Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту
Кафедра комп'ютерних систем та робототехніки

«Затверджую»
в.о. завідуючого кафедри
комп'ютерних систем та робототехніки
_____ к. ф.-м. н., доцент Максим Хруслов
«___» червня 2025 р.

Пояснювальна записка

до кваліфікаційної роботи
бакалавра

на тему: «МОДЕЛЬ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ ДЛЯ КОРПОРАТИВНОГО СЕКТОРУ З АНАЛІЗОМ СТІЙКОСТІ ДО ЗБОЇВ»

Спеціальність 151 –Автоматизація та комп'ютерно-інтегровані технології
Галузь знань 15 – Автоматизація та приладобудування
Освітня програма «Автоматизація та комп'ютерно-інтегровані технології»

Захищено на засіданні
Екзаменаційної комісії № 46
протокол № __ від __.06.2025 р.
Оцінка _____ / _____
Голова Екзаменаційної комісії
_____ **ЧУГАЙ А.М.**

Виконав:
Студентка групи КУ– 41
ХОДЄЄВА Марія Олегівна
Керівник:
к.ф.-м.н, доцент, доцент закладу вищої освіти
ХРУСЛОВ Максим Михайлович
Рецензент:
к.ф.-м.н., доцент кафедри інтелектуальних систем і технологій ХНУ ім. В. Н. Каразіна
КАРАСЬ Ірини В'ячеславівна _____

Харків – 2025

АНОТАЦІЯ

Пояснювальна записка до кваліфікаційної роботи бакалавра складається зі вступу, трьох розділів, висновків, списку використаних джерел і трьох додатків. Загальний обсяг роботи становить 67 сторінки, з яких 48 сторінок основної частини з 8 рисунками, 28 найменуваннями у списку використаних джерел та 3 додатками.

Метою кваліфікаційної роботи є проєктування відмовостійкої серверної інфраструктури для call-центру з використанням мережевого обладнання Fortinet, реалізацією VLAN, SD-WAN, LACP-з'єднань, резервного живлення та забезпеченням гнучкого масштабування.

Об’єкт дослідження – процес створення серверної інфраструктури організації, що функціонує в умовах нестабільного мережевого та електричного підключення, з необхідністю забезпечення безперервного доступу до критичних IT-сервісів.

Предмет дослідження – архітектура мережевої та енергетичної інфраструктури, зокрема механізми забезпечення енергонезалежності, автоматичного балансування навантаження, перемикання між джерелами живлення й каналами зв’язку в разі збоїв та пріорітезації обладнання.

Проблема полягає у побудові надійної, масштабованої та відмово-стійкої інфраструктури з мінімізацією простоїв, втрат даних та ручного втручання.

Область застосування – інфраструктурні рішення для контакт-центрів, офісів, дата-центрів та інших організацій, що потребують стабільної мережевої архітектури з високою готовністю до відмов.

Ключові слова: fault tolerance, Fortinet, VLAN, SD-WAN, LACP, резервування, серверна інфраструктура, безперебійне живлення, інфраструктурна безпека, відмовостійкість, UPS, генератор, топологія мережі, резервні канали, мережеве адміністрування.

ABTRACT

The explanatory note of the bachelor's qualification work consists of an introduction, three chapters, conclusions, a list of references, and three appendices. The total volume of the work is 67 pages, including 48 pages of the main content, 8 figures, 28 items in the list of references, and 3 appendices.

The purpose of this qualification work is to design a fault-tolerant server infrastructure for a call center using Fortinet networking equipment, with the implementation of VLANs, SD-WAN, LACP connections, backup power systems, and scalable architecture.

The object of the research is the process of designing a server infrastructure for an organization operating under conditions of unstable network and power connectivity, with the requirement to ensure uninterrupted access to critical IT services.

The subject of the research is the architecture of the network and power infrastructure, particularly the mechanisms for energy independence, automatic load balancing, switching between power sources and communication channels in case of failures, and equipment prioritization.

The problem addressed in this work is the development of a reliable, scalable, and secure infrastructure that minimizes downtime, data loss, and manual intervention during failures.

The application domain includes infrastructure solutions for contact centers, offices, data centers, and other organizations that require a stable network architecture with high fault tolerance.

Keywords: fault tolerance, Fortinet, VLAN, SD-WAN, LACP, redundancy, server infrastructure, uninterruptible power supply, infrastructure security, UPS, generator, network topology, backup channels, network administration.

ЗМІСТ

ВСТУП

Сучасний корпоративний сектор значною мірою залежить від надійності серверної інфраструктури, яка забезпечує функціонування критично важливих бізнес-процесів. Однак в умовах нестабільного інтернет-з'єднання та перебоїв у електропостачанні ефективність таких систем може суттєво знижуватися.

Особливу актуальність робота набуває через російське вторгнення в Україну, яке розпочалося 24 лютого 2022 року та суттєво вплинуло на стабільність критичної інфраструктури країни [1]. Згідно з працею [2], цілеспрямовані удари по критичній інфраструктурі та подальша відсутність доступу до енергоресурсів призводять до масштабних гуманітарних наслідків і масового переміщення цивільного населення. Військова агресія РФ супроводжується систематичними обстрілами енергетичних об'єктів, що призводить до масових відключень електроенергії та нестабільної роботи телекомунікаційних мереж. Незважаючи на резолюцію Генеральної Асамблеї ООН від 2 березня 2022 року [3], Росія продовжує атаки на критичну інфраструктурую. Загалом, джерело [4] зазаначає, що за час повномаштабного вторгнення відбулось більше 70 тисяч бомбардувань, близько тисячі атак поштодили урядові будівлі, майже 5,5 тисяч атак відбулось на об’єкти бізнесу.

Військові дії супроводжуються не лише руйнуванням енергетичних об’єктів, але й масовими кібератаками на українські ІТ-системи [5]. Це створює додаткові виклики для стабільності серверної інфраструктури та вимагає розробки рішень для забезпечення її безперебійної роботи в наявних умовах.

У даній роботі буде розглянуто моделювання серверної інфраструктури, яка здатна ефективно функціонувати навіть за умов нестабільного інтернет-з'єднання та частих перебоїв електропостачання. Окрему увагу буде приділено аналізу стійкості до збоїв, а також розробці стратегій забезпечення безперебійної роботи серверних систем в умовах сучасних загроз.

На сьогоднішній день існує низка методів і технологій, що дозволяють підвищити стійкість серверних систем. Зокрема, широко застосовуються

механізми резервного живлення, зокрема джерела безперебійного живлення та генератори, які можуть тимчасово забезпечувати електропостачання. Крім того, великого значення набувають технології автоматичного перемикання на резервні канали зв'язку, що дозволяють мінімізувати втрати доступності при проблемах з основною мережею. Також активно використовуються методи балансування навантаження та віртуалізації, що сприяють підвищенню ефективності використання ресурсів та покращенню доступності серверних систем.

Попри значний прогрес у сфері забезпечення надійності серверних інфраструктур, залишається низка проблем, які потребують вирішення. Серед них – недостатня адаптивність існуючих систем до різноманітних сценаріїв відмов, висока вартість впровадження комплексних рішень та обмеженість доступу до якісного інтернет-з'єднання у певних регіонах. Багато підприємств стикаються з труднощами при інтеграції сучасних рішень через складність їхньої реалізації та необхідність постійного моніторингу та оновлення обладнання.

Актуальність дослідження зумовлена потребою у розробці гнучких і ефективних моделей серверної інфраструктури, здатних функціонувати у нестабільних умовах. У світлі глобальних змін та збільшення ризиків у кіберпросторі корпоративні серверні системи потребують вдосконалених механізмів захисту, адаптації та резервування. Таким чином, дослідження в цій галузі є важливим як для великих корпорацій, так і для середнього та малого бізнесу, що також потребує надійної IT-інфраструктури.

У цій роботі буде запропоновано підхід до моделювання стійких серверних інфраструктур, який включає аналіз та застосування failover-механізмів, стратегій резервного живлення та підвищення мережевої доступності. Основна ідея полягає у створенні ефективної моделі, що дозволить підприємствам мінімізувати вплив зовнішніх факторів на їхні серверні системи та забезпечити безперервність бізнес-процесів.

Таким чином, робота спрямована на розробку оптимальних рішень, що дозволять підвищити стійкість корпоративних серверних інфраструктур, враховуючи сучасні виклики та обмеження.

РОЗДІЛ 1.
ПОСТАНОВКА ЗАДАЧІ ТА ОГЛЯД ЛІТЕРАТУРИ

1.1. Об’єкт, предмет та мета дослідження

Об’єктом даного дослідження є процес створення моделі серверної інфраструктури організації, що функціонує в умовах нестабільного мережевого та електричного підключення, з необхідністю забезпечення безперервного доступу до критичних IT-сервісів. Це включає як апаратні, так і програмні компоненти, які забезпечують стійкість та надійність роботи в умовах зовнішніх дестабілізуючих чинників.

Предметом дослідження є архітектура мережевої та енергетичної інфраструктури, зокрема:

- Механізми забезпечення енергонезалежності серверного обладнання в умовах перебоїв із живленням;
- Технології автоматичного балансування навантаження між мережевими та енергетичними компонентами;
- Системи перемикання між основними та резервними джерелами живлення й каналами зв’язку у разі збоїв;
- Принципи пріоритезації роботи обладнання з метою оптимізації використання ресурсів в аварійних ситуаціях.

Метою дослідження є проектування та моделювання ефективної архітектури серверної інфраструктури, здатної забезпечити безперебійну роботу критично важливих IT-сервісів організації в умовах нестабільного інтернет-з’єднання та електропостачання. Для досягнення цієї мети здійснено аналіз сучасних підходів до підвищення надійності та стійкості IT-інфраструктур, розроблено моделі резервування, адаптивного управління ресурсами та запропоновано практичні рекомендації щодо впровадження таких рішень у корпоративному середовищі.

1.2. Аналіз науково-технічної літератури та існуючих рішень

Забезпечення стійкості серверних інфраструктур є однією з ключових задач сучасного корпоративного сектору. У зв'язку з цим значна кількість досліджень та наукових робіт присвячена вивченню методів підвищення надійності та відмовостійкості серверних систем. Аналіз науково-технічної літератури та існуючих рішень дозволяє визначити основні напрями розвитку даної сфери та виявити їх переваги та недоліки.

Одним із ключових аспектів стабільної роботи серверних інфраструктур є наявність надійного джерела резервного живлення. В науковій літературі широко розглядаються такі технології:

- Джерела безперебійного живлення (UPS) – забезпечують тимчасову підтримку живлення у разі відключення електроенергії [6]. Однак, обмежений час автономної роботи та зниження ефективності при високих навантаженнях є їх основними недоліками.

- Дизельні та газові генератори – використовуються для довготривалого резервного живлення, проте вимагають регулярного обслуговування та значних капіталовкладень. У той же час у праці [7] вірно зазначено «В цілому впровадження генераторів в Україні забезпечує стабільність енергопостачання, надійність живлення...»

- Гібридні системи живлення (сонячні панелі, акумуляторні батареї, альтернативні джерела) – «інтеграція відновлювальних джерел енергії з резервними системами здатна зменшити витрати на енергію в періоди пікового споживання» зазначено в праці [8]. У той же час такі системи мають високі початкові витрати та залежать від погодних умов.

Відмовостійкість серверних систем та failover-механізми. Забезпечення безперервної роботи серверних інфраструктур передбачає використання failover-механізмів та кластерних технологій. Сучасні рішення включають:

- Кластеризація серверів – дозволяє розподіляти навантаження між кількома вузлами, забезпечуючи їхню відмовостійкість. До популярних

технологій належать VMware HA, Microsoft Failover Clustering, Proxmox VE та Kubernetes [27].

- Автоматичне перемикання (failover) – використовується для швидкої заміни несправного сервера на резервний [9]. Недоліками є складність налаштування та висока вартість таких рішень для середнього бізнесу.
- Реплікація даних – забезпечує синхронне або асинхронне копіювання даних між серверами, що мінімізує ризик втрати інформації. Такі рішення застосовуються у базах даних (MySQL Replication, PostgreSQL Streaming Replication) та файлових системах (Ceph, GlusterFS) [10].

Мережеві технології та оптимізація доступності. Окрім внутрішніх механізмів відмовостійкості, важливим фактором є стабільність мережевого підключення. Основні технології, що розглядаються у наукових публікаціях:

- Software-Defined Wide Area Network (SD-WAN) – дозволяє динамічно керувати маршрутизацією трафіку та балансувати навантаження між різними провайдерами інтернету [11].
- Load Balancing (балансування навантаження) – використовується для рівномірного розподілу запитів між кількома серверами, що зменшує ризик перевантаження та відмови. Приклади рішень: Nginx, HAProxy, AWS Elastic Load Balancing [12].
- Мережеві протоколи з високою доступністю (BGP, VRRP, HSRP) – дозволяють забезпечити резервне маршрутизаційне з'єднання між серверами та дата-центрами [28].

1.3. Виявлення проблем та обґрунтування необхідності дослідження

Аналіз існуючих рішень та необхідність подальших досліджень

Проведений аналіз показує, що існуючі методи забезпечення стійкості серверних інфраструктур мають свої переваги та недоліки. Зокрема:

- Більшість резервних джерел живлення мають обмежений час автономної роботи та потребують значних капіталовкладень.
- Failover та кластерні технології складні у налаштуванні та потребують високого рівня технічної експертизи.

- Оптимізація мережевої доступності за допомогою SD-WAN та балансування навантаження є ефективною, але не завжди доступною для малого та середнього бізнесу через високі витрати.

Розробка моделі об'єднання існуючих підходів буде розглянута в роботі надалі. У даній роботі буде розглядатися розробка моделі, яка б дозволила поєднати вже існуючі підходи, аби забезпечити систему, стійку до відключень електроенергії, інтернет-відключень та нестабільного з'єднання. Об’єднання технологій резервного живлення, failover-механізмів та мережевої оптимізації дозволить створити комплексне рішення, яке забезпечить високий рівень надійності та доступності серверної інфраструктури. Особлива увага буде приділена розробці ефективного алгоритму інтеграції цих підходів, оцінці їх продуктивності та економічної доцільності.

Висновки за розділом 1

У першому розділі визначено, що об’єктом дослідження є побудова серверної інфраструктури для забезпечення безперервної роботи IT-сервісів в умовах нестабільного електро- та мережевого живлення. Предметом дослідження виступають технічні рішення, що забезпечують енергонезалежність, відмовостійкість і адаптивне керування ресурсами. Сформульовано мету дослідження — проєктування стійкої архітектури серверної інфраструктури для корпоративного середовища.

Огляд літератури дозволив узагальнити сучасні підходи до резервування енергопостачання, кластеризації, реплікації даних і мережевої оптимізації. Встановлено, що ці рішення хоч і підвищують надійність, але часто є дорогими, складними у впровадженні або малодоступними для малого та середнього бізнесу.

Виявлено потребу в комплексній моделі, що поєднує переваги наявних технологій і здатна забезпечити високу надійність та доступність IT-сервісів у складних умовах експлуатації.

РОЗДІЛ 2.
ПРОЕКТУВАННЯ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ

2.1. Вибір інструментів та платформ для проектування

Для побудови моделі серверної інфраструктури з урахуванням сучасних вимог до надійності, масштабованості та безпеки було обрано інструменти, які забезпечують високий рівень деталізації, підтримку технічних стандартів та можливість адаптації до специфіки IT-інфраструктур. Основним середовищем для візуального проєктування стала програма Microsoft Visio, яка відзначається своєю зрозумілістю, доступністю для користувачів різного рівня підготовки та зручністю внесення змін у процесі розробки.

Однією з ключових причин вибору саме Microsoft Visio є підтримка кастомних трафаретів (stencils) від виробників мережевого обладнання, зокрема Fortinet, що включають точні графічні зображення пристроїв серій FortiGate, FortiSwitch та супутнього обладнання.

Для уточнення технічних характеристик обраного обладнання, а також перевірки сумісності компонентів, були використані офіційні технічні специфікації від виробника Fortinet, а також документація по SD-WAN [13], VLAN [14], LACP [15], UPS та генераторам.

2.2. Архітектурне рішення

Основу мережевої інфраструктури складають два міжмережеві екрани (firewalls) типу Fortinet FortiGate (модельний ряд 100F/200F), які функціонують у режимі кластеризації високої доступності (HA clustering). У цьому режимі один пристрій виконує роль активного вузла, тоді як інший залишається пасивним і бере на себе обробку трафіку лише у разі відмови активного вузла [27]. Синхронізація станів між вузлами кластера здійснюється через виділені інтерфейси, що дозволяє мінімізувати час перемикання.

Для підключення до глобальної мережі використовується три інтернет-провайдери, два з яких надають оптоволоконні (FTTH) канали доступу, а третій — система супутникового зв’язку Starlink. Така конфігурація гарантує

географічне та технологічне різноманіття каналів зв’язку, що знижує ймовірність одночасної втрати всіх каналів. Всі інтерфейси зовнішніх підключень маршрутизаторів з’єднані з усіма провайдерами відповідно до принципу повної сітки (full-mesh topology).

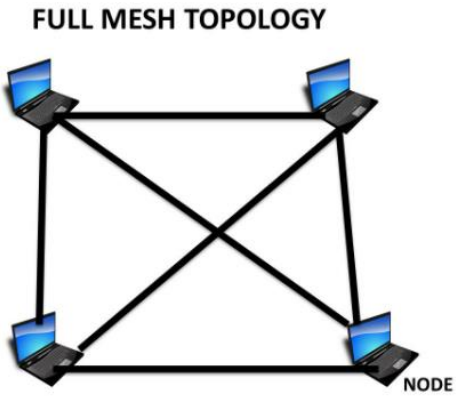


Рисунок 2.1 – візуалізація типології повної сітки [23].

Для керування трафіком між каналами зв’язку реалізовано програмно-визначену мережу широкосмугового доступу (SD-WAN), яка дозволяє динамічно маршрутизувати трафік залежно від поточних метрик якості каналу. Моніторинг параметрів — таких як затримка (latency), варіативність затримки (jitter) та втрата пакетів (packet loss) — виконується в реальному часі. На основі цих параметрів розраховується інтегральна метрика якості каналу зв’язку за формулою:

$$Q = w_1 \times L + w_2 \times J + w_3 \times P, \quad (2.1)$$

де Q — інтегральна оцінка якості обслуговування;

L — затримка передавання (latency), мс;

J — варіативність затримки (jitter), мс;

P — втрата пакетів (packet loss), %;

w_1, w_2, w_3— вагові коефіцієнти, що визначають відносну важливість кожного з параметрів залежно від специфіки застосунку чи бізнес-вимог.

Ядро мережі сформоване двома core-комутаторами рівня 3 (L3), які з’єднані з кожним маршрутизатором окремими фізичними каналами. До кожного

з core-комутаторів підключено access-комутатори, які відповідають за логічне розділення мережі на сегменти (VLAN 10, VLAN 20, VLAN 30 та Server VLAN). Фізичне з'єднання access-комутаторів із core-комутаторами реалізовано за допомогою агрегації каналів зв'язку (LACP — Link Aggregation Control Protocol), що дозволяє об'єднати декілька фізичних портів в один логічний канал, підвищуючи смугу пропускання та відмовостійкість.

Для забезпечення стійкості до топологічних петель у мережі використовується протокол Spanning Tree Protocol (STP), який динамічно визначає та блокує надлишкові шляхи, що можуть призвести до циклічного розповсюдження трафіку. Таким чином забезпечується унітарність шляху в комутаційній площині мережі.

Кожен сервер фізично підключений до двох access-комутаторів за схемою dual-homing, що дозволяє зберегти з'єднання навіть у разі виходу з ладу одного комутатора. Для логічного об'єднання цих комутаторів у єдиний віртуальний пристрій використовується технологія Multi-Chassis Link Aggregation (MLAG), яка синхронізує стан портів між комутаторами, зберігаючи прозорість топології для підключеного обладнання.

Живлення мережевої інфраструктури здійснюється через джерело безперебійного живлення (UPS), яке забезпечує стабільну подачу енергії у разі зникнення основного електропостачання. До UPS підключено електромеханічний перемикач джерел живлення (A/B power switch), який дозволяє автоматично перемикатися між мережею та резервним дизельним генератором, підтримуючи енергетичну автономність системи.

Визначення ступеня надійності системи відбувається за допомогою коефіцієнта доступності (Availability, A), який розраховується як:

$$A = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}, \tag{2.2}$$

де MTBF — середній час між відмовами (Mean Time Between Failures),

MTTR — середній час відновлення (Mean Time To Repair).

Чим ближче значення A до 1, тим вища надійність системи.

Розподіл мережевих ресурсів між сервісами виконується за допомогою механізму Quality of Service (QoS), який дозволяє призначати різні пріоритети для різних типів трафіку (наприклад, IP-телефонії, баз даних, поштових серверів тощо). Смуга пропускання для кожного класу трафіку визначається згідно з формулою:

$$BW_i = \frac{BW_{total} \times W_i}{\sum_{j=1}^{n} W_j}, \quad (2.3)$$

де BW_i — смуга пропускання, що виділяється для і-го класу трафіку, Мбіт/с;

BW_{total} — загальна доступна смуга пропускання каналу, Мбіт/с;

W_i — ваговий коефіцієнт пріоритету для і-го класу трафіку;

$\sum_{j=1}^{n} W_j$ — сума вагових коефіцієнтів усіх n класів трафіку.

Це дозволяє гнучко адаптувати мережу до змін у навантаженні та забезпечити безперебійне функціонування критичних служб.

Надмірність топології аналізується за допомогою коефіцієнта надмірності (Redundancy ratio):

$$R = \frac{N_{actual}}{N_{required}}, \quad (2.4)$$

де N_{actual} — фактична кількість незалежних з'єднань,

$N_{required}$ — мінімально необхідна кількість для забезпечення базової функціональності.

У стабільних мережах корпоративного рівня вважається доцільним, щоб R ≥ 2.

2.3. Вибір обладнання та обґрунтування вибору

2.3.1. Маршрутизатори FortiGate — обґрунтування вибору

Маршрутизатори FortiGate належать до класу NGFW (Next Generation Firewall) і виконують широкий спектр функцій — від фільтрації трафіку й захисту від мережевих загроз до підтримки VPN, маршрутизації та балансування навантаження. У серверній інфраструктурі корпоративного рівня вони відіграють ключову роль як шлюз між локальною мережею та зовнішніми мережами, забезпечуючи як продуктивність, так і безпеку. Для досягнення високої доступності застосовується конфігурація з двома однаковими

пристроями в режимі HA (High Availability), що дозволяє одному маршрутизатору миттєво замінити інший у разі відмови.

Наприклад, для потреб call-центру, в якому працюють від 60 до 100 активних користувачів, та використовується 3 окремі VLAN (наприклад, для операторів, адміністрації та технічного персоналу), доцільно обрати моделі FortiGate 100F або FortiGate 200F. Модель FortiGate 100F забезпечує до 20 Gbps базової пропускної здатності міжмережевого екрану, близько 1.4 Gbps для IPS (Intrusion Prevention System) і до 1 Gbps при повному навантаженні функцій NGFW. Модель FortiGate 200F забезпечує ще вищу продуктивність: до 35 Gbps для базового фаєрволу, 3.5 Gbps для IPS і до 2.5 Gbps при повному навантаженні.

Для оцінки потреби в пропускній здатності враховується середнє навантаження від одного користувача — близько 2 Mbps (враховуючи голосові дзвінки, доступ до CRM-системи, відео-дзвінки та інші сервіси). Таким чином, при 100 одночасно активних користувачах маємо мінімальну необхідну пропускну здатність:

$$B_{min} = N \times L_{user} = 100 \times 2 = 200, \quad (2.5)$$

де B_{min} — мінімально необхідна смуга пропускання для забезпечення коректної роботи мережевої інфраструктури, Мбіт/с;

N — кількість одночасно активних користувачів;

L_{user} — середнє навантаження від одного користувача, Мбіт/с.

З урахуванням можливих пікових навантажень, шифрування трафіку, використання DPI (Deep Packet Inspection), VPN та резерву на масштабування, рекомендується п’ятикратний запас:

$$B_{rec} = B_{min} * K_{res} = 200 * 5 = 1000, \quad (2.6)$$

де B_{rec} — рекомендована смуга пропускання з урахуванням резерву, Мбіт/с;

K_{res} — коефіцієнт резервування (рекомендовано $K_{res} = 5$).

Це відповідає можливостям FortiGate 100F, однак модель FortiGate 200F забезпечує кращу продуктивність на перспективу, знижує ризики перевантаження та дозволяє впроваджувати додаткові функції без шкоди для швидкодії.

Обидві моделі мають SFP-порти для оптичного підключення до Core Switch, що є необхідним для реалізації схеми з високою доступністю. Для підвищення надійності використовується SD-WAN Fortinet, який дозволяє контролювати якість каналів до інтернет-провайдерів і автоматично перемикатися на резервний канал у разі проблем із основним.

2.3.2. Комутатори Core switches

Core Switch — це центральний елемент мережевої інфраструктури, що забезпечує швидку маршрутизацію між VLAN, з'єднання між маршрутизаторами, серверами та доступними комутаторами (access/VLAN switches). На відміну від комутаторів доступу, core switch має високі показники пропускної здатності, кількість портів із підтримкою SFP+ (10G), а також функціональність L3 для маршрутизації на основі IP.

У запропонованій інфраструктурі використовується два core switch для забезпечення відмовостійкості. Кожен з них підключений до обох FortiGate (через порти SFP1 та SFP2) і до кожного VLAN-комутатора через порти 5–8 (по 4 лінії), що працюють у режимі LACP (Link Aggregation Control Protocol). LACP дозволяє агрегувати декілька фізичних портів в один логічний канал, збільшуючи пропускну здатність і забезпечуючи резервування.

Для call-центру з 60–100 користувачами та сервером, що обслуговує бази даних, IP-телефонію, CRM, тощо, мінімальні вимоги до пропускної здатності визначаються так:

- Для користувачів: 100 користувачів × 2 Mbps = 200 Мбіт/с
- Для доступу до сервера: 200 Мбіт/с (вхідний трафік) + 200 Мбіт/с (вихідний)
- Для внутрішньої маршрутизації між VLAN (inter-VLAN routing): ≈ 500 Мбіт/с
- З урахуванням запасу: ≥ 1000 Мбіт/с

Отже, необхідно обрати комутатор із щонайменше 8 портами 1G і кількома портами 10G (наприклад, для підключення до FortiGate та між собою). Прикладами таких моделей є:

- Cisco Catalyst 9500 — до 40 портів 10G SFP+, підтримка L3, MLAG, VRRP.
- Fortinet FortiSwitch 1048E — 48 × GE + 4 × 10GE SFP+, інтеграція з FortiGate, підтримка STP та LACP.
- MikroTik CRS317 — бюджетний варіант із 16 SFP+ портами, підтримкою L3, QoS, STP.

Рисунок 2.2 – Комутатор CRS317-1G-16S+RM [24].

Крім пропускної здатності, ключовим є підтримка протоколів:

1. STP (Spanning Tree Protocol) — виключає петлі в мережі.
2. VRRP або MC-LAG — дозволяють забезпечити логічну єдність між core switch та резервування на рівні L3.
3. QoS — для пріоритизації критичного трафіку (IP-телефонія, бази даних).

Формально, кількість портів комутатора n повинна задовольняти вимогу:

$$n \geq N_{VLAN} * L_{switch} + N_{router} + N_{uplink}, \quad (2.7)$$

де n — мінімальна кількість портів, необхідна на одному комутаторі, шт.;

N_{VLAN} — кількість віртуальних локальних мереж (VLAN), які обслуговує комутатор, шт.;

L_{switch} — середня кількість користувачів або пристроїв, підключених до однієї VLAN через даний комутатор, шт.;

N_{router}— кількість портів, необхідна для підключення до маршрутизаторів або шлюзів безпеки (наприклад, FortiGate), шт.;

N_{uplink} — кількість uplink-портів для підключення до core-комутаторів або організації резервування (LACP, stacking), шт.

У нашому випадку:

$$n \geq 4 \times 4 + 2 + 2 = 20.$$

Отже, комутатор із 24 портами (частково SFP+) відповідає вимогам. Бажано наявність принаймні 4 SFP+ портів для 10G-зв'язку з FortiGate і між собою.

2.3.3. Комутатори рівня доступу (VLAN Switches)

Комутатори рівня доступу (або Access Switches) використовуються для підключення кінцевих пристроїв у межах визначеної віртуальної локальної мережі (VLAN). У запропонованій архітектурі використовуються чотири окремі VLAN-комутатори: для VLAN 10, VLAN 20, VLAN 30 та Server VLAN. Вони підключені до обох core switch через LACP-зв'язки, що забезпечують резервування та підвищену пропускну здатність.

Кожен access switch має принаймні два uplink-порти (1 і 2) для підключення до core switch (по одному на кожен), що забезпечує dual-homing. Це гарантує, що в разі відмови одного з core switch або лінії зв'язку, другий шлях продовжить забезпечувати з'єднання.

Пропускна здатність access-комутаторів визначається кількістю користувачів, які підключені до кожної VLAN, а також характером їх трафіку. Для call-центру можна припустити рівномірний розподіл 100 користувачів по 3 VLAN (по ~33 на VLAN).

Типовий профіль користувача call-центру включає:

- IP-телефонія (≈ 100 Kbps),
- Доступ до CRM через веб-інтерфейс (≈ 1 Mbps),
- Надсилання запитів до сервера баз даних (≈ 500 Kbps).

Сумарне навантаження на один access switch:

$$BW_{total} = N_{users} \times BW_{user}, \quad (2.8)$$

де BW_{total} — сумарна пропускна здатність, необхідна для обслуговування всіх користувачів, підключених до одного access switch, Мбіт/с;

N_{users} — кількість активних користувачів або пристроїв, підключених до комутатора доступу, шт.;

BW_{user} — середнє навантаження на одного користувача, Мбіт/с.

Отже, для одного комутатора:

$$BW_{total} = 33 \times 1.5 \ = 49.5 \ (\approx 50) \text{ Мбіт/с.}$$

З урахуванням запасу на пікові навантаження, доцільно закладати мінімум 100 Mbps uplink із підтримкою LACP (2x100 Mbps або 1x1 Gbps). Тобто, навіть бюджетні комутатори з двома 1G портами uplink підходять для цієї задачі. Якщо планується зростання кількості користувачів або більший обсяг даних, краще обирати моделі із підтримкою 10G uplink.

Приклади відповідних комутаторів:

- Cisco Catalyst 2960X — 24 або 48 портів GE + 2 SFP uplink, підтримка VLAN, QoS [16].
- TP-Link JetStream T1600G-28TS — до 24 GE + 4 SFP, L2+, бюджетний варіант [17].
- FortiSwitch 224E/248E — інтеграція з FortiGate, підтримка VLAN, QoS, STP [18].

Рисунок 2.3 – комутатор FortiSwitch 224E Series.

Формальні критерії вибору access-комутатора:

- Uplink: ≥ 2 порти 1G для LACP;
- Кількість портів ≥ кількість користувачів + запас (для 33 користувачів — 48 портів оптимально);
- Uplink: ≥ 2 порти 1G для LACP;
- Підтримка VLAN, STP, QoS.
- Можливість централізованого управління через core switch або контролер.

У випадку Server Switch, що використовується для підключення серверного обладнання, доцільно застосовувати моделі з підтримкою SFP+ (10G) для забезпечення високої швидкості доступу до даних. Два uplink-порти до core switch через 10G — це стандартна практика в дата-центрах для мінімізації затримок.

2.3.4. Інтернет провайдери

В умовах триваючої війни в Україні забезпечення стабільного та безперервного інтернет-з’єднання стає одним з ключових завдань для корпоративного сектору, особливо для критичних систем, таких як call-центри, державні установи, гуманітарні організації. Надійність провайдерів повинна гарантувати доступ до зовнішніх ресурсів навіть у разі перебоїв з енергопостачанням, обстрілів чи пошкодження наземної інфраструктури.

Мінімальна рекомендація — підключення щонайменше до трьох незалежних провайдерів з різними маршрутами передачі даних, фізичними точками входу в будівлю та різною технологічною природою (волокно, супутник, мобільний доступ).

Використання двох оптичних каналів зв’язку (Fiber to the Building/Home) дає високу пропускну здатність, низьку затримку та стабільність з’єднання. Для вибору провайдерів потрібно враховувати:

1. Топологічну незалежність (кабелі не повинні проходити однією трасою);
2. Наявність генераторів на вузлах зв’язку (для роботи під час відключення електроенергії);
3. Резервне живлення обладнання провайдера поблизу об'єкта;
4. Відмовостійкість DNS, наявність IPv6, захист від DDoS.
5. В умовах війни важливо, щоб провайдер мав резервні канали за межами України через Польщу, Угорщину або Словаччину.

Для call-центру зі 100 активними користувачами з піковим споживанням трафіку 1.5 Mbps на користувача (включно з голосовими сервісами), загальна потреба в пропускній здатності:

$$BW_{required} = N_{active} \times BW_{peak} = 100 \times 1{,}5 = 150, \quad (2.9)$$

де $BW_{required}$ — мінімально необхідна пропускна здатність каналу, Мбіт/с;

N_{active} — кількість одночасно активних користувачів, шт.;

BW_{peak} — пікове навантаження, яке створює один користувач, Мбіт/с.

З урахуванням резерву на протокольний overhead, використання VPN, шифрування, DPI (Deep Packet Inspection), а також вимог до відмовостійкості системи, доцільно враховувати дворазовий запас пропускної здатності для кожного каналу зв'язку. Отже, для кожного з двох провайдерів потрібно передбачити:

$$BW_{provider} \geq 2 \times BW_{required} = 2 \times 150 = 300 \text{ Мбіт/с}. \quad (2.10)$$

Starlink виступає як третій провайдер, що забезпечує незалежність від наземної інфраструктури, яка є найбільш вразливою до атак чи пошкоджень. Основні переваги:

- Автономність — працює навіть за повної втрати оптоволоконного зв'язку;
- Власне резервне живлення (може працювати через UPS чи генератор);
- Глобальне покриття — зв'язок здійснюється напряму з супутниками.

Недоліки, які потрібно враховувати:

- Затримка вище, ніж у оптоволоконного зв'язку (від 30 до 60 мс);
- Варіативність швидкості залежно від погоди та завантаження;
- Орієнтованість на резерв, а не постійне використання [19].

З огляду на це, Starlink ідеально підходить як третій резервний канал, який активується автоматично через SD-WAN при повній втраті основних каналів.

Формалізовано вибір можна виконувати за зваженою сумою балів, що враховує параметри:

$$S = w_1 \times U + w_2 \times R + w_3 \times L + w_4 \times D, \quad (2.11)$$

де S — підсумковий інтегральний бал;

w_1, w_2, w_3, w_4 — вагові коефіцієнти, що відображають важливість кожного з параметрів (де $w_1 + w_2 + w_3 + w_4 = 1$);

U — оцінка пропускної здатності або швидкодії (Throughput);

R — оцінка рівня надійності (Availability / Reliability);

L — оцінка затримок (Latency), зворотна величина (тобто нижчі затримки — вищий бал);

D — оцінка підтримки додаткових функцій (наприклад, DPI, VPN, SD-WAN, тощо).

Максимальне значення S вказує на оптимального кандидата.

2.3.5. Вибір ДБЖ та генератора

Нестабільність електропостачання є однією з найбільших загроз для безперебійної роботи серверної інфраструктури, зокрема у випадках раптових відключень, перепадів напруги чи пошкодження зовнішніх електричних мереж. Це особливо важливо для корпоративних об'єктів, таких як call-центри, де надійність електроживлення безпосередньо впливає на стабільність бізнес-процесів.

Резервна система живлення виконує два основні завдання:

- Забезпечення безперебійного переходу на альтернативне джерело живлення при аварійному вимкненні основного (завдяки ДБЖ).
- Забезпечення живлення інфраструктури протягом тривалого часу (до кількох годин чи навіть днів) – за допомогою генератора.

Одним із ключових елементів системи безперебійного живлення, як зазначено вище, є ДБЖ (джерело безперебійного живлення). Воно забезпечує електроживлення на час, необхідний для автоматичного перемикання на резервний генератор. Враховуючи можливі збої у роботі основної енергомережі, ДБЖ повинне надавати резервне живлення на кілька хвилин, що дозволяє системі уникнути збоїв та коректно виконати процедуру автоматичного перемикання на генератор.

Існує кілька типів джерел безперебійного живлення (ДБЖ), кожен з яких характеризується своїм принципом роботи, рівнем захисту навантаження та часом перемикання на резервне живлення. Найбільш поширеними є три типи:

Off-line (або Stand-by), Line-interactive та On-line (або Double Conversion). Розглянемо їх детальніше.

Off-line ДБЖ (Stand-by UPS) – це найбільш проста й економічна конструкція джерела безперебійного живлення. За нормальних умов навантаження отримує живлення безпосередньо від електромережі. У разі зникнення напруги мережі система перемикається на акумуляторну батарею за допомогою реле. Час перемикання становить від 2 до 10 мс, що є прийнятним для некритичних пристроїв (наприклад, персональних комп'ютерів, офісного обладнання), але може бути недостатнім для серверного обладнання, чутливого до короткочасних перерв у живленні.

Line-interactive ДБЖ на відміну від Off-line, ці пристрої мають автотрансформатор з можливістю корекції вхідної напруги (AVR — Automatic Voltage Regulation), завдяки чому вони можуть стабілізувати живлення без переходу на акумулятори. Як і Off-line моделі, вони працюють у нормальному режимі через мережу, але реагують швидше на збої, із часом перемикання 2–4 мс. Line-interactive ДБЖ є оптимальними для робочих станцій, мережевого обладнання середньої критичності, однак у разі серйозних коливань напруги або високих вимог до безперервності живлення їхня ефективність недостатня.

On-line ДБЖ (Double Conversion) є найбільш надійним і технологічно досконалим. Його принцип роботи полягає в подвійному перетворенні енергії: змінний струм з електромережі перетворюється в постійний, після чого знову інвертується у стабілізований змінний струм, який подається на навантаження. Така архітектура забезпечує повну електричну ізоляцію навантаження від мережі та постійне живлення обладнання від інвертора, незалежно від якості вхідної напруги. Переваги On-line ДБЖ:

- Нульовий час перемикання (0 мс) — живлення подається без перерви навіть при зникненні мережі.
- Максимальний рівень захисту від просідань, піків напруги, електромагнітних перешкод та гармонік.

- Можливість роботи в умовах сильно нестабільної або забрудненої електромережі.

Усі ці переваги є важливими, оскільки навіть короткочасні перебої в електроживленні можуть призвести до пошкодження серверного обладнання або втрати важливих даних. Саме тому для серверних приміщень, дата-центрів, вузлів зв'язку та call-центрів, де неприпустимі навіть мілісекундні збої у живленні, доцільно використовувати On-line ДБЖ. Їх застосування забезпечує високу надійність функціонування IT-інфраструктури та захист даних від пошкодження або втрати внаслідок аварійного вимкнення обладнання. Незважаючи на вищу вартість у порівнянні з іншими типами, On-line ДБЖ є економічно доцільним вибором при розрахунку сукупної вартості простою критичних систем.

Рисунок 2.4 – приклади можливих ДБЖ [26].

Таким чином, ДБЖ є необхідним компонентом для забезпечення високої доступності та безпеки серверної інфраструктури.

Для коректного вибору потужності ДБЖ потрібно провести розрахунки з урахуванням всіх пристроїв, що будуть підключені до резервного живлення. Це включає сервери, мережеві пристрої, робочі станції та допоміжну техніку. Загальна потужність інфраструктури може варіюватися в межах 20-30 кВт, в залежності від конкретної конфігурації обладнання.

Формула для визначення потужності:

$$P_{total} = \sum_{i=0}^{n} P_i, \tag{2.12}$$

де P_{total} — споживання потужності всією інфраструктурою, кВт;

P_i — потужність окремого пристрою, кВт;

n — кількість пристроїв в системі.

Формула для визначення потужності ДБЖ та генератора:

$$P_{\text{ДБЖ}} = P_{total} \times k, \tag{2.13}$$

де $P_{\text{ДБЖ}}$ — розрахункова потужність, яку має забезпечити ДБЖ, кВт;

k — коефіцієнт запасу потужності (рекомендоване значення: 1.2–1.3).

Якщо система споживає в середньому 20 кВт, враховуючи потенційні коливання потужності та пік навантаження, треба вибирати ДБЖ та генератор з резервом потужності.

Якщо загальна потужність інфраструктури складає 20 кВт, то вибір ДБЖ з коефіцієнтом запасу k=1.3 дозволить вибрати ДБЖ з потужністю:

$$P_{\text{ДБЖ}} = 20 \times 1.3 = 26 \text{ кВт}.$$

Час автономної роботи ДБЖ має визначати, скільки часу воно може забезпечувати живлення до автоматичного запуску резервного генератора. Час автономії залежить від потужності акумуляторних батарей та споживаної потужності.

Формула для розрахунку часу автономної роботи ДБЖ:

$$T_{aut} = \frac{E_{battery}}{P_{consumption}}, \tag{2.14}$$

де T_{aut} — час автономної роботи ДБЖ, год;

$E_{battery}$ — загальна ємність акумуляторів, кВт·год;

$P_{consumption}$ —потужність навантаження (споживання), кВт.

Припустимо, що ємність акумуляторних батарей складає 20 кВт·год, а споживана потужність серверної інфраструктури — 10 кВт. Тоді час автономної роботи ДБЖ складе:

$$T_{aut} = \frac{20 \times 1000}{10 \times 1000} = 2 \text{ години}$$

Для забезпечення безперебійної роботи на тривалий період (при довготривалих відключеннях електропостачання) необхідно використовувати резервний генератор, який може працювати протягом кількох годин або діб.

Для тривалих відключень, генератор має забезпечувати безперервне живлення на тривалий час. Враховуючи середнє споживання пального (наприклад, 8 л/год), можна розрахувати автономність роботи генератора.

Формула для розрахунку автономності роботи генератора:

$$T_{gen} = \frac{V_{fuel}}{C_{fuel}}, \quad (2.15)$$

де T_{gen} — автономність генератора (тривалість роботи без дозаправки), год;

V_{fuel} — об’єм пального в баку, л;

C_{fuel}— середнє споживання пального генератором, л/год.

Якщо в баку генератора 500 л пального, а споживання складає 8 л/год, то автономність генератора складе:

$$T_{gen} = \frac{500}{8} = 62.5 \text{ годин}$$

Вибір потужності ДБЖ та резервного генератора є критичним для забезпечення надійності та безперебійної роботи серверної інфраструктури. Правильний розрахунок потужності з урахуванням коефіцієнтів запасу та часу автономної роботи дозволяє мінімізувати вплив перебоїв електропостачання та забезпечити стійкість до довготривалих відключень.

У разі невизначеного або потенційно тривалого відключення електроенергії, особливо в умовах обмежених запасів пального для генератора, як це спостерігалося під час перших місяців повномасштабного вторгнення Російської Федерації в Україну, доцільно заздалегідь визначити пріоритетність живлення для кожної групи обладнання. Це дозволяє в разі потреби реалізовувати поетапне вимкнення менш критичних компонентів інфраструктури (наприклад, офісних робочих станцій, тестових серверів або систем відеонагляду), залишаючи енергоживлення для найважливіших елементів, таких як сервери баз даних, системи віртуалізації, маршрутизатори та SD-WAN-обладнання.

Такий підхід забезпечує раціональне використання енергетичних ресурсів та подовжує загальний час автономної роботи системи при обмежених ресурсах. Ці механізми можуть бути реалізовані як вручну, так і засобами автоматизації.

Доцільно розглядати включення таких рішень у середньострокову перспективу розвитку інфраструктури, зокрема, як частину побудови failover-механізмів, що будуть детальніше проаналізовані в розділі 2.6 "Інтеграція компонентів для забезпечення failover-механізмів".

У деяких випадках, коли відновлення електропостачання затягується на 24–48 годин, вимкнення частини навантаження є єдиним способом зберегти працездатність критичних систем.

У випадку віялових відключень, коли графік є відомим, рекомендовано одразу враховувати тривалість таких періодів при виборі ємності ДБЖ та генератора. Зокрема, генератор має бути здатним забезпечити живлення щонайменше на тривалість відключення згідно з графіком, із урахуванням часу на запуск, стабілізацію навантаження та можливу затримку з відновленням основного живлення.

2.4. Інтеграція компонентів для забезпечення failover-механізмів

Failover-механізми є ключовим елементом забезпечення надійності та безперервності функціонування серверної інфраструктури. Під терміном failover розуміється здатність системи автоматично перемикатися на резервний маршрут, обладнання або джерело живлення у випадку відмови основного компонента. Така функціональність є критично важливою в умовах, коли навіть короткочасне порушення зв’язку або живлення може призвести до значних втрат даних або зупинки бізнес-процесів.

У представленій інфраструктурі реалізовано багаторівневу архітектуру резервування, що охоплює як мережеві, так і енергетичні компоненти. Основним елементом зовнішнього мережевого доступу є три незалежні інтернет-провайдери, які підключені до кластеризованої пари маршрутизаторів FortiGate. Застосування кількох провайдерів значно підвищує доступність мережевих ресурсів, знижуючи ймовірність повної втрати зв’язку через несправність одного з каналів.

Для динамічного керування маршрутизацією та пріоритизації трафіку між провайдерами використовується технологія SD-WAN (Software-Defined Wide

Area Network), реалізована засобами Fortinet. SD-WAN дозволяє здійснювати інтелектуальний розподіл навантаження між каналами на основі таких параметрів, як затримка, втрата пакетів та пропускна здатність. Це забезпечує перевагу критично важливому трафіку (наприклад, IP-телефонії чи доступу до серверів), з одночасною оптимізацією використання мережевих ресурсів.

Зовнішнє резервування доповнено впровадженням каналу супутникового зв'язку Starlink, який є незалежним від наземної інфраструктури і здатен забезпечити мінімальний рівень доступності у надзвичайних ситуаціях.

Усі зовнішні канали передаються через кластер FortiGate з підтримкою режиму High Availability (HA). У разі відмови одного з маршрутизаторів, другий автоматично перебирає на себе функціонування без втрати стану з'єднань, що досягається завдяки синхронізації сесій між пристроями.

Далі інфраструктура передбачає два комутатори ядра (Core Switch), що з'єднані між собою за допомогою агрегації каналів згідно з протоколом LACP (Link Aggregation Control Protocol). Така агрегація дозволяє об'єднати кілька фізичних ліній у логічний інтерфейс, підвищуючи як пропускну здатність, так і стійкість до відмов.

Зв'язок між комутаторами, а також між ядром і рівнем доступу, реалізовано із застосуванням резервування каналів та портів. Сервери підключені за схемою dual-homing, тобто мають фізичні з'єднання з двома незалежними комутаторами, що забезпечує безперервність доступу у випадку відмови одного з них.

Передача даних усередині мережі логічно сегментована за допомогою VLAN (Virtual Local Area Network), що дозволяє ізолювати трафік окремих груп користувачів і сервісів, зменшити ризик широкомовних штормів та підвищити рівень безпеки.

Одним із ключових аспектів при проєктуванні відмовостійкої мережі є управління мережевими петлями, які можуть виникати у випадку неправильного налаштування з'єднань між компонентами. Мережеві петлі, особливо в комутаційних мережах, можуть призвести до серйозних проблем, таких як

перенавантаження мережі, збільшення часу передачі даних та втрата доступу до ресурсів.

У цій інфраструктурі було застосовано декілька методів для виключення можливості утворення мережевих петель:

1. LACP (Link Aggregation Control Protocol) між комутаторами забезпечує надійне управління з’єднаннями, що дозволяє кільком фізичним лініям функціонувати як один логічний канал без утворення петель. LACP допомагає автоматично визначати та обробляти надмірні або непотрібні з’єднання, що дозволяє запобігти утворенню циклічних з’єднань, які можуть викликати петлі.

2. Використання STP (Spanning Tree Protocol) на рівні комутаторів дозволяє визначати найоптимальніший шлях для передачі даних і відключати надлишкові з'єднання, якщо вони створюють замкнуті цикли. STP забезпечує безпечне управління мережею, автоматично блокуючи порти, що можуть спричиняти петлі, і залишаючи активними лише найбільш ефективні з’єднання.

3. Ієрархічна організація мережі також запобігає виникненню мережевих петель. Оскільки у цій інфраструктурі є чітке розподілення ролей між core-комутаторами, access-комутаторами та маршрутизаторами, мережа будується за принципом дерева з єдиним коренем. Кожен з компонентів має чітко визначену роль, і зв'язки між ними налаштовані так, що відсутні замкнуті цикли або можливості для їх утворення. Це забезпечує належне управління трафіком та запобігає зайвим маршрутам.

4. FortiGate в режимі HA також вносить свій вклад у запобігання утворенню петель. Всі з’єднання між FortiGate маршрутизаторами, а також з іншими компонентами, налаштовані так, щоб працювати в координації та автоматично перемикатися в разі відмови одного з елементів. Це дозволяє уникнути можливості циклічних з’єднань, адже маршрутизатори FortiGate використовують спеціалізовані механізми для оптимізації мережевого трафіку і підтримки лише необхідних з’єднань у разі збоїв.

Завдяки таким підходам, система не лише забезпечує високу доступність, але й повністю виключає можливість утворення мережевих петель, що є важливим аспектом для стабільної та ефективної роботи мережі в умовах високих навантажень і відмовостійкості. Всі компоненти, включаючи комутатори, маршрутизатори і інші елементи, взаємодіють між собою таким чином, що підтримують цілісність та стабільність мережі на всіх етапах її роботи.

Окрему увагу приділено системі енергетичного резервування. Усі критичні компоненти інфраструктури підключені до джерел безперебійного живлення (UPS), які забезпечують підтримку роботи протягом 10–15 хвилин після зникнення основного електроживлення. Протягом цього часу активується дизельний генератор, підключений до автоматичного вводу резерву (АВР), здатний автономно забезпечити живлення серверної кімнати. Потужність генератора (до 50 кВА) дозволяє підтримувати роботу не лише мережевого й серверного обладнання, але й систем охолодження.

У контексті довготривалих перебоїв електропостачання особливої ваги набуває задача пріоритезації навантажень для забезпечення стабільної роботи критично важливих компонентів серверної інфраструктури. В умовах обмеженого енергоресурсу, навіть за наявності дизельного генератора та UPS, необхідно здійснювати чітке розмежування між обладнанням, яке має залишатись активним, і тим, що може бути тимчасово відключене без суттєвого впливу на основні бізнес-процеси. З цією метою реалізовано систему пріоритезації навантажень, що функціонує на основі попередньо визначених сценаріїв та критеріїв важливості обладнання. Встановлено три рівні пріоритету:

Пріоритет 1 (високий): обладнання, необхідне для базового функціонування інфраструктури – маршрутизатори (FortiGate HA-кластер), Core-комутатори, сервери аутентифікації та маршрутизації, системи моніторингу та управління мережею, телекомунікаційне обладнання для підтримки зовнішнього зв’язку (у тому числі Starlink).

Пріоритет 2 (середній): сервери прикладного рівня, внутрішні сервіси доступу (файлові сховища, внутрішній портал), частина VLAN-комутаторів, які обслуговують другорядні підрозділи.

Пріоритет 3 (низький): допоміжне обладнання, системи відеоспостереження, друковані сервери, окремі модулі обробки великих обсягів даних або аналітики, які не є критичними у реальному часі.

Також може бути реалізовано політику резервного копіювання конфігурацій обладнання, що дасть змогу швидко відновити роботу мережі у випадку втрати або пошкодження програмних налаштувань.

Таким чином, завдяки інтеграції згаданих компонентів та технологій, інфраструктура набуває високого рівня відмовостійкості, що дає змогу забезпечити безперервність функціонування інформаційних сервісів навіть у разі комплексних збоїв мережевого чи енергетичного характеру.

2.5. Побудова комп’ютерної схеми серверної інфраструктури

Побудова комп’ютерної схеми серверної інфраструктури є практичним етапом дипломної роботи, що дозволяє відобразити проектовану архітектуру мережі у вигляді структурованої візуалізації. Такий підхід дає змогу не лише систематизувати взаємозв’язки між компонентами, а й заздалегідь виявити потенційні вузькі місця, забезпечити резервування, перевірити логіку маршрутизації та готуватися до подальшого впровадження. Для побудови схеми використано програмне середовище Microsoft Visio, яке забезпечує гнучкі можливості створення професійної мережевої топології.

До середовища було додатково імпортовано трафарети Fortinet (див. Рисунок 2.1), що дозволило працювати з актуальними іконками для маршрутизаторів, міжмережевих екранів та іншого обладнання цього виробника. Використовуючи імпортовані трафатери та можливості Microsoft Visio було створено схему, що зображена на рисунку 2.2.

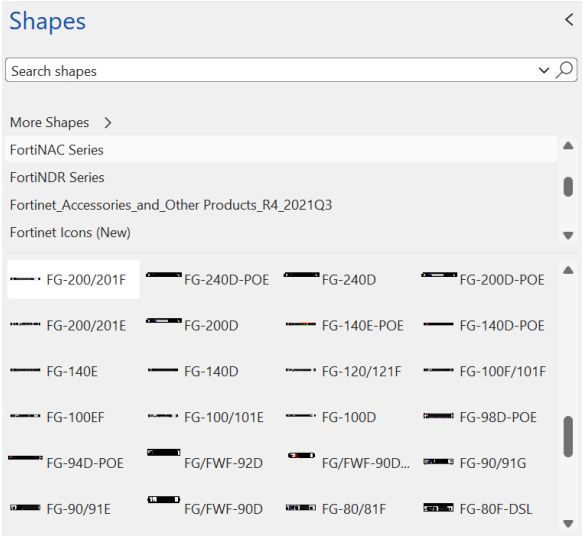


Рисунок 2.1 – скріншот імпортованих трафаретів Fortinet.

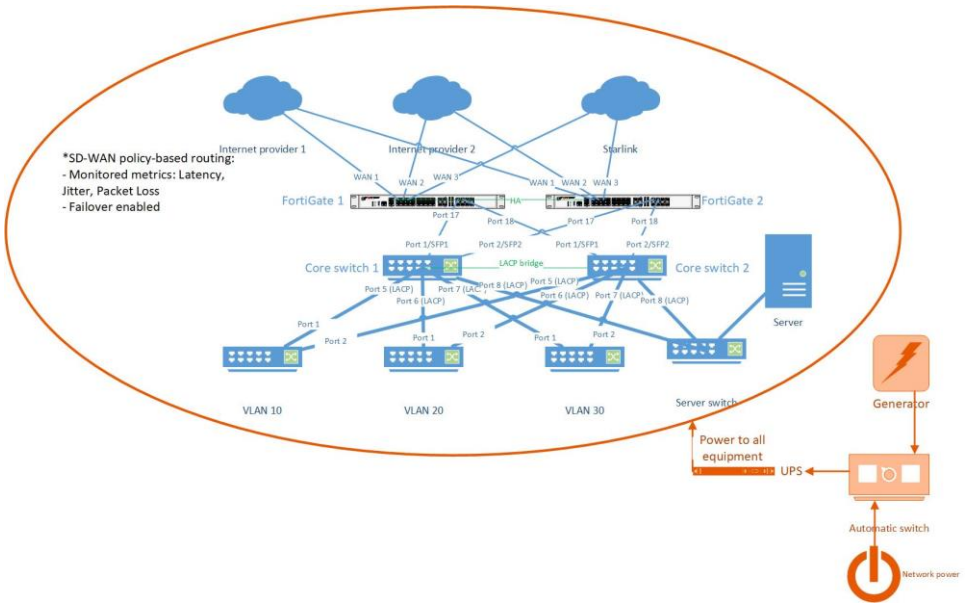


Рисунок 2.2 – Візуалізована схема серверної інфраструктури.

На схемі (див. Рисунок 2.2) першим компонентом є сегмент інтернет-з’єднання, який включає три незалежні джерела доступу до мережі:

- Два провайдери із дротовим з’єднанням;
- Один резервний канал через супутниковий зв’язок Starlink.

Кожен з цих каналів під’єднано до двох FortiGate-маршрутизаторів, що працюють у режимі високої доступності (High Availability). До кожного маршрутизатора додано відповідні підписи та вказано використовувані порти —

Port17 та Port18. Таке резервування забезпечує відмовостійкість та безперервність сервісів у разі відмови одного з елементів.

Нижче по схемі розташовано два Core-комутатори, які відіграють роль центрального вузла комутації з підключеннями до обох маршрутизаторів через порти SFP1 та SFP2, що забезпечує балансування трафіку.

Від Core-комутаторів йде мультиканальне з'єднання (за технологією LACP) до чотирьох VLAN-комутаторів, які розподіляють мережу на окремі сегменти. Кожен з цих комутаторів відповідає за окремий логічний сегмент: VLAN10, VLAN20, VLAN30 і Server VLAN. Для реалізації LACP використано порти Port5–Port8, по два на кожен комутатор доступу.

У нижній частині схеми розміщено основний сервер, підключений до VLAN-комутатора серверного сегменту. Підключення здійснене за принципом dual-homing — сервер має два мережевих інтерфейси, кожен з яких веде до окремого комутатора, що забезпечує повну резервованість на рівні доступу.

Особливу увагу приділено електроживленню (див. Рисунок 2.2). У правому нижньому куті схеми зображено систему UPS (джерела безперебійного живлення), до яких підключені всі критично важливі компоненти (маршрутизатори, комутатори, сервери).

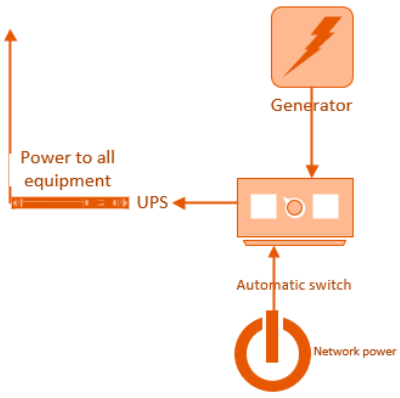


Рисунок 2.2 – схематичне зображення подання електроенергії до обладнання серверної інфраструктури.

Також на схемі розміщено генератор, що підключений через автоматичний ввід резерву (АВР). При зникненні основного електропостачання, АВР активує генератор, який забезпечує живлення UPS, а ті — вже передають електроенергію до мережевого обладнання. Така послідовність гарантує безперервність функціонування інфраструктури навіть у разі тривалих аварій.

Схема побудована із застосуванням стандартних умовних графічних символів, прийнятих у мережевому адмініструванні. Для кожного елемента:

- Вказано назву пристрою, його функціональне призначення;
- Використано колірну індикацію для підкреслення логічної структури;
- Додано примітки щодо конфігурації портів, режимів роботи тощо.

Крім основної схеми, що демонструє повнофункціональну архітектуру мережі, було також розроблено альтернативний варіант візуалізації з реалізацією пріоритезації обладнання відповідно до рівня його критичності у випадку довготривалих відключень електроенергії. Такий підхід дозволяє забезпечити гнучке керування навантаженням на джерела резервного живлення, подовжити час автономної роботи та зберегти працездатність ключових сервісів у надзвичайних ситуаціях, зокрема подібних до тих, що спостерігались у перші місяці повномасштабного вторгнення Російської Федерації в Україну.

У межах цієї схеми було впроваджено трирівневу систему пріоритетів:

Пріоритет 1 — критично важливе обладнання, безперебійне функціонування якого є необхідною умовою підтримки базових сервісів інфраструктури. До цієї категорії віднесено: один з міжмережевих екранів FortiGate (що забезпечує маршрутизацію трафіку та фільтрацію); один Core-комутатор (центральна точка комутації даних); комутатор VLAN30 (сегмент управління); комутатор Server VLAN; основний сервер.

Окрім того, до пріоритету 1 віднесено систему UPS, генератор та відповідний комутатор живлення, оскільки саме ці елементи забезпечують розподіл та стабільне електроживлення всієї інфраструктури. Їх безперервна робота має бути гарантована в будь-якому сценарії.

Пріоритет 2 — важливі, але не критичні сегменти, які забезпечують роботу користувацьких мереж. Це VLAN10 та VLAN20, які можуть бути тимчасово відключені для зменшення споживання енергії, зберігаючи при цьому основну функціональність серверної інфраструктури.

Пріоритет 3 — резервні компоненти, необхідні для забезпечення повної відмовостійкості за нормальних умов, але які можуть бути тимчасово виведені з експлуатації під час енергетичної кризи. До цієї категорії належать другий маршрутизатор FortiGate та другий Core-комутатор.

Що стосується інтернет-провайдерів, то кожен фізично підключений до обох FortiGate-маршрутизаторів. В звичний умовах обидва використовуються для балансування навантаження та резервування, однак у разі вимкнення одного з маршрутизаторів — автоматично активується перенаправлення трафіку через доступний канал, що знижує ризик втрати з’єднання з глобальною мережею.

Впровадження подібної схеми з ієрархією живлення дозволяє адаптуватися до сценаріїв обмеженої доступності електроенергії, зберігаючи працездатність критичних компонентів, мінімізуючи час простою та покращуючи загальну стійкість інфраструктури до зовнішніх впливів.

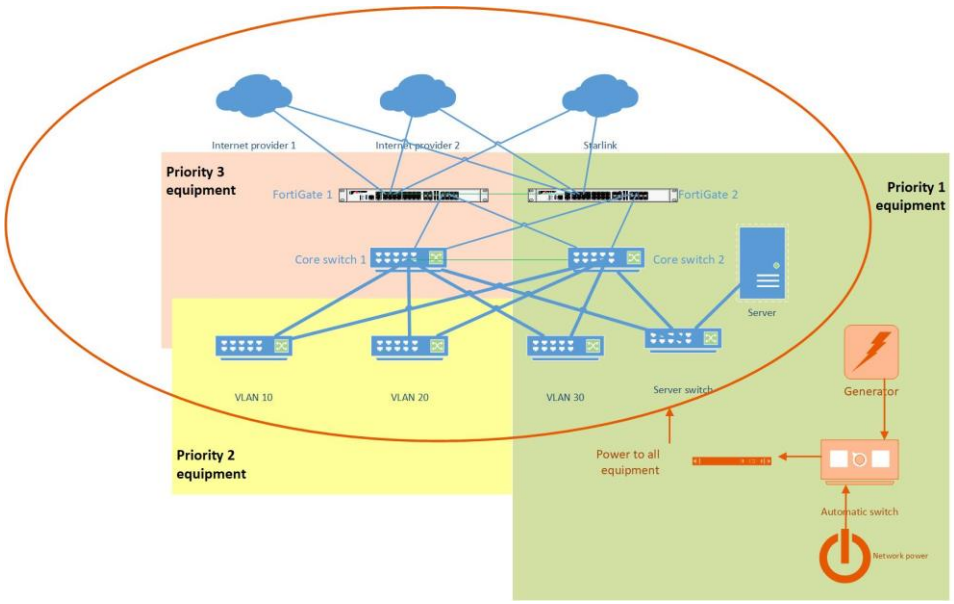


Рисунок 2.4 – Візуалізована схема серверної інфраструктури з пріорітезацією обладнання.

Висновки за розділом 2

У другому розділі було виконано комплексне проектування серверної інфраструктури з орієнтацією на забезпечення високої надійності, масштабованості та відмовостійкості системи. Обґрунтовано вибір інструментів проектування (Microsoft Visio, трафарети Fortinet) та технічних рішень, зокрема застосування архітектури з SD-WAN, резервуванням інтернет-каналів, використанням комутаторів із підтримкою LACP та організацією логічних сегментів через VLAN.

Побудована мережна схема чітко демонструє взаємозв’язки між усіма елементами інфраструктури: від інтернет-провайдерів до серверів і систем електроживлення. Особливу увагу приділено реалізації принципів fault tolerance — впроваджено подвійну маршрутизацію, комутацію, резервування живлення через UPS і генератор, dual-homing для серверів, а також організовано багаторівневу систему пріоритезації обладнання на випадок довготривалих енергетичних відключень.

Таким чином, розроблена інфраструктура відповідає сучасним вимогам до корпоративних систем і враховує актуальні ризики, зокрема пов’язані з воєнним станом та енергетичною нестабільністю. Створена візуальна модель може бути використана як основа для реалізації фізичної мережі та подальшого розгортання IT-сервісів.

РОЗДІЛ 3.
АНАЛІЗ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

3.1. Верифікація архітектури з урахуванням вимог (availability, scalability, performance)

Після побудови архітектурної моделі серверної інфраструктури було проведено верифікацію відповідності проєктного рішення ключовим нефункціональним вимогам: доступності (availability), масштабованості (scalability) та продуктивності (performance). Верифікація здійснювалась шляхом аналізу топології, характеристик обладнання, механізмів резервування, а також потенційної поведінки системи в умовах пікових навантажень або часткової відмови компонентів.

3.1.1. Доступність (Availability)

Одним із основних критеріїв при проектуванні серверної інфраструктури для підтримки критичних бізнес-процесів є забезпечення високої доступності. Висока доступність передбачає безперервну роботу інфраструктури при мінімальних порушеннях, незалежно від внутрішніх або зовнішніх збоїв, таких як відмова обладнання або відключення енергопостачання. У зв'язку з цим, система повинна мати вбудовані механізми резервування, які автоматично компенсують відмови, забезпечуючи безперервний доступ до сервісів і ресурсів. Моделювання архітектури високої доступності для цієї серверної інфраструктури базується на впровадженні кількох ключових технологій та принципів.

Одним із важливих аспектів забезпечення високої доступності є маршрутизація трафіку через кілька незалежних каналів, що дозволяє автоматично перемикатися на резервні канали у разі відмови основного з'єднання. Для досягнення цієї мети застосовано технологію SD-WAN (Software-Defined Wide Area Network), яка дозволяє не тільки моніторити стан кожного каналу, але й оптимізувати вибір маршруту для передачі даних.

В даному випадку, використовуються два маршрутизатори FortiGate, що працюють у режимі High Availability (HA), підключені до трьох незалежних інтернет-провайдерів. У разі збоїв одного з провайдерів або зниження якості з’єднання, маршрутизатори автоматично перемикаються на інший канал. Цей процес здійснюється без втрати сесії, що забезпечує неперервність з'єднання для критичних додатків, таких як IP-телефонія або фінансові транзакції. Таким чином, SD-WAN забезпечує надійне управління трафіком через кілька каналів і дозволяє підтримувати стабільний рівень доступності при мінімальних збоїв.

Безперервність живлення є критично важливим аспектом для будь-якої серверної інфраструктури, що обслуговує критичні сервіси. Для цього в архітектурі реалізовано систему резервування енергопостачання, що включає джерела безперебійного живлення (UPS) та дизельний генератор.

UPS забезпечує короткочасне резервне живлення для серверів і мережевого обладнання на період до 10–15 хвилин, що дає можливість розпочати автоматичний запуск дизельного генератора, який забезпечить роботу інфраструктури протягом тривалого часу у разі тривалої відсутності основного живлення. Цей підхід гарантує, що навіть у разі повного відключення зовнішнього електроживлення, всі критичні компоненти інфраструктури продовжать працювати без перерв, запобігаючи втратам даних або простою системи.

Для забезпечення відмовостійкості мережі та запобігання вузьким місцям у передачі даних, використовуються технології агрегації ліній на рівні комутаторів. У цій інфраструктурі застосовується LACP (Link Aggregation Control Protocol), який дозволяє об’єднувати кілька фізичних з’єднань між core-комутаторами та access-комутаторами в єдиний логічний канал.

Це не тільки збільшує пропускну здатність між ключовими елементами мережі, але й забезпечує автоматичне резервування каналів. У разі відмови одного з ліній з'єднання, протокол LACP дозволяє перерозподілити трафік через інші активні канали, не порушуючи зв’язок між пристроями. Завдяки такому підходу вдається уникнути ефекту вузьких місць, коли один канал не може

обробити весь трафік, що може призвести до затримок або відмов у роботі сервісів.

Одним із найбільш ефективних способів забезпечення відмовостійкості є фізичне дублювання ключових компонентів інфраструктури. Це досягається через реалізацію схеми dual-homing, що передбачає підключення кожного критичного компонента (наприклад, серверів та комутаторів) до двох незалежних інтерфейсів або комутаторів.

Таким чином, навіть якщо один з інтерфейсів або комутаторів виходить з ладу, інший інтерфейс або комутатор автоматично приймає на себе навантаження без переривання роботи. Це забезпечує безперервність доступу до сервісів та даних і є важливим кроком до забезпечення високої доступності інфраструктури.

3.1.2. Масштабованість (Scalability)

Інфраструктура передбачає як вертикальну, так і горизонтальну масштабованість:

1. Усі ключові мережеві компоненти мають запас по портам і продуктивності, що дозволяє додавати нові сегменти без заміни обладнання;
2. Впровадження VLAN-сегментації дозволяє логічно масштабувати користувацькі групи, сервіси та політики доступу без фізичних змін у мережі;
3. Серверна інфраструктура допускає розширення обчислювальних потужностей через додавання нових серверів до наявної стійки (rack);
4. Використання модульних UPS-рішень (як перспектива розвитку) забезпечить гнучке масштабування резервного живлення відповідно до зростання навантаження.

Таким чином, поточне проєктне рішення забезпечує передумови для безперешкодного розширення інфраструктури на найближчий горизонт планування (3–5 років) без суттєвих капітальних витрат.

3.1.3. Продуктивність (Performance)

Продуктивність оцінювалася через характеристики каналів зв’язку, обчислювальних ресурсів, а також можливість підтримки необхідної якості обслуговування:

- Канали LACP між core та access-комутаторами забезпечують агреговану пропускну здатність, що перевищує пікове навантаження у робочі години;
- Впровадження QoS (як рекомендоване вдосконалення) дозволить диференціювати трафік і пріоритезувати критичні сервіси (VoIP, відеоконференції, доступ до БД);
- Сервери з підтримкою віртуалізації дозволяють оптимізувати використання ресурсів шляхом динамічного розподілу навантаження між віртуальними машинами;
- Моніторинг та логування (через FortiAnalyzer або подібні інструменти) дозволяють оперативно виявляти аномалії, оптимізуючи продуктивність у реальному часі.

Таким чином, результати верифікації свідчать про відповідність змодельованої архітектури цільовим показникам доступності, масштабованості та продуктивності.

3.2. Визначення слабких місць та порівняльний аналіз

У процесі моделювання серверної інфраструктури було виявлено низку потенційних вразливостей, які можуть негативно впливати на стабільність та відмовостійкість системи. Основним компонентом, що викликає занепокоєння, є механізм маршрутизації та балансування трафіку на базі Fortinet SD-WAN. Незважаючи на його здатність ефективно розподіляти навантаження між провайдерами, у разі програмного або апаратного збою даної функціональності спостерігається ризик виникнення затримок при перемиканні каналів або навіть короткочасного розриву з’єднання. З огляду на відсутність окремого механізму аварійної маршрутизації, ця вразливість може призвести до недоступності критичних сервісів на час відновлення роботи.

Іншим аспектом, що потребує уваги, є використання супутникового зв’язку Starlink як одного з резервних каналів доступу до Інтернету. Хоча така технологія забезпечує незалежність від місцевої інфраструктури, її стабільність залежить від погодних умов, зокрема опадів та хмарності. Це, у свою чергу, спричиняє флуктуації у затримці пакетів, що критично для сервісів реального часу, таких як голосовий зв’язок (VoIP) або віддалене адміністрування серверів. В умовах несприятливої погоди можуть спостерігатися втрати пакетів, що впливатиме на якість обслуговування кінцевих користувачів.

Ще одне слабке місце пов’язане з реалізацією логічної сегментації мережі засобами VLAN. У разі інтенсивного трафіку у межах VLAN 10, що обслуговує офісні комп’ютери, без впровадження механізмів QoS (Quality of Service) існує ймовірність перевантаження каналу та погіршення продуктивності для інших сегментів. Додатково, гостьовий Wi-Fi, реалізований у VLAN 40, може становити загрозу інформаційній безпеці у випадку недостатньої ізоляції клієнтів або помилок у налаштуваннях доступу.

У сфері енергозабезпечення було виявлено потенційний ризик, пов’язаний із затримкою запуску дизельного генератора. Хоча наявність UPS дозволяє забезпечити короткочасне живлення, у випадку нестабільної роботи перемикача або затримки в активації генератора критичні системи можуть залишитися без електропостачання. Потужність генератора, що становить 40–50 кВА, наразі покриває потреби інфраструктури, однак у разі розширення серверного середовища вона може виявитися недостатньою. Відповідно, планування масштабування повинно супроводжуватись переоцінкою параметрів резервного живлення.

Для поглибленого аналізу було здійснено порівняння змодельованої інфраструктури з альтернативними підходами за ключовими технічними параметрами. Зокрема, можливим варіантом удосконалення є відмова від SD-WAN на користь маршрутизаторів із підтримкою OSPF або BGP. OSPF забезпечує адаптивність до змін топології та швидке відновлення маршрутів, однак не передбачає гнучкого розподілу навантаження між зовнішніми

каналами. BGP, у свою чергу, дозволяє реалізувати повноцінне резервування шляхом паралельного підключення до кількох провайдерів, проте його конфігурація є складнішою та вимагає ручного управління політиками.

У якості альтернативи Starlink запропоновано підключення до третього кабельного інтернет-провайдера або використання LTE-зв’язку. Перший варіант покращує стабільність, але залежить від фізичної доступності оператора, другий — підвищує мобільність, однак обмежений швидкістю і пропускною здатністю у пікові години. Щодо сегментації трафіку, більш радикальним підходом є заміна логічного поділу VLAN на фізичну сегментацію мережі, що забезпечує вищий рівень безпеки, але потребує значно більших ресурсів та ускладнює керування.

У контексті енергозабезпечення порівнювалися традиційна конфігурація з одним генератором із сценарієм використання двох менших за потужністю джерел живлення. Останній забезпечує вищу відмовостійкість і гнучкість у балансуванні навантаження, але вимагає ускладненого керування та резервного перемикання. Додатково було розглянуто впровадження модульних UPS-рішень, які дозволяють масштабувати автономну потужність відповідно до зростаючих потреб, підвищуючи надійність системи.

Ще одним слабким місцем змодельованої інфраструктури є механізм відключення другорядного обладнання у випадку довготривалих відключень електропостачання. Хоча в рамках технічного проєкту визначено пріоритетність компонентів інфраструктури та сформовано черговість їх відключення для зменшення навантаження на резервні джерела живлення (UPS і генератор), на поточному етапі ці операції передбачено здійснювати вручну.

Відсутність автоматизованої системи управління навантаженням призводить до залежності від наявності кваліфікованого персоналу на об’єкті у момент виникнення аварійної ситуації. У разі його відсутності або затримки з прийняттям рішень, існує ризик несвоєчасного або помилкового відключення, що може спричинити припинення роботи критично важливих сервісів або порушення логіки функціонування мережевих протоколів.

Крім того, ручне втручання потребує точного дотримання інструкцій щодо порядку дій, що не виключає впливу людського фактору, зокрема помилок у визначенні пріоритетів або фізичному виконанні перемикань. У майбутніх роботах доцільно розглянути можливість впровадження часткової або повної автоматизації процесу відключення, зокрема шляхом:

- використання інтелектуальних модулів керування живленням (PDU) із дистанційним доступом;
- розробки сценаріїв на базі NMS/BMS для автоматичного реагування на зміну рівня заряду UPS або навантаження на генератор;
- впровадження систем оповіщення для пришвидшення ручного втручання у разі аварійної ситуації.

Окремої уваги потребує також візуальна схема серверної інфраструктури, яка хоч і відображає основні логічні та фізичні компоненти системи, однак має низку обмежень, що можуть ускладнити її практичне використання для оперативного прийняття рішень або подальшого розширення мережі:

- Обмежена деталізація рівнів VLAN — схема не відображає чітке логічне розділення трафіку між сегментами (офісний, гостьовий, серверний), що ускладнює розуміння маршрутизації всередині інфраструктури й може стати причиною помилок під час оновлень або усунення несправностей.

- Відсутність позначення маршрутів резервування трафіку — хоча в моделі реалізовано багатоканальний доступ до Інтернету, схема не містить умовних позначень або стрілок, які демонструють порядок перемикання каналів або пріоритетність маршрутів, що знижує її інформативність у контексті SD-WAN.

- Непозначене джерело управління енергоживленням — блоки UPS та генератора зображено спрощено, без конкретизації їхньої інтеграції з автоматикою або відсутності систем моніторингу, що може призвести до недооцінки ролі цих компонентів у відмовостійкості системи.

- Недостатня візуалізація резервних зв’язків між комутаторами — при реалізації LACP-агрегацій між ядром і доступними комутаторами не вказано

активні/пасивні лінії, що створює складнощі для інтерпретації топології та її подальшого обслуговування.

Узагальнюючи, змодельована серверна інфраструктура демонструє адекватний рівень відмовостійкості та продуктивності відповідно до поточних вимог. Однак для підвищення її довгострокової стабільності доцільно розглядати впровадження окремих елементів з альтернативних рішень, особливо у сферах маршрутизації, резервування каналів зв'язку та живлення. Також незважаючи на наявність логіки пріоритезації навантажень, відсутність засобів її автоматизованого застосування наразі є вразливістю, що потенційно знижує рівень відмовостійкості системи в умовах довготривалої відсутності основного живлення. Такий підхід дозволить мінімізувати ризики збоїв та адаптувати інфраструктуру до змін у масштабах і профілі навантаження.

3.3. Оцінка масштабованості та перспектив розвитку системи

Масштабованість проєктованої серверної інфраструктури є одним із ключових чинників її довготривалої ефективності та адаптивності до змін у кількості користувачів, обсягах трафіку та функціональних потребах організації. Виходячи з поточних архітектурних рішень, система демонструє задовільний рівень масштабованості, однак існують аспекти, які потребують детального аналізу та потенційного вдосконалення у майбутньому.

Зокрема, мережева архітектура із застосуванням core switch та логічної сегментації на базі VLAN дозволяє розширювати кількість сегментів без значних змін у фізичній топології. Проте за збільшення навантаження з боку активних користувачів або впровадження додаткових сервісів (наприклад, систем відеоспостереження чи VoIP-телефонії), може знадобитися оптимізація політик QoS та збільшення пропускної здатності міжмережевих з'єднань.

У сфері серверного обладнання передбачено можливість підключення додаткових серверів завдяки резервним портам на комутаторах, а також реалізованій системі dual-homing. Це забезпечує балансування навантаження та високу доступність ресурсів. Тим не менш, із часом може виникнути потреба у розгортанні віртуалізованих середовищ або хмарних компонентів, що

передбачає інтеграцію з зовнішніми обчислювальними ресурсами (гібридна інфраструктура).

Щодо інтернет-зв’язку, наразі використовується мультиканальне підключення із балансуванням на базі SD-WAN, що дозволяє гнучко керувати зовнішнім трафіком. Для підвищення надійності та масштабованості в майбутньому доцільно розглянути впровадження додаткових кабельних підключень або використання незалежних мобільних технологій (5G/LTE). Це дозволить розширити діапазон доступності сервісів у разі відмови окремих провайдерів.

У контексті енергозабезпечення, поточне рішення на основі одного дизельного генератора з UPS забезпечує базовий рівень автономності. Проте за збільшення навантаження (наприклад, впровадження нових серверних модулів або систем кондиціонування) необхідно передбачити перехід до модульних UPS-систем або впровадження двох генераторів меншої потужності з автоматичним перемиканням. Це підвищить надійність і дозволить гнучко керувати споживанням енергії.

Крім того, у перспективі доцільним є впровадження автоматизованих засобів керування електроживленням, зокрема інтелектуальних модулів PDU (Power Distribution Unit) з підтримкою віддаленого доступу. Такі пристрої дозволять централізовано контролювати споживання енергії, здійснювати пріоритетне вимкнення другорядного обладнання під час критичних ситуацій та зменшити залежність від людського фактору у процесі аварійного перемикання. Загалом, автоматизація реагування на критичні події є важливим напрямом розвитку: інтеграція з BMS (Building Management System) або NMS (Network Management System), впровадження сценаріїв дій у разі падіння рівня заряду UPS або перевантаження генератора, а також реалізація протоколів оповіщення відповідального персоналу значно підвищать відмовостійкість інфраструктури.

З точки зору інформаційної безпеки, важливо враховувати необхідність впровадження централізованої системи моніторингу подій (SIEM), а також розширення політик доступу у разі зростання кількості користувачів і

підключень. Такі заходи є критичними у разі масштабування системи до рівня кількох офісів або філій.

Щодо візуального сприйняття, одним із можливих напрямків подальшого розвитку є переведення візуальної моделі в симуляційне середовище, яке дозволить не лише візуалізувати логіку роботи мережі, але й проводити тестування сценаріїв аварій, змін конфігурації та навантаження. Таке рішення дасть змогу виявляти критичні вузькі місця ще на етапі проєктування та підвищити достовірність оцінки ефективності прийнятих технічних рішень. Таке вдосконалення дозволить покращити не лише читабельність моделі, а й практичну користь для обслуговуючого персоналу та майбутніх інтеграторів.

Підсумовуючи, проєктована інфраструктура має достатній потенціал для поступового масштабування та вдосконалення. Подальший розвиток системи можливий шляхом:

- інтеграції з хмарними платформами для підвищення гнучкості в обчисленнях;
- впровадження резервних каналів зв’язку з використанням мобільного або супутникового зв’язку нового покоління;
- модернізації енергетичних рішень через використання модульних та відмовостійких джерел живлення;
- автоматизації процесів керування живленням та пріоритезації навантаження через інтелектуальні PDU та BMS/NMS-сценарії;
- автоматизації керування мережею через централізовані засоби моніторингу та управління;
- переходу до повнофункціонального резервування маршрутизації за допомогою протоколів OSPF/BGP;
- переведення візуальної моделі в симуляційне середовище.

Такі кроки дозволять адаптувати інфраструктуру до нових викликів та забезпечити її стабільну роботу в умовах змін технологічного середовища.

Висновки за розділом 3

Проведена верифікація підтвердила, що запропонована серверна інфраструктура відповідає основним вимогам високої доступності, масштабованості та продуктивності. Використання SD-WAN із FortiGate у режимі High Availability, агрегація ліній через LACP, а також система живлення з UPS і генератором забезпечують безперервну роботу навіть при збої обладнання чи мережі.

Водночас виявлено потенційні ризики, зокрема можливі затримки у роботі SD-WAN, залежність від погодних умов супутникового каналу Starlink та відсутність автоматизації управління живленням при довготривалих відключеннях. Також існує ризик перевантаження VLAN і загрози безпеці через гостьовий Wi-Fi.

Для підвищення надійності в майбутньому можливо впровадити альтернативні маршрути, автоматизацію керування живленням і покращену сегментацію мережі. Це дозволить забезпечити стабільну роботу системи та підготувати її до збільшення навантажень і аварійних ситуацій.

ВИСНОВКИ

У процесі дослідження було проаналізовано серверну інфраструктуру корпоративного сектору, яка функціонує в умовах нестабільного інтернет-з'єднання та електропостачання. Враховуючи сучасні загрози, особливу увагу було приділено методам забезпечення надійності та відмовостійкості мережевих і серверних систем.

Було розглянуто три ключові аспекти: резервне живлення, механізми failover та оптимізація мережевої доступності. Для кожного з цих напрямків було змодельовано рішення, які дозволяють мінімізувати вплив зовнішніх чинників на стабільність роботи серверів.

Було розроблено архітектуру мережі, яка складається з двох основних маршрутизаторів FortiGate, двох Core-комутаторів, чотирьох VLAN-комутаторів (із застосуванням LACP), кількох виділених VLAN (для офісної мережі, серверів, гостьового доступу тощо), а також серверів, підключених до окремого VLAN. Живлення інфраструктури забезпечується через систему UPS з автоматичним перемиканням на дизельний генератор. Передбачено підключення до трьох інтернет-провайдерів, включаючи супутниковий канал Starlink.

Забезпечення резервного живлення є критичним фактором для підтримки безперервності роботи серверної інфраструктури. Було змодельовано систему резервного електропостачання, що включає комбінацію UPS і дизельного генератора, здатну забезпечити автономну роботу серверного обладнання у разі тривалих відключень електроенергії. Проте було виявлено, що UPS забезпечує короткочасне резервування, а генератор потужністю 40–50 кВА може стати недостатнім у разі підвищеного навантаження або несправностей.

Для забезпечення безперервності роботи серверних систем у разі відмови основного обладнання було впроваджено систему failover-механізмів. Використання Fortinet SD-WAN дозволило організувати автоматичне перемикання між інтернет-каналами залежно від параметрів latency, jitter та packet loss. Це значно зменшило ризики втрати з'єднання. Проте виявлено

потенційні затримки при перемиканні між каналами у разі збою SD-WAN. Крім того, резервний зв’язок через Starlink хоч і забезпечує додаткову надійність, однак має нестабільні показники latency, що може негативно впливати на VoIP-зв’язок та інші критично важливі сервіси.

Було реалізовано через VLAN-сегментацію та балансування навантаження між комутаторами та маршрутизаторами. Було створено декілька VLAN для розділення трафіку між офісними пристроями, серверами, периферійними пристроями та гостьовими користувачами. Таке рішення дозволило підвищити безпеку мережі та мінімізувати ризики перевантаження окремих сегментів. Проте було виявлено, що у разі високого навантаження на VLAN 10 (офісні комп’ютери) можливе перевантаження основного каналу зв’язку, якщо не застосовано механізми QoS. Крім того, гостьовий Wi-Fi (VLAN 40) може створювати потенційні загрози безпеці без належної ізоляції користувачів та обмеження трафіку.

Також було розроблено додаткову схему з пріоритетами та передбачено, що частина обладнання може бути відключена для зменшення енергоспоживання в умовах обмеженого резервного живлення або у разі відсутності необхідності в роботі певних сервісів, що підвищує загальну гнучкість системи.

Загальний аналіз змодельованої серверної інфраструктури продемонстрував її високу ефективність у забезпеченні стабільності роботи корпоративних сервісів. Реалізовані рішення щодо резервного живлення, балансування трафіку та мережевої сегментації значно зменшили ризики відмови та втрати з'єднання. Проте було виявлено ряд слабких місць, які потребують подальшого вдосконалення.

Для підвищення надійності серверної інфраструктури рекомендовано додати альтернативні механізми аварійного маршрутизаційного резервування, наприклад, використання резервних тунелів VPN або інтеграцію з іншими SD-WAN-рішеннями (Cisco, Palo Alto Networks). Також доцільно розглянути альтернативні резервні канали зв’язку, такі як 5G-з'єднання з агрегуванням

каналів, що дозволить підвищити стабільність інтернет-з'єднання у критичних ситуаціях.

У сфері енергозабезпечення можливе впровадження додаткового рівня резервування, наприклад, використання акумуляторних батарей з довшим терміном автономної роботи або збільшення потужності генератора. Оптимізація VLAN-сегментації можлива шляхом застосування QoS для гарантування стабільного рівня продуктивності критичних сервісів. Для підвищення безпеки гостьового Wi-Fi варто впровадити додаткові рівні аутентифікації та ізоляцію користувачів.

Враховуючи особливу актуальність питання стійкості серверних інфраструктур через військові дії та постійні кібератаки, результати даного дослідження мають важливе значення для українських підприємств та державних установ. Подальші дослідження можуть включати тестування нових методів забезпечення безперебійної роботи серверних систем у реальних умовах експлуатації, що дозволить створити ще більш стійку та продуктивну серверну інфраструктуру для корпоративного сектору.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Singla R., Srinivasa S., Reddy N., Pedersen J. M., Vasilomanolakis E., Bettati R. An Analysis of War Impact on Ukrainian Critical Infrastructure Through Network Measurements // Proceedings of the International Conference on Traffic Monitoring and Analysis (TMA), 26–29 June 2023, Naples, Italy. – IEEE, 2023.

2. Bogusław Pacek, Piotr Pacek. Russia’s devastating impact on critical infrastructure during the hybrid war in Ukraine. BEZPIECZEŃSTWO. SECURITY. THEORY AND PRACTICE, No. 2 (LI), 2023. – 23 c.

3. Резолюція Генеральної Асамблеї ООН ES-11/2 [Електронний ресурс]. – режим доступу: URL: https://uk.wikipedia.org/wiki/Резолюція_Генеральної_Асамблеї_ООН_ES-11/2 (дата звернення – 12.05.2025).

4. Статистика бази даних воєнних злочинів T4P [Електронний ресурс]. – режим доступу: URL: https://t4pua.org/stats (дата звернення – 12.05.2025).

5. Присяжнюк Н. Кібервійна в Україні – інфографіка кібератак за 2022–24 роки. Які країни проводять найбільше політизованих кібератак у світі: Україна увійшла до п'ятірки // LIGA.net [Електронний ресурс]. – 28.02.2024. – режим доступу: URL: https://tech.liga.net/ua/other/article/yaki-krainy-provodiat-naibilshe-polityzovanykh-kiberatak-u-sviti-ukraina-uviishla-do-piatirky (дата звернення – 12.05.2025).

6. Ukagwu K., Kapalata P., Eze V. Automated Power Source Selection System for Uninterrupted Supply: Integration of Main Power, Solar Energy, and Generator Power [Електронний ресурс] // Journal of Engineering. – 13.05.2024. – Режим доступу: https://pdfs.semanticscholar.org/f89f/1aac971bb57b26f7fa8c5050989018e0ba27.pdf (дата звернення – 23.05.2025).

7. Баранов Ю. О., Косминський І. В., Мельниченко М. С., Вініченко В. О. Обґрунтування вибору дизель-генераторів за питомою потужністю в будівельній галузі // Техніка будівництва. – 2020. – № 36. – С. 73–82. –

[Електронний ресурс]. – режим доступу: URL: http://tehbud.knuba.edu.ua/article/view/205351 (дата звернення – 12.05.2025).

8. Нестерова К. С., Бринзило А. В. Управління впровадженням інноваційних технологій резервного живлення у діяльність торговельно-розважального центру // Економічний вісник НТУУ «КПІ». – 2024. – № 31. – [Електронний ресурс]. – Режим доступу: https://doi.org/10.20535/2307-5651.31.2024.319022 (дата звернення – 12.05.2025).

9. Kuzminykh I. Failover and load sharing in SIP-based IP telephony // Proceedings of the 2008 International Conference on “Modern Problems of Radio Engineering, Telecommunications and Computer Science” (TCSET), 19–23 лютого 2008 р., Львів, Україна. – Lviv: IEEE, 2008. – [Електронний ресурс]. – Режим доступу: https://ieeexplore.ieee.org/document/5445924 (дата звернення – 12.05.2025).

10. Özsu M. Tamer, Valduriez P. Data Replication // Principles of Distributed Database Systems. – 3rd ed. – New York: Springer, 2011. – С. 459–495. – [Електронний ресурс]. – Режим доступу: https://link.springer.com/chapter/10.1007/978-1-4419-8834-8_13 (дата звернення – 12.05.2025).

11. Yang Z., Cui Y., Li B., Liu Y., Xu Y. Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities // Proceedings of the 28th International Conference on Computer Communication and Networks (ICCCN). – 2019. – [Електронний ресурс]. – Режим доступу: https://doi.org/10.1109/ICCCN.2019.8847124 (дата звернення – 12.05.2025).

12. Wellyandi G. Implementation of Load Balancing and Failover Network Using Fortinet SDWAN Technology at PT. Lintasarta // Ceddi Journal of Information System and Technology (JST). – 2022. – Т. 1, № 2. – С. 8-13.

13. Fortinet. FortiGate / FortiOS 7.0.0 SD-WAN / SD-Branch Concept Guide: Introduction [Електронний ресурс] / Fortinet. – Режим доступу: https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan-sd-branch-concept-guide/336354/introduction (дата звернення: 12.05.2025).

14. Grandstream. VLAN Guide [Електронний ресурс] / Grandstream. – Оновлено 2 листопада 2023 р. – Режим доступу: https://documentation.grandstream.com/knowledge-base/vlan-guide/ (дата звернення: 12.05.2025).

15. Seaman, M. Link Aggregation Control Protocol [Електронний ресурс] / M. Seaman. – 1999. – Режим доступу: https://www.ieee802.org/3/ad/public/mar99/seaman_1_0399.pdf (дата звернення: 12.05.2025).

16. Cisco Systems. Cisco Catalyst 2960-X Series Switch Datasheet [Електронний ресурс] / Cisco Systems. – Режим доступу: https://www.router-switch.com/media/upload/product-pdf/cisco-switch-catalyst-2960x-datasheet.pdf#:~:text=Cisco%C2%AE%20Catalyst%C2%AE%202960-X%20Series%20Switches%20are%20fixed-configuration%2C%20stackable,access%20for%20campus%20and%20branch%20applications%20%28Figure%201%29 (дата звернення: 12.05.2025).

17. TP-Link. JetStream 24-Port Gigabit Smart Switch with 4 SFP Slots Omada logo [Електронний ресурс] / TP-Link. – Режим доступу: https://www.tp-link.com/us/business-networking/smart-switch/t1600g-28ts/ (дата звернення: 12.05.2025).

18. Fortinet. FortiSwitch™ Secure Access [Електронний ресурс] / Fortinet. – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortiswitch-secure-access-series.pdf (дата звернення: 12.05.2025).

19. Starlink. Центр підтримки [Електронний ресурс]. – режим доступу: https://www.starlink.com/support (дата звернення – 12.05.2025).

20. Humair. Single/Dual and Multihomed Connections [Електронний ресурс]. – режим доступу: https://humairahmed.com/blog/?p=3883 (дата звернення – 12.05.2025).

21. Wikipedia contributors. Dual-homed [Електронний ресурс]. – режим доступу: https://en.wikipedia.org/wiki/Dual-homed (дата звернення – 12.05.2025).

22. CERT-UA. CERT-UA минулого року опрацювала 4315 кіберінцидентів [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (дата звернення – 12.05.2025).

23. Full Mesh Topology [Електронний ресурс]. – Режим доступу: https://ar.inspiredpencil.com/pictures-2023/full-mesh-topology (дата звернення – 14.05.2025).

24. CRS317-1G-16S+RM. Cloud Router Switch – Product Datasheet [Електронний ресурс]. – Режим доступу: https://cdn.mikrotik.com/web-assets/product_files/CRS317-1G-16Splus_211004.pdf (дата звернення – 14.05.2025).

25. FortiSwitch 224E Series: FS-224E, FS-224E-PO – Quick Start Guide [Електронний ресурс]. – Режим доступу: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/e80c525a-202f-11e9-b6f6-f8bc1258b856/FortiSwitch-224E-Series-QSG.pdf (дата звернення – 14.05.2025).

26. Як вибрати ДБЖ? [Електронний ресурс] // ITbox.ua – Режим доступу: https://www.itbox.ua/ua/blog/Yak-vibrati-DBZh/ (дата звернення – 14.05.2025).

27. Purkis M. What is server clustering? [Електронний ресурс]. – Liquid Web, 2023. – Режим доступу: https://www.liquidweb.com/blog/what-is-server-cluster/ (дата звернення – 23.05.2025).

28. HSRP vs VRRP vs GLBP Protocols [Електронний ресурс]. – Режим доступу: https://www.geeksforgeeks.org/hsrp-vs-vrrp-vs-glbp-protocols/ (дата звернення – 23.05.2025).

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В. Н. Каразіна

Навчально-науковий інститут комп'ютерних наук та штучного інтелекту
Кафедра комп'ютерних систем та робототехніки
Рівень вищої освіти (освітньо-кваліфікаційний рівень) **Бакалавр**
Галузь знань: 15 – Автоматизація та приладобудування
Спеціальність: 151 – Автоматизація та комп'ютерно-інтегровані технології
Освітня програма «Автоматизація та комп'ютерно-інтегровані технології»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри комп'ютерних
систем та робототехніки
к. ф.-м. н., доц. ХРУСЛОВ М. М.
«02» жовтня 2024року

З А В Д А Н Н Я
НА ДИПЛОМНУ РОБОТУ (ПРОЕКТ)

ХОДЄЄВА Марія Олегіна
(прізвище, ім'я, по батькові студента)

1. Тема роботи **«Модель серверної інфраструктури для корпоративного сектору з аналізом стійкості до збоїв»**
керівник роботи Хруслов Максим Михайлович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від ***16 квітня 2025року №4101-5/962***
2. Строк подання студентом роботи ***30 травня 2025 року***

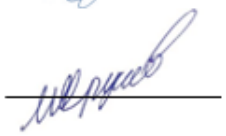
3. Перелік питань, які потрібно розробити)
1) Основні принципи моделювання серверної інфраструктури для корпоративного сектору в умовах зовнішньої нестабільності;
2) Методи забезпечення відмовостійкості: інтеграція резервного живлення, failover-механізмів та систем моніторингу;
3) Проектування архітектури серверної інфраструктури: вибір обладнання, технологій, структура системи та інтерфейс управління;
4) Реалізація основних функціональних компонентів інфраструктури та механізмів автоматичного відновлення після збоїв;
5) Аналіз результатів: визначення переваг, недоліків та шляхів оптимізації процесів відновлення системи.

4. План роботи

№ з/п	Назви етапів роботи	
1	Ознайомитись із постановкою задачі кваліфікаційної роботи.	2.10.2024-25.11.2024
2	Визначення основних вимог до серверної інфраструктури: надійність та відмовостійкість.	26.11.2024-17.12.2024
3	Дослідження доступних технологій та інструментів для забезпечення резервування, failover-механізмів і мережевої доступності.	02.01.2025-29.01.2025
4	Створення прототипу моделі серверної інфраструктури: визначення ключових компонентів, їх взаємодії та вибір обладнання.	03.02.2025-02.03.2025
5	Реалізація симуляційної моделі та тестування системи у різних сценаріях збоїв.	03.03.2025-31.03.2025
6	Підготувати пояснювальну записку, що містить опис методології, результатів дослідження та обґрунтування вибору обладнання.	17.05.2025-29.05.2025
7	Підготувати графічний та демонстраційний матеріал: схеми, діаграми, відео або презентацію результатів симуляцій.	30.05.2025
8	Представлення кваліфікаційної роботи керівнику та рецензенту	

5. Дата видачі завдання ***2 жовтня 2024 року.***

Студент  Ходєєва М. О.
підпис ініціали, прізвище

Керівник роботи  Хруслов М. М.
підпис ініціали, прізвище

Додаток Б

Затверджую

_____

«_____»_____2025 р.

Технічне завдання

на розробку програмного виробу ««Модель серверної інфраструктури для корпоративного сектору з аналізом стійкості до збоїв»

1.	Введення	1.1. Назва. Модель серверної інфраструктури для корпоративного сектору з аналізом стійкості до збоїв. 1.2. Галузь застосування. Інформаційні технології, комп'ютерні мережі, серверна інфраструктура, автоматизація.
2.	Підстава для розробки	2.1. Навчальний план за спеціальністю 151 – Автоматизація та комп'ютерно-інтегровані технології 2.2. Завдання на кваліфікаційну роботу бакалавра затверджене наказом по університету від "16" квітня 2025 року № 4101-5/962 (представлено як Додаток А до пояснювальної записки до кваліфікаційної роботи).
3.	Призначення розробки	3.1. Мета розробки. Створення моделі серверної інфраструктури для call-центру з підвищеною стійкістю до збоїв на основі технологій Fortinet, SD-WAN, VLAN, LACP, резервного живлення. 3.2. Призначення розробки. Забезпечення безперервного доступу до IT-послуг, зменшення

		простоїв, автоматичне перемикання у разі збоїв, підвищення надійності корпоративної мережі. 3.3. Вихідні дані розробки. Технічні характеристики обладнання, вимоги до відмовостійкості, результати аналізу рішень резервування і архітектурних схем.
4.	Технічні вимоги до програмного виробу	4.1. Вимоги до функціональних характеристик: – моделювання інфраструктури; – аналіз стійкості до збоїв; – візуалізація схеми; – підготовка технічного обґрунтування. 4.2. Вимоги до надійності: – імітація роботи failover-механізмів; – опис і тестування сценаріїв відмов. 4.3.Вимоги до умов експлуатації: – використання ПК або ноутбука. 4.4. Вимоги до складу і параметрів технічних засобів: – програмне забезпечення: MS Visio, Microsoft Office, PDF-редактор. – апаратне забезпечення: ПК. 4.5. Вимоги до інформаційної та програмної сумісності: немає 4.6. Вимоги до маркування та упаковки: немає 4.7. Вимоги до транспортування і зберігання: на звичайних носіях інформації 4.8. Спеціальні вимоги: – забезпечити зрозумілу та логічну структуру пояснювальної записки та діаграм.

5.	Вимоги до програмної документації	До програмної документації до виробу «Модель серверної інфраструктури для корпоративного сектору з аналізом стійкості до збоїв» входять: 1. Справжнє технічне завдання (Додаток Б до пояснювальної записки); 2. Методика побудови моделі та обґрунтування вибору обладнання (розділ 2 і 3 пояснювальної записки); 3. Опис інфраструктури (розділ 3 пояснювальної записки).	
6.	Вимоги до техніко-економічних показників	– Підвищення стійкості до збоїв; – Оптимізація вартості за рахунок правильного вибору архітектури та обладнання; – Мінімізація витрат на простої IT-систем.	
7.	Стадії і етапи розробки	Дата	Назва етапу
		до 15 січня	Ознайомитись із постановкою задачі дипломної роботи
		до 15 лютого	Визначення основних вимог до серверної інфраструктури: надійність та відмовостійкість
		до 15 березня	Дослідження доступних технологій резервування, failover, доступності мереж
		до 1 квітня	Дослідження інструментів для проектування модельної інфраструктури
		до 20 квітня	Створення візуалізації моделі серверної інфраструктури: визначення ключових

		компонентів, їх взаємодії та вибір обладнання. до 12 травня Підготовка пояснювальної записки до 20 травня Підготовка графічного матеріалу (схем, презентації, відео) до 30 травня Представлення дипломної роботи керівнику та рецензенту
8.	Порядок контролю і приймання програмного продукту (моделі)	1. Контроль прогресу розробки здійснювати щонайменше один раз на три тижні. 2. Захист моделі – на засіданні Атестаційної комісії. 3. Пояснювальну записку надати в електронному вигляді у форматі PDF або DOCX..

Виконавиця
студентка КУ41
Ходєєва Марія

Замовник
к.ф.-м.н, доцент, доцент закладу вищої освіти
Хруслов Максим Михайлович

Додаток В

«Узгоджено» «Затверджено»

Програма та методика випробувань програмного виробу
«Модель серверної інфраструктури call-центру з використанням обладнання Fortinet у середовищі Microsoft Visio»

1. Об'єкт випробувань

1.1 Найменування програмного виробу.

Програмний виріб — "Модель серверної інфраструктури call-центру з використанням обладнання Fortinet у середовищі Microsoft Visio".

1.2 Область застосування.

Розроблена модель призначена для використання під час проєктування корпоративної IT-інфраструктури з розмежуванням віртуальних локальних мереж (VLAN), маршрутизацією трафіку, забезпеченням резервування каналів зв'язку та електроживлення. Модель може застосовуватись для навчальних, демонстраційних, планувальних або тендерних цілей у сфері IT, телекомунікацій та безпеки.

1.3 Умовне призначення розробки (за потреби).

Розробка моделі має на меті створення наочної технічної візуалізації інфраструктури call-центру, здатного обслуговувати 60–100 одночасних користувачів з 3 віртуальними мережами, централізованим доступом до серверів та резервованим живленням. Умовне призначення — використання моделі як шаблону для впровадження на практиці або для подальшого розширення проєктної документації.

Перелічені відомості запозичуються із відповідних розділів Технічного завдання.

2. Мета випробувань

Метою проведення випробувань є підтвердження відповідності розробленої моделі серверної інфраструктури функціональним, технічним та візуальним вимогам, визначеним у Технічному завданні, а також перевірка її коректної структури, цілісності, узгодженості компонентів та відповідності принципам побудови надійної корпоративної мережі.

3. Загальні положення

3.1 Підстави щодо випробувань

Підставою для проведення випробувань є:

- Наказ ХНУ № 4101-5/962 від «16» квітня 2025 року про затвердження тем кваліфікаційних робіт бакалаврів;
- Навчальний план спеціальності 151 "Автоматизація та комп'ютерно-інтегровані технології";
- Технічне завдання до дипломної роботи, погоджене на кафедрі автоматизації та комп'ютерно-інтегрованих технологій.

3.2 Місце та тривалість випробувань

Приймальні випробування проводяться на базі комп'ютерного класу кафедри автоматизації та комп'ютерно-інтегрованих технологій ХНУ.

Тривалість випробувань — протягом 1 тижня з моменту подання остаточної версії моделі на перевірку.

Підрозділ 3.3. «Обсяг випробувань»

Приймальні випробування програмного виробу проводяться в обсязі відповідно до цієї Програми та методики випробувань.

3.4 Організації, які беруть участь у випробуваннях

У випробуваннях беруть участь:

- Виконавець кваліфікаційної роботи (студент);
- Керівник кваліфікаційної роботи;
- Комісія, призначена для приймання та оцінки кваліфікаційних робіт відповідно до наказу ХНУ.

4. Вимоги до програмного виробу

Під час випробувань перевіряється відповідність розробленої моделі таким вимогам:

Функціональні вимоги:

- Наявність трьох інтернет-провайдерів з підключенням до FortiGate;
- Коректне зображення двох брандмауерів FortiGate з розмежуванням інтерфейсів port17 та port18;
- Розміщення та зв'язки з двома Core-комутаторами (Port 1/SFP1 та Port 2/SFP2);
- Наявність щонайменше чотирьох VLAN-комутаторів з підключенням через LACP (Port 5–8);
- Логічне та візуальне поділення на VLAN-сегменти: робочі станції, керівництво, IP-телефонія, серверна;
- Підключення сервера до комутатора Server VLAN;
- Реалізація резервного живлення: UPS з перемиканням на генератор у разі зникнення живлення.

Технічні вимоги:

- Відповідність стандартам побудови корпоративних мереж;
- Відображення резервованих каналів зв'язку (dual-homing) на рівні брандмауерів та комутаторів;
- Використання зрозумілих та уніфікованих умовних позначень (стенсили Fortinet).
- Естетичні та ергономічні вимоги:
- Зрозуміле та охайне компонування елементів;
- Логічна групація компонентів за призначенням;
- Мінімізація перетину ліній зв'язку;
- Доступність для редагування без втрати структури.

5. Вимоги до програмної документації

Склад документації, що подається на випробування, включає:

- Технічне завдання на розробку програмного виробу (представлено в Додатку А до кваліфікаційної роботи);

- Пояснювальну записку з описом архітектури моделі, обґрунтуванням вибору обладнання та сценарієм її використання (розділи 1–3 роботи);
- Програма та методика випробувань (цей додаток).

Документація повинна відповідати вимогам ДСТУ 3973:2000 (ЄСПД) та внутрішнім стандартам кафедри щодо оформлення кваліфікаційних робіт.

6. Засоби та порядок випробувань

6.1 Засоби випробувань

Технічні засоби

- ПК з ОС Windows 10 або новішою;
- Оперативна пам'ять не менше 8 ГБ;
- Монітор з роздільною здатністю Full HD або більше.

Програмні засоби:

- Microsoft Visio 2019 або новіший;
- Встановлений набір стенсилів Fortinet (офіційна бібліотека);
- Програмне забезпечення для перегляду та редагування документації (Microsoft Word / PDF Reader).

6.2 Порядок проведення випробувань

1-й етап – Ознайомчий

1-й підетап. Перевірка комплектності документації та інструментів

- Перевірка наявності технічного завдання, пояснювальної записки, методики випробувань.
- Перевірка наявності стенсильних бібліотек та шаблону Visio.

2-й підетап. Перевірка якості документації

- Візуальний огляд відповідності структури документів вимогам ЄСПД.
- Оцінка логіки опису, наявності необхідних пояснень до кожного модуля.

2-й етап – Власне випробування програмного виробу

Тест 1: Перевірка працездатності моделі у середовищі Microsoft Visio

- Відкрити файл моделі у Microsoft Visio.
- Перевірити коректність відображення всіх елементів.
- Змінити розташування кількох блоків для перевірки цілісності ліній зв'язку.

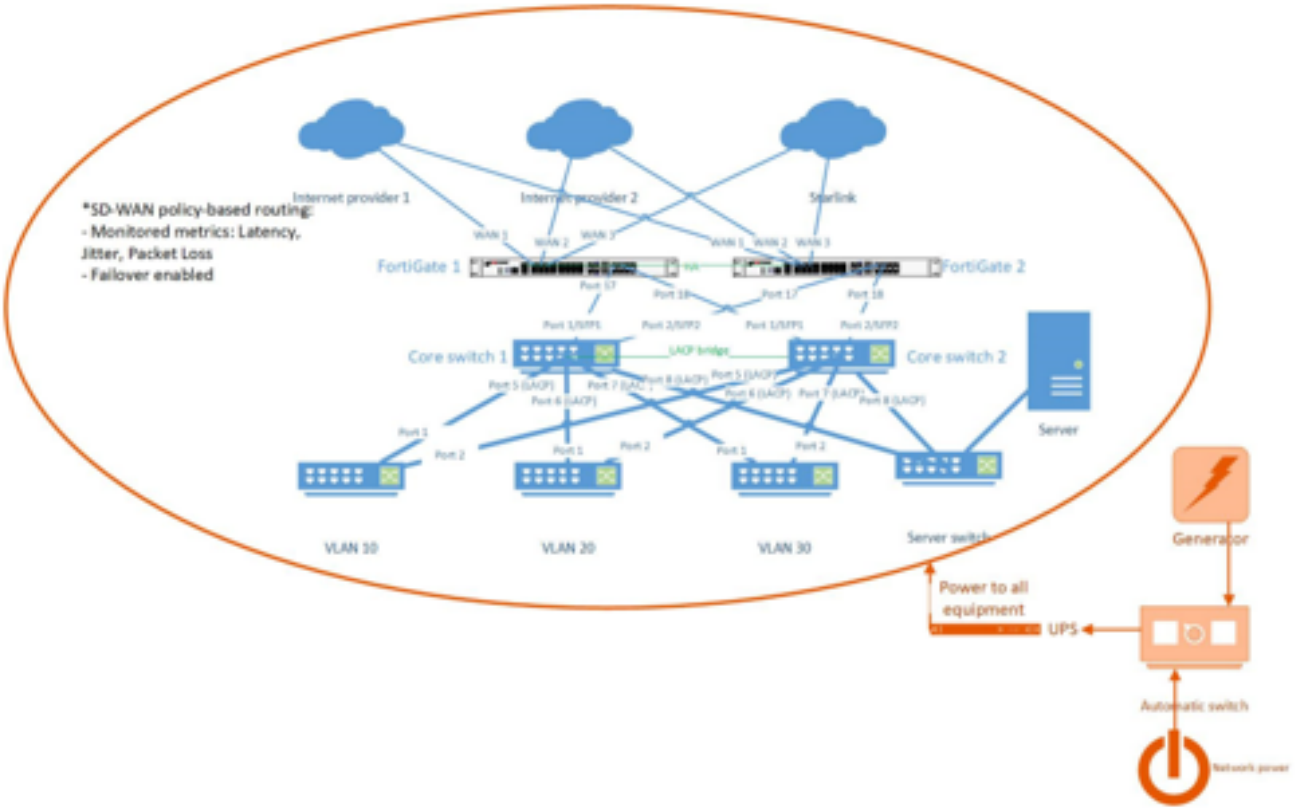


Рисунок В.1 – результат відкриття моделі.

Висновок: модель працює стабільно, усі елементи редагуються, структура не порушується.

Тест 2: Перевірка відповідності функціональних вимог

Послідовно перевірити:

- Наявність усіх типів комутаторів і маршрутизаторів;
- Правильність підключення за специфікацією VLAN і портів;
- Візуальне маркування сегментів;

- Зображення маршрутизації, резервування каналів, електроживлення.

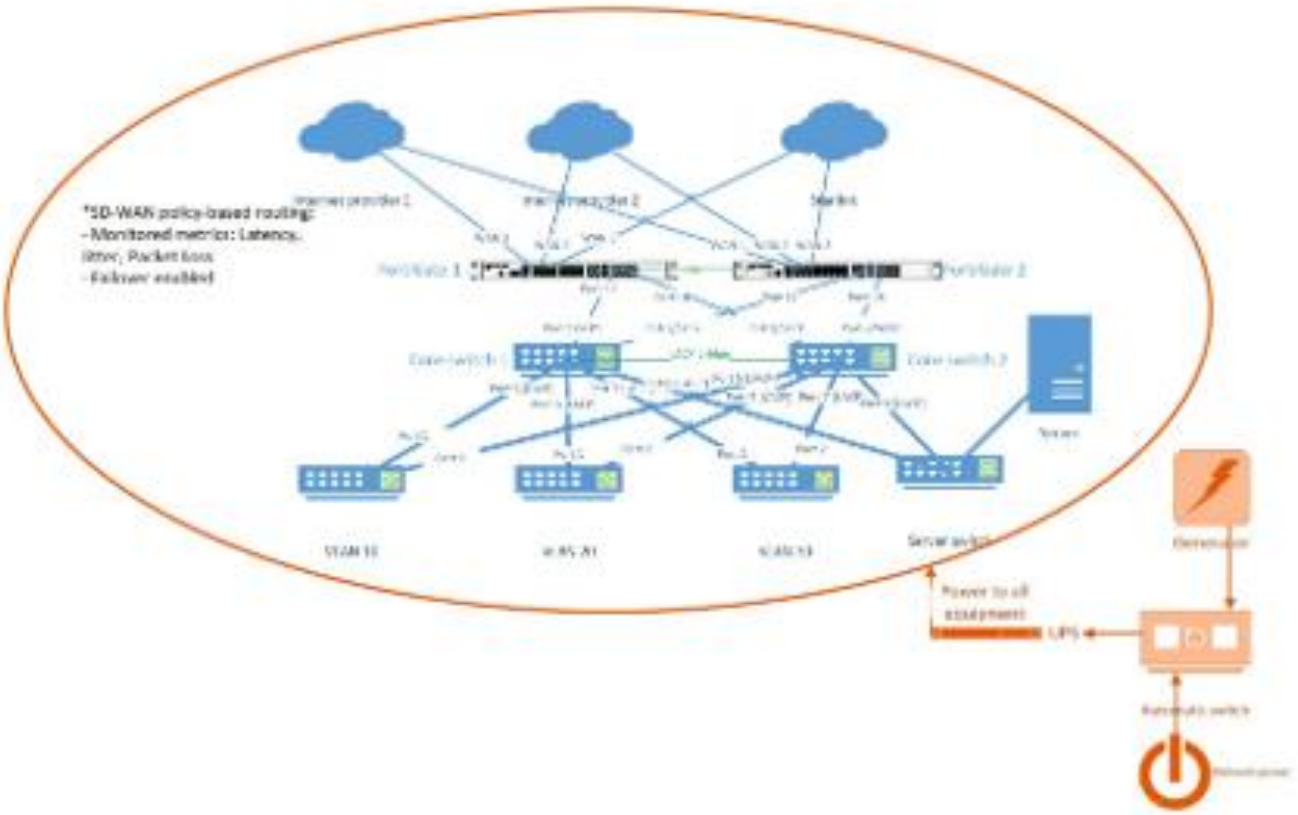


Рисунок В.2 – модель для візуальної перевірки.

Висновок: усі функціональні вимоги задоволено, модель відповідає технічному завданню.

Тест 3: Симуляція сценарію відмови електроживлення

- Імітація перемикання живлення з основного на генератор.
- Перевірка наявності UPS та схеми перемикання.

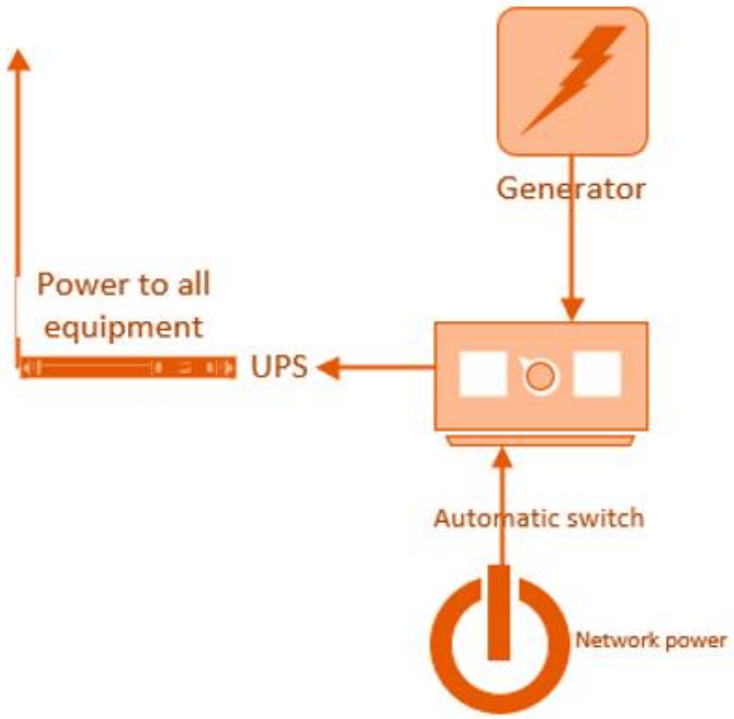


Рисунок В.3 – частина моделі, що зображує подання електроенергії до серверної інфраструктури.

Висновок: модель демонструє резервування живлення.

Виконавець

студентка КУ41, Ходєєва Марія