу: https://blogs.cisco.com/internet-of-things/modern-manufacturing-does-your-network-have-what-it-takes – Назва з екрану. – Дата звернення: 7.05.2023

23. Drath, R. Horch, A. “Industrie 4.0 Hit or Hype? IEEE Industrial Electronics Magazine.” June 2014, 56–58.

24. Беркман Л. Н. Архітектурна концепція побудови, принцип реалізації, ефективність застосування інтелектуальної телекомунікаційної мережі / Л. Н. Беркман, С. В. Толюпа // Зб. наук. праць ВІТІ НТУУ ―КПІ‖. – 2007. – №3. – С. 9-17.

25. Колченко В. О. Впровадження інтелекту в мережі наступного покоління (NGN) – перехід до мереж майбутнього покоління (FGN) / В. О. Колченко / Наукові записки УНДІЗ. – 2010. – №2(14). – С.80-85.

26. Беркман Л. Н. Проблеми створення сучасної конвергентної мережі на базі концепції FMC (Fixed-Mobile Convergence) / Л. Н. Беркман, О. І. Чумак, В. В. Григорович, П. Ю. Дещинський // Вісник УНДІЗ. – 2008. – №2. – С. 61-63.

27. Толюпа С. В. Структура інформаційної мережі та показники її ефективності / С. В. Толюпа, А. В. Сухін. // Зб. наук. праць КВІУЗ. – 2001. – №3. – С. 68-73.

28. Мурай А. В. Оценка качества телекоммуникационных услуг с учетом степени удовлетворения ожиданий и требований пользователей / А. В. Мурай // Наукові записки УНДІЗ. – 2013. – № 2(26). – С. 68-75.

29. Гребенніков В. О. Проблема загальнодоступності основних телекомунікаційних і інформаційних послуг в Україні та загальні підходи до її розв’язання / В. О. Гребенніков, Г. Ф. Колченко // Наукові записки УНДІЗ. – 2013. № 1(25). – С. 5-13.

30. Hermann, M. Pentek, T. Otto, B. “Design Principles for Industrie 4.0 Scenarios.” Presented at the 49th Hawaii International Conference on System Sciences. 2016

31. Колченко Г. Ф. Розроблення нормативних документів для забезпечення функціонування системи оперативно-технічного управління телекомунікаційними мережами / Г. Ф. Колченко, І. В. Шестак // Наукові записки УНДІЗ. – 2012. – № 2(24). – С. 5-8.

32. Система управління сучасними телекомунікаційними мережами : монографія : у 2 ч. / [Кривуца В. Г., Беркман Л. Н., Климаш М. М. та ін.]. – Київ : ДУІКТ, 2009. – 268 с.

33. Kagermann, H. Anderl, R. Gausemeier, J. Schuch, G. Wahlster, W. “Industrie 4.0 in a Global Context.” ACATECH 2016.

34. Industrial-Internet-of-Things-IIoT [Електронний ресурс]. – Режим доступу: https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT – Назва з екрану. – Дата звернення: 8.05.2023.

35. Industrial-internet-of-things-complete-guide [Електронний ресурс]. – Режим доступу: https://www.imperosoftware.com/blog/industrial-internet-of-things-complete-guide/ – Назва з екрану. – Дата звернення: 8.05.2023.

36. Cisco Software-Defined WAN (SD-WAN) FAQ [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us /solutions/collateral/enterprise-networks/sd-wan/nb-06-sw-defined-wan-faq-cte-en.html? dtid=osscdc000283 – Назва з екрану. – Дата звернення: 8.05.2023.

37. Cisco Software-Defined WAN (SD-WAN) Cloud onRamp for Colocation At-a-Glance [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-on-ramp-aag-cte-en.html – Назва з екрану. – Дата звернення: 8.05.2023.

38. Internet-of-things [Електронний ресурс]. – Режим доступу: https://www.wi-fi.org/discover-wi-fi/internet-of-things – Назва з екрану. – Дата звернення: 8.05.2023.

39. What Is Network Virtualization? [Електронний ресурс]. – Режим доступу: https://blog.gigamon.com/2018/01/04/network-virtualization-optimize/ – Назва з екрану. – Дата звернення: 8.05.2023.

40. Best Network Automation Tools [Електронний ресурс]. – Режим доступу: https://www.dnsstuff.com/network-automation-tools – Назва з екрану. – Дата звернення: 9.05.2023

41. What is network automation? [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/automation/network-automation.html – Назва з екрану. – Дата звернення: 9.05.2023.

42. Network automation and orchestration tools review and ratings [Електронний ресурс]. – Режим доступу: https://www.gartner.com/reviews/market/network-automation – Назва з екрану. – Дата звернення: 9.05.2023.

43. Network automation tools [Електронний ресурс]. – Режим доступу: https://www.pcwdld.com/network-automation-tools-and-software #wbounce-modal – Назва з екрану. – Дата звернення: 9.05.2023.

44. Solving the Network Virtualization Conundrum [Електронний ресурс]. – Режим доступу: https://www.arista.com/en/solutions/network-virtualization – Назва з екрану. – Дата звернення: 9.05.2023.

45. IoT devices separate wi-fi network [Електронний ресурс]. – Режим доступу: https://csolutionsit.com/iot-devices-separate-wi-fi-network/ – Назва з екрану. – Дата звернення: 9.05.2023.

46. F. Dad et al., “Optimal Path Selection Using Dijkstra’s Algorithm in Cluster-based LEACH Protocol,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 2, pp. 194–198, Feb. 2017.

47. Z. U. Rahman et al., “Investıgatıng the Pakıstan's Offshore Software Industry Infrastructure,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 3, pp. 237–243, Mar. 2017

48. Z. U. Rahman et al., “Magnetic Resonance Images Classification through Relevance Vector Machine,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 1, pp. 213–217, Jan. 2017

49. Types of IoT networks [Електронний ресурс]. – Режим доступу: https://euristiq.com/types-of-iot-networks/ – Назва з екрану. – Дата звернення: 10.05.2023.

50. Cellular vs wi-fi for IoT [Електронний ресурс]. – Режим доступу: https://www.particle.io/iot-guides-and-resources/cellular-vs-wifi-for-iot/ – Назва з екрану. – Дата звернення: 10.05.2023.

51. Private LTE or 5G [Електронний ресурс]. – Режим доступу: https://www.iplook.com/solutions/private-lte-5g-solution_s0013.html?gclid=CjwKCAiAs8acBhA1EiwAgRFdw6QjenpP7DfgJ_DFKVNMc0lE4cQmgOIAfmsWoDUoRxFFQN1kGpYc8BoCQJMQAvD_BwE – Назва з екрану. – Дата звернення: 10.05.2023.

52. Державні будівельні норми України. Інженерне обладнання будинків і споруд. Природне і штучне освітлення [Електронний ресурс]. – Режим доступу: http://kbu.org.ua/assets/app/documents/dbn2/95.1.%20%D0%94%D0%91%D0%9D%20%D0%92.2.5-28-2006.%20%D0%9F%D1%80%D0%B8%D1%80%D0%BE%D0%B4%D0%BD%D0%B5%20%D1%96%20%D1%88%D1%82%D1%83%D1%87%D0%BD%D0%B5%20%D0%BE%D1%81%D0%B2%D1%96%D1%82%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F.pdf – Назва з екрану. – Дата звернення: 06.05.2022.

53. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0007282-98#Text – Назва з екрану. – Дата звернення: 06.05.2022.

54. Про затвердження правил охорони праці під час експлуатації електронно-обчислювальних машин [Електронний ресурс]. – Режим доступу: https://dnaop.com/html/31562/doc-%D0%9D%D0%9F%D0%90%D0%9E%D0%9F_0.00-1.28-10 – Назва з екрану. – Дата звернення: 06.05.2022.

55. Про затвердження Правил охорони праці під час виконання робіт на висоті [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0573-07#Text – Назва з екрану. – Дата звернення: 06.05.2022.

56. Про затвердження Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці та Переліку робіт з підвищеною небезпекою [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0231-05#Text – Назва з екрану. – Дата звернення: 06.05.2022.

57. Проектування електрообладнання об’єктів цивільного призначення [Електронний ресурс]. – Режим доступу: http://kbu.org.ua/assets/app/documents/dbn2/92.1.%20%D0%94%D0%91%D0%9D%20%D0%92.2.5-23~2010.%20%D0%86%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%BD%D0%B5%20%D0%BE%D0%B1%D0%BB%D0%B0%D0%B4%D0%BD%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%B1%D1%83%D0%B4%D0%B8%D0%BD%D0%BA%D1%96%D0%B2%20%D1%96.pdf – Назва з екрану. – Дата звернення: 06.05.2022.

58. Правила улаштування електроустановок [Електронний ресурс]. – Режим доступу: https://art-energetyka.com.ua/%D0%9F%D1%80%D0%B0%D0%B2%D0%B8%D0%BB%D0%B0-%D1%83%D0%BB%D0%B0%D1%88%D1%82%D1%83%%B0%D0%BD%D0%BE%D0%B2%D0%BE%D0%BA.pdf – Назва з екрану. – Дата звернення: 06.05.2022.

59. Про затвердження "Правил будови електроустановок. Електрообладнання спеціальних установок" [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0272203-01#Text – Назва з екрану. – Дата звернення: 06.05.2022.

60. Про затвердження державних будівельних норм ДБН В.2.5-56:2010 "Інженерне обладнання будинків і споруд. Системи протипожежного захисту" [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0537738-10#Text – Назва з екрану. – Дата звернення: 06.05.2022.

Додатки

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Міжнародний університет цивільної авіації (Марокко)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник
тез доповідей

XI Міжнародної науково-практичної конференції молодих учених та студентів
7-8 грудня 2022 року

УКРАЇНА
ТЕРНОПІЛЬ – 2022

6. **В.А. Готович, І.Р. Ралік**
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ КЛІЄНТ-СЕРВЕРНОЇ АРХІТЕКТУРИ ДЛЯ ОБЛІКУ РЕАЛІЗАЦІЇ ТОВАРІВ В ТОРГІВЛІ 126
7. **В.В. Ковальчук, І.В. Чихіра, О.В. Тотосько**
КЕРУВАННЯ ПРОЦЕСОМ ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ПОЛІМЕРКОМПОЗИТНИХ ПОКРИТТІВ ПРИ ЗГИНІ 127
8. **А. Хом'як**
МЕТОДИ АНАЛІЗУ ЧАСОВИХ РЯДІВ З ВИКОРИСТАННЯМ РЕКУРЕНТНИХ НЕЙРОННИХ МЕРЕЖ 128
9. **Р.С. Гром'як, С.С. Серкіз**
ВЗАЄМОДІЯ БІЗНЕС ПРОЦЕСІВ З КЛІЄНТАМИ ЗА ДОПОМОГОЮ CRM-СИСТЕМ 129
10. **Р.С. Гром'як, С.С. Серкіз**
CRM-СИСТЕМА ЯК ІНСТРУМЕНТ УДОСКОНАЛЕННЯ ВЗАЄМОВІДНОСИН З КЛІЄНТАМИ 130
11. **В.А. Готович, А.В. Мачужак**
ЗАСТОСУВАННЯ МЕТОДОЛОГІЇ CI/CD ДЛЯ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ТЕСТУВАННЯ ТА РОЗГОРТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ 131
12. **І.В. Струтинська, В.О. Мельник**
РОЛЬ АВТОМАТИЗОВАНИХ СИСТЕМ КЕРУВАННЯ ЗАМОВЛЕННЯМИ 133
13. **Є.Б. Яворська, А.С. Каплунова**
АЛГОРИТМ ПОДАВЛЕННЯ ЗАВАД В ЕЛЕКТРОКАРДІОСИГНАЛАХ 135
14. **Є.Б. Яворська, А.О. Карнов**
ЗАСОБИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ОСОБИ У СИСТЕМАХ МОНІТОРИНГУ СТАНУ ЗДОРОВ'Я 136
15. **О.М. Петрик, В.О. Суховерша, С.В. Марценко**
ДОСЛІДЖЕННЯ МЕРЕЖЕВИХ АРХІТЕКТУР ДЛЯ КРИТИЧНИХ ІНФРАСТРУКТУР 137
16. **О.М. Петрик, В.О. Суховерша, С.В. Марценко**
ДОСЛІДЖЕННЯ РОЛІ ЮТ-ТЕХНОЛОГІЙ В ПРОМИСЛОВИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ 138
17. **І.В. Воробець**
ВПЛИВ КОМПОНЕНТІВ ЧАСОВИХ РЯДІВ НА ВИБІР МЕТОДУ ПРОГНОЗУВАННЯ 139
18. **О.О. Кузьо, В.К. Крилов, Н.Л. Мацюк**
ВИКОРИСТАННЯ ТЕХНОЛОГІЇ OSINT ДЛЯ ФОРМУВАННЯ ПОРТРЕТУ КОРИСТУВАЧА 140
19. **А.К. Карнаухов, О.О. Кузьо**
КОНСОЛІДАЦІЯ ІНФОРМАЦІЇ КОРИСТУВАЧІВ ЗА ДОПОМОГОЮ СТРУКТУР BIG DATA 141
20. **І.Г. Купратий, А.М. Паламар**
КОМП'ЮТЕРНА СИСТЕМА ДЛЯ ДИСТАНЦІЙНОГО МОНІТОРИНГУ СТАНУ ЗДОРОВ'Я ПАЦІЄНТІВ 142
21. **В. Лісовський, А. Зелінський, О. Сороківський**
АНАЛІЗ ЗАДАЧ МАШИННОГО АНАЛІЗУ ЗОБРАЖЕННЯ ТА СУЧАСНИХ МЕТОДІВ ЇХ ВИРІШЕННЯ 143
22. **А. Зелінський, В. Лісовський**
ПРОЕКТУВАННЯ ХМАРНОГО РІШЕННЯ ДЛЯ АНАЛІЗУ ПОТОКОВИХ ДАНИХ НА ОСНОВІ AWS KINESIS 145

Матеріали XI Міжнародної науково-практичної конференції молодих учених та студентів «АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль, 7-8 грудня 2022 року

УДК 004.72

О.М. Петрик, В.О. Суховерша, С.В. Марценко, к.т.н., доцент
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ДОСЛІДЖЕННЯ МЕРЕЖЕВИХ АРХІТЕКТУР ДЛЯ КРИТИЧНИХ ІНФРАСТРУКТУР

O.M.Petryk, V.O. Sukhoversha, S.V. Martsenko, Ph.D., Assoc. Prof.

RESEARCH OF NETWORK ARCHITECTURES FOR CRITICAL INFRASTRUCTURES

Згідно з інформацією від Cybersecurity and Infrastructure Security Agency для США виділено 16 критичних інфраструктурних секторів [1], що закріплені президентською директивою. Україна відноситься до країн, що активно розвиваються і перебувають у процесі цифрової трансформації. Досвід провідних країн світу у організації роботи мережевих архітектур для критичних інфраструктур потребує всебічного дослідження щодо використання в аналогічних шаблонах нашої країни.

Разом з іншими до секторів критичних інфраструктур відносять хімічну промисловість, комунікаційний сектор, дамби, невідкладну допомогу та систему надзвичайних ситуацій, фінансовий сектор, урядові організації, сектор IT технологій, транспортну систему, критичне виробництво, оборонна промисловість, енергетика, сільське господарство, охорону здоров'я, ядерну енергетику, водопостачання та водовідведення. Кожен з вищеназваних секторів має свої вимоги до організації мережевих архітектур та їх спільної взаємодії в межах держави.

Дослідження показують, що спільним для кожного з секторів при організації мережевої архітектури критичних інфраструктур є забезпечення масштабованості з максимальним використанням користувацького досвіду і зменшення вузьких місць для критичних даних. Має бути забезпечено оптимізацію вартості доставки даних через модернізацію існуючих мереж з використанням розумних технологій та програмування. Необхідно зменшити ризики та підвищити рівень довіри до таких мереж впроваджуючи міри безпеки для захисту критичних даних. Бажаним є спрощення роботи через використання автоматизації функцій та створення системи спостереження в реальному часі для покращення передбачуваності і надійності.

Для вирішення поставлених завдань можна використати рішення, що дадуть змогу:

- модернізувати мережу з використанням конвергованих IP та оптоволоконних рішень;
- змасштабувати мережеву роботу через модульність, енергетичну ефективність та захищеність платформ маршрутизації;
- спростити та пришвидшити мережеву прозорість, управління і роботу через автоматизацію мережевих функцій;
- покращити контроль через впровадження інтелектуальних, мережево програмованих технологій.

Використання досвіду провідних компаній при організації мережевих архітектур для критичних інфраструктур дасть змогу адаптувати їх до реалій України та забезпечити надійну роботу критичних секторів з можливістю подальшої модернізації. Масштабованість, захищеність та адаптивність необхідні при їх розробці.

1. Critical Infrastructure Sectors [Електронний ресурс]. – Режим доступу: https://www.cisa.gov/critical-infrastructure-sectors – Назва з екрану. – Дата звернення: 24.11.2022.

Матеріали XI Міжнародної науково-практичної конференції молодих учених та студентів «АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль, 7-8 грудня 2022 року

УДК 004.72

О.М. Петрик, В.О. Суховерша, С.В. Марценко, к.т.н., доцент
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ДОСЛІДЖЕННЯ РОЛІ ІОТ-ТЕХНОЛОГІЙ В ПРОМИСЛОВИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

O.M.Petryk, V.O. Sukhoversha, S.V. Martsenko, Ph.D., Assoc. Prof.

RESEARCH ON THE ROLE OF IOT TECHNOLOGIES IN INDUSTRIAL COMPUTER NETWORKS

Важко уявити сучасне виробництво без великої кількості сенсорів та давачів, актуаторів і системних рішень, що покращують виробничі процеси, підвищують безпеку, спрощують управління і забезпечують зростання капіталомісткості організації. Дослідження ролі Internet of Things (IoT) технологій в промислових мережах є важливим науково-технічним завданням в умовах індустрії 4.0 та 5.0.

Початок 4-ї технологічної революції відносять до 2011 року коли Working Group of Industry 4.0 презентувала набір рекомендацій для німецького уряду. Це призвело до комп'ютеризації виробничих процесів з використанням концепцій кібер-фізичних систем та IoT для досягнення "виробництва майбутнього". Це в свою чергу призвело до появи парадигм "Розумний продукт", "Розумна машина" та "Доповнений працівник". У розумному продукті збережено операційні дані, розумна машина стала частиною кібер-фізичної виробничої системи, а доповнений працівник отримав розумні методи та засоби для роботи у складних середовищах.

Технології IoT включають в себе використання сучасного бездротового телекомунікаційного покриття для обміну даними між радіочастотними мітками, сенсорами, актуаторами, мобільними телефонами забезпечуючи їх взаємодію при виконанні спільного завдання. Модель IoT складається з послуг, що використовують хмарні обчислення і створюють віртуальну інфраструктуру для роботи систем моніторингу, зберігання, інструментів аналітики та візуалізації результатів роботи. Це створює мережу глобального споживчого ланцюга, де приватність та захист даних виходять на перше місце і мають бути гарантовано забезпечені.

Індустрія 5.0 покликана доповнити 4.0 ставлячи дослідження та інновації на службу для переходу до стійкої, орієнтованої на людину європейської промисловості [1]. Цей підхід змінює вектор промисловості, який забезпечував ефективність та продуктивність виробництва, на індустрію покликану служити суспільству. Елементами, що пропонуються є адаптація орієнтованого на людину підходу впровадження цифрових технологій включаючи штучний інтелект, підготовка та перепідготовка працівників з використанням цифрових навичок, створення енергоефективних технологій з можливістю переробки та повторного використання, створення конкурентоспроможної світової індустрії базованої на дослідженнях.

У результаті впровадження IoT в промислові мережі покращились ефективність відслідковування робочого місця і час реакції на непередбачувані ситуації. Створились умови для протидії пандемії COVID-19 через використання моніторингу робочого середовища з визначенням соціального дистанціювання та дотримання карантинних мір. Зросла ефективність процесів трекінгу та обліку, знаходження та вирішення вузьких місць, моніторингу всіх ланок організації роботи компанії. Разом з тим виникло ряд питань пов'язаних з захистом інформації та самих IoT пристроїв.

1. What is Industry 5.0 [Електронний ресурс]. – Режим доступу: https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en – Назва з екрану. – Дата звернення: 24.11.2022.