Міністерство освіти і науки України
Університет митної справи та фінансів

Факультет інноваційних технологій
Кафедра комп'ютерних наук та інженерії програмного забезпечення

Кваліфікаційна робота бакалавра
на тему: «Проєктування інформаційної системи для розвитку інфраструктури комп'ютерної мережі УМСФ»

Виконав: студент групи ІПЗ-21-2
Спеціальність 121 «Інженерія програмного забезпечення»
Костров Влас Олександрович
(прізвище та ініціали)

Керівник к.т.н., доц. Чупілко Т.А.
(науковий ступінь, вчене звання, прізвище та ініціали)

Рецензент Університет митної справи та фінансів
(місце роботи)

Доцент кафедри кібербезпеки та інформаційних технологій
(посада)

к.т.н., доц. Савченко Ю.В.
(науковий ступінь, вчене звання, прізвище та ініціали)

Дніпро – 2025

АНОТАЦІЯ

Костров В.О. Проєктування інформаційної системи для розвитку інфраструктури комп'ютерної мережі УМСФ.

Кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 121 «Інженерія програмного забезпечення» -- Університет митної справи та фінансів, Дніпро, 2025.

Пояснювальна записка: 65 сторінок, 18 рисунків, 27 джерел.

У кваліфікаційній роботі виконано комплексне дослідження предметної області інформаційних систем та комп'ютерних мереж вищих навчальних закладів на прикладі Університету митної справи та фінансів - УМСФ. Аналіз наявного стану мережі виявив існуючі технічні, організаційні та безпекові проблеми, серед яких фрагментарність систем, відсутність централізованого моніторингу та недостатня масштабованість. Розроблено методику моделювання мережевої інфраструктури з використанням DFD, ERD та UML-діаграм, проведено порівняльний аналіз інструментів (Cisco Packet Tracer, GNS3).

На основі узагальнених вимог спроектовано інформаційну систему, що забезпечує: вибір архітектури «клієнт-сервер» з підтримкою віртуалізації та хмарних сервісів; логічну та інформаційну моделі даних; схему фізичної топології та сегментацію мережі для підвищення безпеки; підсистеми централізованого управління, моніторингу та аналітики.

Об'єкт дослідження: процеси передачі даних з використанням комп'ютерних мереж вищих навчальних закладів. Предмет дослідження: методи та інструменти моделювання комп'ютерних мереж та іншої мережевої інфраструктури УМСФ. Мета: удосконалення інфраструктури комп'ютерної мережі УМСФ.

Ключові слова: ПРОЄКТУВАННЯ, ІНФОРМАЦІЙНА СИСТЕМА, КОМП'ЮТЕРНА МЕРЕЖА, ІНФРАСТРУКТУРА, БЕЗПЕКА, МОДЕЛЮВАННЯ, ХМАРНІ СЕРВІСИ, ВІРТУАЛІЗАЦІЯ, ТОПОЛОГІЯ МЕРЕЖІ, МОНИТОРИНГ, МАСШТАБОВАНІСТЬ, УПРАВЛІННЯ МЕРЕЖЕЮ

ANNOTATION

Kostrov V.O. “Design of an Information System for the Development of the Computer Network Infrastructure of UMSF.”

Bachelor’s qualification work for the educational degree of Bachelor in specialty 121 “Software Engineering” – University of Customs and Finance, Dnipro, 2025.

Explanatory note: 65 pages, 18 figures, 27 sources.

The qualification paper presents a comprehensive study of the subject area of information systems and computer networks in higher education institutions on the example of the University of Customs and Finance (UMSF). An analysis of the existing network revealed technical, organizational, and security problems, among them fragmented systems, lack of centralized monitoring, and insufficient scalability. A methodology for modeling the network infrastructure using DFD, ERD, and UML diagrams was developed, and a comparative analysis of tools (Cisco Packet Tracer, GNS3) was conducted.

Based on the consolidated requirements, an information system was designed to provide: choice of a client–server architecture with support for virtualization and cloud services; logical and information data models; a physical topology scheme and network segmentation to enhance security; subsystems for centralized management, monitoring, and analytics.

Object of Research: Data transfer processes using computer networks in higher education institutions.

Subject of Research: Methods and tools for modeling computer networks and other network infrastructure of UMSF.

Purpose: Improvement of the computer network infrastructure of UMSF.

Keywords: DESIGN, INFORMATION SYSTEM, COMPUTER NETWORK, INFRASTRUCTURE, SECURITY, MODELING, CLOUD SERVICES, VIRTUALIZATION, NETWORK TOPOLOGY, MONITORING, SCALABILITY, NETWORK MANAGEMENT.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

УМСФ – Університет митної справи та фінансів

ІС – інформаційна система

ІТ – інформаційні технології

ВНЗ – вищий начальний заклад

VPN – Virtual Private Network (віртуальна приватна мережа)

Wi-Fi – Wireless Fidelity (стандарт бездротового доступу)

ЗМІСТ

ВСТУП

Актуальність теми «Проєктування інформаційної системи для розвитку інфраструктури комп'ютерної мережі УМСФ» полягає в тому, що у сучасному інформаційному суспільстві комп'ютерні мережі є невід'ємною частиною інфраструктури будь-якої організації, зокрема у вищих начальних закладах. В умовах цифровізації освітнього середовища, зростання обсягів переданих даних, переходу до змішаних та дистанційних форматів навчання, потреба у надійній, безпечній та масштабованій мережевій інфраструктурі набуває критичної важливості. Університет митної справи та фінансів (УМСФ) є державним вищим навчальним закладом, який активно впроваджує сучасні технології в освітній процес, проте стикається з низкою викликів у сфері розвитку власної IT-інфраструктури.

Перелік аргументів, що підкреслюють актуальність даної теми:

– Зростання навантаження на мережеву інфраструктуру. Кількість пристроїв, підключених до університетської мережі, постійно зростає. До традиційних комп'ютерів і серверів додаються мобільні пристрої, інтернет речей (IoT), мультимедійне обладнання для аудиторій тощо. Це створює значне навантаження на канали зв'язку, комутатори та точки доступу, що вимагає від системи високої пропускної здатності, стабільності та гнучкості в управлінні трафіком.

– Впровадження хмарних сервісів і дистанційної освіти. Поширення таких платформ, як Google Workspace for Education, Moodle, Microsoft 365 та Zoom, змінює характер навчання і вимагає постійного онлайн-доступу. Для цього потрібна підтримка надійних і безпечних VPN-з'єднань, можливість балансування навантаження, захист каналів передачі даних та гарантія доступності ресурсів у будь-який час.– Фрагментарність наявної IT-інфраструктури. Існуючі технічні рішення реалізовані точково, без єдиної концепції або інтегрованої архітектури. Це ускладнює технічну підтримку, масштабування мережі та її подальший розвиток. Відсутність взаємозв'язку між

підсистемами призводить до дублювання функцій, втрати даних і зниження загальної ефективності ІТ-середовища.

– Відсутність системного підходу до проєктування. Багато елементів мережі створювались окремо без урахування єдиної логіки, вимог безпеки або перспектив розвитку. Це призводить до неузгодженості у виборі обладнання, відсутності резервування, нераціонального використання ресурсів та ускладнює управління мережею.

– Зростання вимог до цифрового середовища студентів та викладачів. Сучасні користувачі очікують стабільного та швидкого доступу до навчальних платформ, електронної бібліотеки, наукових баз даних та онлайн-сервісів без затримок або збоїв. Це вимагає від ІТ-інфраструктури високої надійності, швидкодії та адаптивності.

– Потреба в автоматизації та моніторингу. Ефективне управління великою мережею неможливе без централізованих систем моніторингу, збору логів, сповіщень про збої та автоматичного резервування. Відсутність таких систем збільшує час реагування на інциденти та навантаження на ІТ-персонал.

– Підвищення частоти та складності кібератак. Університетські мережі є привабливою ціллю для кіберзлочинців через наявність великої кількості персональних даних, облікових записів і відкритих каналів доступу. Без належного рівня захисту навіть незначна вразливість може призвести до серйозних наслідків.

Таким чином, проєктування інформаційної системи для розвитку інфраструктури комп'ютерної мережі УМСФ є актуальним завданням, що спрямоване на підвищення надійності, продуктивності та безпеки мережі, забезпечення якісної цифрової підтримки освітнього процесу та відповідність сучасним ІТ-викликам.

Об'єктом дослідження є процес передачі даних з використанням комп'ютерних мереж Університету митної справи та фінансів.

Предметом дослідження є методи та інструменти моделювання комп'ютерної мережі УМСФ, зокрема розробка логічної та інформаційної

моделей мережі за допомогою DFD, ERD та UML-діаграм, а також порівняльний аналіз програмних засобів (Cisco Packet Tracer, GNS3 тощо) для оцінки їхньої ефективності при побудові віртуальної моделі мережі з урахуванням вимог безпеки, масштабованості та надійності .

Метою дослідження є удосконалення інфраструктури комп'ютерної мережі УМСФ задля створення єдиного цифрового простору, який забезпечуватиме безпечний та централізований доступ студентів і викладачів до навчальних, наукових і адміністративних ресурсів, підтримку дистанційного й гібридного навчання, ефективне адміністрування інформаційних систем закладу з оптимізацією використання обчислювальних та технічних ресурсів, а також масштабовану й гнучку мережеву архітектуру для подальшого розширення сервісів і інтеграції з хмарними рішеннями.

Завдання кваліфікаційної роботи бакалавра:

– дослідити сучасні підходи до проєктування інформаційних систем та інфраструктури комп'ютерних мереж у ВНЗ;

– проаналізувати поточний стан комп'ютерної мережі УМСФ та виявити основні проблеми її функціонування;

– сформувати вимоги до нової інформаційної системи з урахуванням стандартів безпеки та технологічних трендів;

– обґрунтувати вибір архітектури інформаційної системи та мережевої топології;

– розробити логічну та інформаційну моделі системи, у тому числі через діаграми DFD, ERD та UML;

– сформулювати рекомендації щодо впровадження системи з урахуванням бюджетних та організаційних обмежень.

Методи дослідження: методи системного аналізу для оцінки поточного стану мережі; методи моделювання для візуалізації інформаційної та мережевої структури (DFD, ERD, UML); методи логічного узагальнення, індукції та дедукції при формуванні вимог та архітектурних рішень; методи порівняльного аналізу для оцінки ефективності програмного забезпечення для моделювання

(Cisco Packet Tracer, GNS3); аналіз нормативно-правової бази, зокрема стандартів ISO/IEC 27001, ISO/IEC 12207, ДСТУ 2627-94 та законодавства України у сфері захисту інформації.

Структура кваліфікаційної роботи: робота складається зі вступу, 3 розділів, списку використаних джерел із 27 посилань, 2 додатків. Кваліфікаційна робота складається з 45 сторінок основної частини, містить 18 рисунків та 8 таблиць.

Практична значимість цієї роботи полягає у створенні реального проєкту інформаційної системи, яка може бути впроваджена в інфраструктуру УМСФ для покращення функціонування комп'ютерної мережі. Запропонована модель системи є гнучкою та масштабованою, що дозволяє адаптувати її до майбутніх змін в організаційній структурі, кількості користувачів або технічних потреб. Університет отримає можливість централізованого управління всіма мережевими ресурсами, що знизить витрати на технічне обслуговування та підвищить рівень контролю над інформаційними потоками.

Розроблені в межах роботи діаграми, моделі та архітектурні рішення можуть бути безпосередньо використані ІТ-відділом УМСФ як проєктна документація для модернізації мережевої інфраструктури. Крім того, результати дослідження можуть слугувати навчальним прикладом для студентів, які вивчають дисципліни з комп'ютерних мереж, системного аналізу та проєктування ІС. Таким чином, ця робота поєднує як теоретичну, так і прикладну цінність, що робить її корисною не лише для розвитку університетської мережі, але й для підготовки майбутніх фахівців у сфері ІТ.

Запропоновані рішення відповідають вимогам сучасних стандартів кібербезпеки, що дозволяє забезпечити захист персональних та корпоративних даних університету. Упровадження цієї системи сприятиме безперервності освітнього процесу, особливо в умовах дистанційного навчання чи кризових ситуацій. Оскільки модель передбачає інтеграцію з хмарними платформами, зокрема Google Workspace for Education, це відкриває нові можливості для ефективної організації освітнього середовища.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Сутність і класифікація інформаційних систем

Інформаційна система (ІС) — це сукупність взаємопов'язаних компонентів, що забезпечують збирання, обробку, зберігання, передачу та представлення інформації для підтримки процесів прийняття рішень, управління та контролю в організації (рисунок 1.1 [27]). Основною метою ІС є забезпечення користувачів необхідною інформацією в потрібний час і у відповідній формі. ІС включає в себе апаратне забезпечення, програмне забезпечення, бази даних, мережеві ресурси та персонал, який забезпечує її функціонування [27].

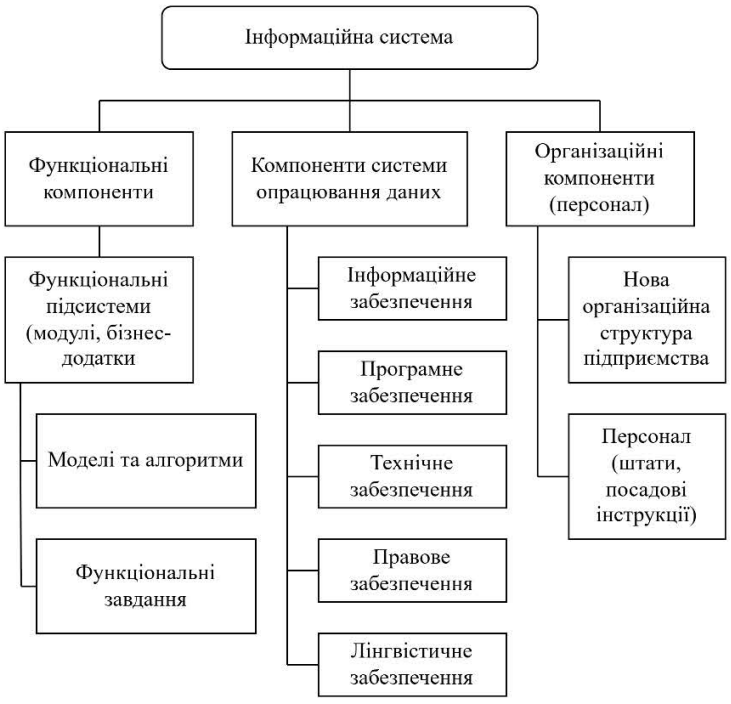

Рисунок 1.1 – Компоненти інформаційної системи

Розвиток інформаційних систем відбувався паралельно з еволюцією інформаційних технологій. Початково ІС були орієнтовані на автоматизацію обчислювальних задач, але з часом їх функціональність розширилася до підтримки управлінських процесів, аналізу даних та прийняття рішень. Сучасні

ІС інтегрують різноманітні технології, включаючи штучний інтелект, хмарні обчислення та мобільні платформи, що дозволяє забезпечити гнучкість та адаптивність до змін у бізнес-середовищі.

Класифікація інформаційних систем є важливою для розуміння їх функціональних можливостей та сфер застосування. ІС можна класифікувати за різними ознаками, представлено у таблиці 1.1, такими як рівень автоматизації, сфера застосування, тип користувачів, функціональне призначення та інші. Це дозволяє ефективно планувати впровадження ІС та оптимізувати їх використання в організації.

Таблиця 1.1

Класифікація інформаційних систем за різними ознаками

Ознака класифікації	Типи інформаційних систем
Сфера застосування	Управлінські, виробничі, фінансові, маркетингові, освітні
Рівень управління	Оперативні, тактичні, стратегічні
Тип користувачів	Індивідуальні, групові, корпоративні
Функціональне призначення	Системи підтримки прийняття рішень, експертні системи
Технологічна основа	Локальні, мережеві, хмарні, мобільні

Однією з ключових класифікацій є поділ ІС за рівнем управління: оперативні системи підтримують щоденні операції, тактичні — середньострокове планування, а стратегічні — довгострокове планування та прийняття рішень. Такий поділ дозволяє організаціям ефективно розподіляти ресурси та оптимізувати управлінські процеси.

Іншою важливою класифікацією є поділ ІС за функціональним призначенням, основі типи ІС за функціональним призначенням наведені у таблиці 1.2. Системи підтримки прийняття рішень (СППР) надають аналітичні інструменти для керівників, експертні системи використовують бази знань для вирішення специфічних задач, а інформаційно-пошукові системи забезпечують доступ до великих обсягів даних. Кожен тип ІС має свої особливості та призначення, що визначає їх використання в різних сферах діяльності.

Таблиця 1.2

Основні типи інформаційних систем за функціональним призначенням

Тип ІС	Основні функції
Системи обробки транзакцій	Реєстрація та обробка щоденних операцій
Системи підтримки прийняття рішень	Аналіз даних, моделювання сценаріїв, підтримка рішень
Експертні системи	Надання рекомендацій на основі бази знань
Інформаційно-пошукові системи	Зберігання та пошук інформації в базах даних
Системи управління знаннями	Збирання, зберігання та розповсюдження знань

Згідно з міжнародним стандартом ISO/IEC 27001, класифікація інформації є важливою складовою системи управління інформаційною безпекою. Стандарт передбачає визначення критеріїв класифікації, призначення відповідних рівнів класифікації даним та забезпечення розуміння співробітниками того, як обробляти класифіковану інформацію безпечно. Це дозволяє організаціям ефективно захищати чутливу інформацію та відповідати вимогам нормативних актів [1].

Класифікація інформаційних систем також може базуватися на технологічній основі. Локальні ІС функціонують в межах однієї організації, мережеві — забезпечують взаємодію між різними підрозділами, хмарні — використовують інтернет-інфраструктуру для надання послуг, а мобільні — орієнтовані на використання на портативних пристроях. Такий поділ дозволяє організаціям вибирати ІС відповідно до своїх потреб та технічних можливостей.

У сучасних умовах розвитку інформаційних технологій важливим є також поділ ІС за ступенем інтеграції. Інтегровані ІС об'єднують різні функціональні підсистеми в єдину систему, що забезпечує узгодженість даних та процесів. Це дозволяє підвищити ефективність управління та прийняття рішень на всіх рівнях організації.

Загалом, класифікація інформаційних систем є багатовимірною та залежить від багатьох факторів, таких як функціональне призначення, рівень управління, технологічна основа та ступінь інтеграції. Правильне розуміння та

застосування класифікації ІС дозволяє організаціям ефективно впроваджувати та використовувати інформаційні технології для досягнення своїх стратегічних цілей.

1.2. Інфраструктура комп'ютерної мережі закладу освіти

Інфраструктура комп'ютерної мережі закладу освіти є комплексом технічних, програмних та організаційних засобів, що забезпечують ефективну підтримку освітнього процесу, наукових досліджень та адміністративного управління. Вона включає в себе апаратне забезпечення, програмне забезпечення, мережеві ресурси та персонал, який забезпечує її функціонування. Сучасна мережна інфраструктура повинна бути масштабованою, надійною та безпечною, щоб відповідати зростаючим вимогам цифрової освіти.

Основними компонентами комп'ютерної мережі закладу освіти є: серверне обладнання, мережеве обладнання (маршрутизатори, комутатори, точки доступу), кінцеві пристрої (комп'ютери, ноутбуки, планшети), програмне забезпечення (операційні системи, системи управління базами даних, навчальні платформи), засоби забезпечення безпеки (фаєрволи, антивірусні програми) та системи резервного копіювання даних, призначення кожного з компонентів наведені у таблиця 1.3. Кожен з цих компонентів виконує важливу роль у забезпеченні безперебійної роботи мережі та підтримці освітнього процесу.

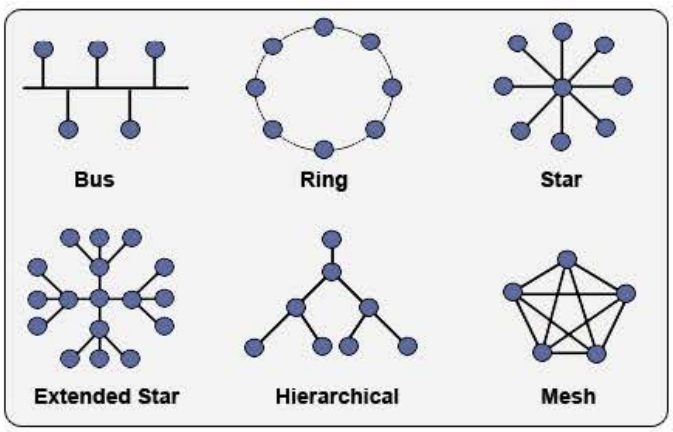

Рисунок 1.2 – Види топології комп'ютерних мереж

Топологія мережі (рисунок 1.2) визначає фізичне та логічне розташування мережевих пристроїв і впливає на ефективність передачі даних, масштабованість та надійність мережі. У закладах освіти найчастіше використовуються зіркоподібна, шинна або змішана топології, які дозволяють забезпечити гнучкість та простоту управління мережею. Вибір топології залежить від розміру закладу, кількості користувачів та специфіки освітнього процесу [2-4].

Забезпечення безпеки комп'ютерної мережі є критично важливим завданням для закладу освіти. Це включає в себе впровадження політик безпеки, використання фаєрволів, антивірусного програмного забезпечення, систем виявлення та запобігання вторгненням, а також регулярне оновлення програмного забезпечення та навчання персоналу з питань інформаційної безпеки. Захист персональних даних студентів та викладачів, а також конфіденційної інформації закладу, є пріоритетом у забезпеченні безпеки мережі.

Інтеграція хмарних технологій у мережеву інфраструктуру закладу освіти дозволяє розширити можливості зберігання та обробки даних, забезпечити доступ до навчальних ресурсів з будь-якого місця та пристрою, а також знизити витрати на обслуговування локального обладнання. Хмарні сервіси, такі як Google Workspace for Education або Microsoft 365 Education, надають інструменти для спільної роботи, комунікації та управління навчальним процесом [5].

Таблиця 1.3

Основні компоненти комп'ютерної мережі закладу освіти

Компонент	Призначення
Серверне обладнання	Зберігання та обробка даних, управління ресурсами мережі
Мережеве обладнання	Забезпечення передачі даних між пристроями, підключення до Інтернету
Кінцеві пристрої	Доступ користувачів до мережі та ресурсів закладу
Програмне забезпечення	Підтримка освітнього процесу, управління даними та ресурсами
Засоби безпеки	Захист мережі від несанкціонованого доступу та шкідливого програмного забезпечення
Системи резервного копіювання	Забезпечення збереження даних у разі збоїв або втрати інформації

Управління комп'ютерною мережею закладу освіти включає в себе моніторинг стану мережі, управління доступом користувачів, оновлення програмного забезпечення, забезпечення безпеки та вирішення технічних проблем. Ефективне управління дозволяє забезпечити безперебійну роботу мережі, своєчасне виявлення та усунення проблем, а також оптимальне використання ресурсів.

Модернізація комп'ютерної мережі є необхідною для адаптації до змін у технологіях та вимогах освітнього процесу. Це може включати оновлення обладнання, впровадження нових програмних рішень, розширення мережевої інфраструктури та інтеграцію нових сервісів. Планування модернізації повинно базуватися на аналізі поточних потреб закладу та прогнозуванні майбутніх вимог.

Таким чином, інфраструктура комп'ютерної мережі закладу освіти є складною системою, яка потребує ретельного планування, впровадження та управління. Її ефективне функціонування забезпечує підтримку освітнього процесу, сприяє впровадженню новітніх технологій та підвищує якість освіти.

1.3. Огляд сучасних тенденцій у розвитку IT-інфраструктури ВНЗ

У сучасному світі інформаційні технології відіграють ключову роль у трансформації освітнього процесу та управління вищим навчальним закладом (ВНЗ). IT-інфраструктура ВНЗ включає в себе апаратне забезпечення, програмне забезпечення, мережеві ресурси та сервіси, які забезпечують ефективну підтримку навчального процесу, наукових досліджень та адміністративних функцій. Сучасні тенденції розвитку IT-інфраструктури спрямовані на забезпечення гнучкості, масштабованості, безпеки та інноваційності освітнього середовища.

Однією з провідних тенденцій є впровадження хмарних технологій у діяльність ВНЗ. Хмарні сервіси дозволяють забезпечити доступ до навчальних матеріалів, програмного забезпечення та обчислювальних ресурсів з будь-якого

місця та пристрою. Це сприяє гнучкості навчального процесу, особливо в умовах дистанційного та змішаного навчання. Крім того, хмарні технології дозволяють знизити витрати на обслуговування локальної інфраструктури та забезпечити масштабованість ресурсів відповідно до потреб закладу [6].

Іншою важливою тенденцією є використання штучного інтелекту (ШІ) та машинного навчання для аналізу даних, автоматизації адміністративних процесів та персоналізації навчання. ШІ дозволяє прогнозувати успішність студентів, виявляти ризики відрахування, автоматизувати оцінювання та надавати рекомендації щодо покращення навчального процесу. Також ШІ використовується для створення інтелектуальних чат-ботів, які забезпечують підтримку студентів у режимі 24/7 [7].

Зростає значення аналітики навчання (Learning Analytics), яка дозволяє збирати та аналізувати дані про взаємодію студентів з навчальними матеріалами, їхню активність та результати. Це дає змогу викладачам адаптувати навчальні стратегії до індивідуальних потреб студентів, підвищуючи ефективність навчання. Аналітика також сприяє прийняттю обґрунтованих рішень щодо вдосконалення освітніх програм та методик викладання [8].

Впровадження технологій віртуальної та доповненої реальності (VR/AR) відкриває нові можливості для створення інтерактивних та імерсійних навчальних середовищ. Ці технології дозволяють студентам проводити віртуальні лабораторні роботи, досліджувати складні об'єкти та процеси, що особливо актуально для технічних та медичних спеціальностей. VR/AR сприяють підвищенню мотивації та залученості студентів у навчальний процес [9].

З огляду на зростаючу кількість кіберзагроз, забезпечення кібербезпеки стає пріоритетним завданням для ЗВО. Це включає впровадження сучасних засобів захисту інформації, навчання персоналу з питань безпеки, розробку політик безпеки та планів реагування на інциденти. Особливу увагу приділяється захисту персональних даних студентів та викладачів, а також забезпеченню безперервності освітнього процесу в умовах кіберінцидентів [10].

Таким чином, сучасні тенденції розвитку ІТ-інфраструктури ВНЗ спрямовані на створення гнучкого, безпечного та інноваційного освітнього середовища, яке відповідає вимогам цифрової епохи та забезпечує якісну освіту для студентів. Впровадження новітніх технологій сприяє підвищенню ефективності навчального процесу, розширенню доступу до освіти та підготовці фахівців, здатних успішно працювати в умовах цифрової економіки.

1.4. Аналіз наявного стану комп'ютерної мережі УМСФ

Комп'ютерна мережа Університету митної справи та фінансів (УМСФ) є ключовим елементом інформаційної інфраструктури закладу, що забезпечує підтримку освітнього процесу, наукових досліджень та адміністративного управління. Основні функції мережі включають забезпечення доступу до Інтернету, внутрішніх інформаційних ресурсів, електронної пошти, навчальних платформ та інших сервісів. Ефективність функціонування мережі безпосередньо впливає на якість освітніх послуг та загальну продуктивність університету.

УМСФ має розгалужену локальну мережу, яка охоплює всі навчальні корпуси, адміністративні будівлі та гуртожитки. Мережа побудована на основі сучасних технологій, включаючи оптоволоконні канали зв'язку та високошвидкісні маршрутизатори. Це забезпечує стабільне та швидке з'єднання для користувачів у всіх підрозділах університету. Крім того, мережа підтримує бездротовий доступ до Інтернету через Wi-Fi, що дозволяє студентам та викладачам підключатися до мережі з будь-якого пристрою[11].

Навчальна лабораторія системного адміністрування УМСФ відповідає за підтримку та розвиток ІТ-інфраструктури університету. Її фахівці здійснюють моніторинг мережі, забезпечують безпеку даних, оновлюють програмне забезпечення та надають технічну підтримку користувачам. Лабораторія також бере участь у впровадженні нових технологій та рішень для покращення функціонування мережі. Це включає впровадження систем управління мережею,

віртуалізацію серверів та використання хмарних сервісів для зберігання та обробки даних[12].

З метою оцінки поточного стану комп'ютерної мережі УМСФ було проведено SWOT-аналіз, який дозволяє виявити сильні та слабкі сторони мережі, а також можливості та загрози, що можуть впливати на її розвиток.

Таблиця 1.4

SWOT-аналіз комп'ютерної мережі УМСФ

Сильні сторони (Strengths)	Слабкі сторони (Weaknesses)
Розгалужена мережа, що охоплює всі підрозділи університету.	Обмеженість фінансових ресурсів для модернізації обладнання.
Використання сучасних технологій передачі даних.	Недостатня кількість кваліфікованого персоналу для обслуговування мережі.
Наявність спеціалізованої лабораторії для підтримки IT-інфраструктури.	Відсутність централізованої системи моніторингу та управління мережею.
Можливості (Opportunities)	Загрози (Threats)
Впровадження нових технологій, таких як хмарні сервіси та віртуалізація.	Зростання кіберзагроз та необхідність посилення заходів безпеки.
Співпраця з іншими навчальними закладами та IT-компаніями для обміну досвідом.	Швидкий розвиток технологій, що вимагає постійного оновлення обладнання та знань персоналу.

Аналіз показує, що комп'ютерна мережа УМСФ має значний потенціал для подальшого розвитку та модернізації. Впровадження нових технологій, таких як хмарні сервіси, віртуалізація та централізоване управління мережею, дозволить підвищити ефективність та безпеку мережі. Однак для цього необхідно вирішити проблеми, пов'язані з обмеженістю фінансових ресурсів та нестачею кваліфікованого персоналу.

Одним із напрямків розвитку мережі є впровадження системи централізованого моніторингу та управління, яка дозволить оперативно виявляти та усувати проблеми, а також забезпечить більш ефективне використання ресурсів. Крім того, необхідно посилити заходи з кібербезпеки, включаючи регулярне оновлення програмного забезпечення, впровадження систем виявлення вторгнень та навчання персоналу з питань безпеки.

Співпраця з іншими навчальними закладами та ІТ-компаніями може сприяти обміну досвідом та впровадженню передових рішень у сфері мережевих технологій. Це також може допомогти у залученні додаткових ресурсів для модернізації мережі та підвищення кваліфікації персоналу.

У підсумку, комп'ютерна мережа УМСФ є важливим елементом інфраструктури університету, який потребує постійного розвитку та вдосконалення. Вирішення наявних проблем та впровадження нових технологій дозволить забезпечити високий рівень якості освітніх послуг та ефективне управління університетом.

1.5. Визначення проблем, вимог і постановка задачі проєктування

Комп'ютерна мережа сучасного вищого навчального закладу виконує ключову роль у підтримці освітнього процесу, наукових досліджень та адміністративного управління. Університет митної справи та фінансів, як навчальний заклад державного рівня, активно використовує ІТ-інфраструктуру, однак із часом зростають вимоги до її пропускної здатності, стабільності, безпеки та масштабованості. Проведений аналіз наявного стану мережевої інфраструктури виявив ряд технічних, організаційних та програмних проблем, які перешкоджають ефективному функціонуванню комп'ютерної мережі університету. Проблеми накопичуються у зв'язку зі зростанням кількості пристроїв, переходом до змішаних форматів навчання, потребою в хмарних рішеннях та підвищенням загроз кібербезпеки [1].

Серед виявлених проблем можна виділити як застарілі технічні рішення, так і недоліки в організації адміністрування. Частина мережевого обладнання не відповідає сучасним вимогам швидкості та обробки трафіку, а структурна побудова мережі є недостатньо гнучкою для масштабування. Відсутність централізованих систем моніторингу та управління призводить до неефективного реагування на збої, а безпекові механізми, які використовуються, не враховують сучасні типи атак, як-от фішинг, соціальна інженерія, розподілені

атаки типу DDoS тощо [15]. Відповідно, виникає необхідність формалізувати ці проблеми для подальшого врахування у процесі проєктування.

Ключові проблеми наявної інфраструктури:

- Відсутність єдиної централізованої системи керування та моніторингу мережі;
- Недостатня пропускна здатність та швидкість з'єднань у ключових вузлах;
- Відсутність масштабованості та гнучкості мережевої структури;
- Низький рівень кіберзахисту (відсутність IDS/IPS, обмежене журналювання);
- Застарілі точки доступу Wi-Fi та нестабільність бездротового покриття;
- Відсутність сегментації мережі (VLAN), що підвищує ризик несанкціонованого доступу;
- Відсутність автоматизації резервного копіювання та обліку пристроїв;
- Фрагментарність підходів до організації доступу студентів і викладачів;
- Обмежений доступ до ресурсів університету з віддалених локацій;
- Відсутність інтеграції з хмарними сервісами та платформами електронного навчання.

Означені проблеми вимагають комплексного підходу до проєктування нової інформаційної системи, яка буде не лише відповідати технічним вимогам, але й мати архітектуру, гнучку до змін, адаптації та масштабування. В основі нової ІС повинні бути реалізовані сучасні принципи побудови мережевої інфраструктури: централізація керування, стандартизація протоколів, впровадження механізмів логічної ізоляції трафіку, багаторівневий захист, підтримка віддаленого доступу та інтеграція з хмарними обчисленнями. Крім того, потрібно забезпечити дотримання чинних стандартів з інформаційної безпеки та збереження персональних даних [16].

Основні вимоги до інформаційної системи:

- Підтримка архітектури з централізованим керуванням та моніторингом;
- Сумісність з хмарними сервісами для навчання та зберігання даних;
- Можливість розмежування доступу до ресурсів (VLAN, ACL);

- Висока пропускна здатність магістральних каналів;
- Захист даних відповідно до стандартів ISO/IEC 27001;
- Наявність систем виявлення та реагування на інциденти (IDS/IPS);
- Підтримка мобільного доступу через захищені VPN-з'єднання;
- Автоматизація резервного копіювання;
- Інтеграція з навчальними платформами (Moodle, Google Workspace);
- Підтримка гнучкої масштабованості та резервування.

Проєктування системи має враховувати стандарти IEEE щодо мережевих інтерфейсів, протоколів, а також настанови з архітектури мережевого обладнання. Розробка системи передбачає поділ на функціональні модулі: управління користувачами, управління трафіком, моніторинг, безпека, аналітика, підтримка резервного копіювання, журналювання. Кожен з модулів повинен мати чітке логічне обґрунтування, що буде реалізовано у формі діаграм DFD, UML, ERD тощо. Впровадження нової ІС має базуватися на моделі життєвого циклу інформаційної системи відповідно до ISO/IEC 12207 [17].

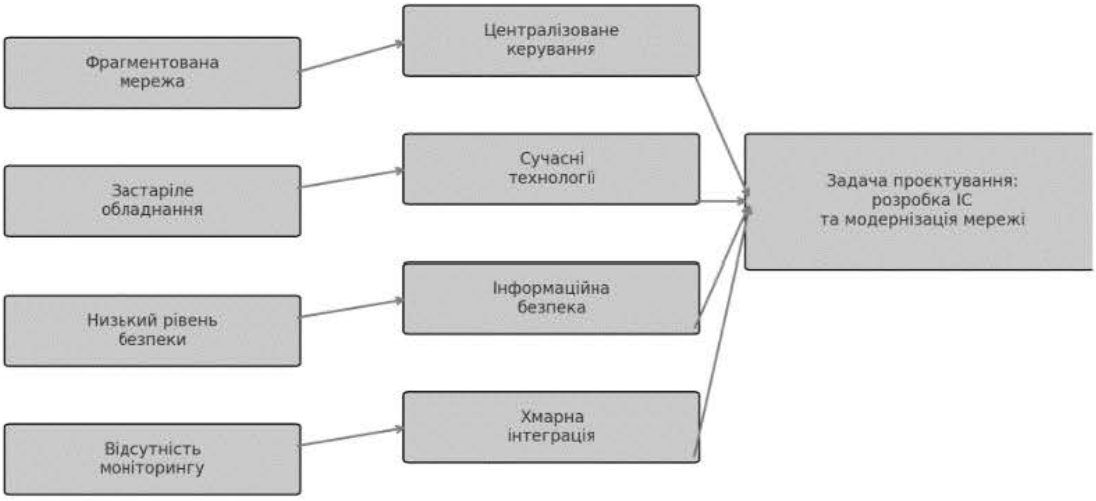

Рисунок 1.3 - Логічна структура взаємозв'язку проблем, вимог

На рисунку 1.3 наведено загальну схему взаємозв'язку основних проблем, вимог і етапів проєктування нової інформаційної системи, що дає змогу візуалізувати логіку переходу від аналізу до реалізації. Як видно, формування

вимог безпосередньо залежить від діагностованих недоліків, а архітектурні рішення – від сформованих технічних і організаційних потреб.

Після формалізації вимог необхідно здійснити постановку задачі проєктування. Вона полягає в розробці логічної, інформаційної та фізичної моделі ІС, яка має забезпечити безперебійну роботу університетської мережі, включаючи централізоване адміністрування, високий рівень безпеки та підтримку сучасних сервісів. До задачі входить розробка схем топології мережі, маршрутизації, системи резервного копіювання, підсистем аутентифікації та логування, а також опис протоколів і механізмів взаємодії між модулями ІС. Реалізація задачі проєктування має завершитися побудовою функціонального прототипу системи у середовищі моделювання Cisco Packet Tracer або GNS3.

Паралельно, варто враховувати нормативні та технічні вимоги, серед яких законодавство України в сфері захисту інформації, вимоги до електронних інформаційних ресурсів та безпеки персональних даних. Це включає Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Закон України «Про інформацію», Закон України «Про освіту» та інші. Проєкт має бути сумісним із програмно-апаратними рішеннями, що вже впроваджені в УМСФ, і повинен бути адаптований до можливостей бюджету та людських ресурсів закладу [18].

Крім виявлених технічних та організаційних недоліків, важливим аспектом, що впливає на функціонування мережевої інфраструктури, є недостатній рівень інтеграції інформаційних систем між собою. В університеті використовується декілька окремих сервісів — для електронного документообігу, управління навчальним процесом, комунікації тощо, однак між ними відсутня повноцінна взаємодія. Це створює складності в обробці даних, дублювання інформації, збільшує навантаження на адміністративний персонал і знижує ефективність прийняття управлінських рішень.

Аналіз сучасних підходів до побудови IT-інфраструктури ЗВО показує, що найбільш ефективними є моделі, що базуються на централізованому управлінні, автоматизації процесів та використанні модульної архітектури. Це дозволяє

забезпечити не лише стабільність і продуктивність, але й адаптивність до змін технологічного середовища та зростання вимог з боку користувачів. У випадку УМСФ така модель має забезпечити оперативне масштабування, швидке впровадження нових сервісів, зменшення часу на адміністрування та підвищення загального рівня безпеки.

Окремо варто підкреслити значення стандартизації на всіх етапах — від побудови фізичної мережі до розгортання прикладного програмного забезпечення. Використання галузевих стандартів (наприклад, ISO/IEC 27001 для безпеки, ISO/IEC 12207 для життєвого циклу ІС, IEEE 802.1Q для VLAN тощо) дозволяє забезпечити сумісність, передбачуваність функціонування системи та полегшує інтеграцію нових компонентів. Відсутність таких стандартів у поточній реалізації мережі є ще одним критичним недоліком, який необхідно усунути в межах нового проєкту.

Таким чином, постановка задачі проєктування інформаційної системи для розвитку інфраструктури комп'ютерної мережі УМСФ є результатом системного аналізу поточного стану та формування реалістичних технічних і функціональних вимог. Вона передбачає побудову моделі, що включає в себе архітектурні, інформаційні та технологічні рішення, а також план поетапного впровадження і модернізації.

1.6. Висновки до першого розділу

У цьому розділі було проведено детальний аналіз існуючої мережевої інфраструктури Університету митної справи та фінансів, що дозволило виявити ключові проблеми, які перешкоджають ефективному функціонуванню інформаційної системи. Серед основних недоліків відзначено фрагментовану мережу, застаріле обладнання, низький рівень безпеки та відсутність централізованого моніторингу. Ці проблеми негативно впливають на стабільність, масштабованість та захищеність системи, що є критичними аспектами для сучасного навчального закладу.

На основі виявлених проблем було сформульовано вимоги до нової інформаційної системи, які включають централізоване керування, використання сучасних технологій, забезпечення інформаційної безпеки та інтеграцію з хмарними сервісами. Ці вимоги спрямовані на створення гнучкої, надійної та безпечної інфраструктури, здатної адаптуватися до змін та забезпечувати потреби користувачів. Врахування цих вимог є необхідним для розробки ефективної та стійкої інформаційної системи.

Постановка задачі проєктування передбачає розробку логічної, інформаційної та фізичної моделі інформаційної системи, яка забезпечить безперебійну роботу мережі університету. Це включає створення схем топології мережі, маршрутизації, систем резервного копіювання, підсистем аутентифікації та логування, а також опис протоколів і механізмів взаємодії між модулями системи. Реалізація задачі проєктування має завершитися побудовою функціонального прототипу системи у середовищі моделювання з подальшим тестуванням запропонованих рішень.

У процесі проєктування необхідно враховувати чинні стандарти та нормативні документи, такі як ISO/IEC 27001:2022, ДСТУ 2627-94 та Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Це забезпечить відповідність системи вимогам інформаційної безпеки та захисту персональних даних. Дотримання цих стандартів є важливим аспектом для забезпечення надійності та довіри до інформаційної системи.

Запропоновані рішення стануть фундаментом для наступного етапу — безпосереднього проєктування інформаційної системи та моделювання її компонентів.

Таким чином, проведений аналіз проблем, формулювання вимог та постановка задачі проєктування створюють основу для розробки сучасної, безпечної та ефективної інформаційної системи Університету митної справи та фінансів. Це дозволить підвищити якість освітнього процесу, забезпечити стабільну роботу мережевої інфраструктури та відповідати сучасним вимогам інформаційного суспільства.

РОЗДІЛ 2. МЕТОДИ ТА ЗАСОБИ МОДЕЛЮВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1. Основи моделювання мережевих інфраструктур

Моделювання мережевих інфраструктур є ключовим етапом у проєктуванні та оптимізації сучасних інформаційно-комунікаційних систем. Цей процес дозволяє створювати віртуальні представлення мережі, що відображають її структуру, функціональні можливості та взаємодію компонентів. Завдяки моделюванню можна передбачити поведінку мережі в різних сценаріях, виявити потенційні вузькі місця та оцінити ефективність запропонованих рішень. Це особливо важливо в умовах постійного зростання вимог до продуктивності, надійності та безпеки мережевих систем [18-21].

Основними цілями моделювання мережевих інфраструктур є:

- Аналіз поточної структури мережі та виявлення її слабких місць.
- Оцінка впливу нових технологій або змін на існуючу інфраструктуру.
- Планування масштабування та оптимізації ресурсів.
- Перевірка безпеки та стійкості мережі до зовнішніх впливів.

Для досягнення цих цілей використовуються різноманітні методи та інструменти моделювання, які дозволяють створювати точні та наочні віртуальні моделі мережевих систем.

Одним із фундаментальних підходів до моделювання є використання еталонної моделі OSI (Open Systems Interconnection), яка розділяє мережеві функції на сім рівнів. Ця модель забезпечує структурований підхід до аналізу та проєктування мереж, дозволяючи розглядати кожен рівень окремо та в контексті взаємодії з іншими рівнями. Зокрема, фізичний рівень відповідає за передачу бітів через фізичні носії, канальний рівень — за встановлення та підтримку з'єднань між пристроями, мережевий рівень — за маршрутизацію пакетів, транспортний рівень — за забезпечення надійної передачі даних, а прикладний рівень — за взаємодію з користувачем та застосунками. Такий підхід дозволяє

детально аналізувати та моделювати кожен аспект мережевої інфраструктури [19,21].

У процесі моделювання важливо враховувати типи мережевих топологій, які визначають спосіб з'єднання пристроїв у мережі. Найпоширенішими є зіркова, шинна, кільцева, деревоподібна та сітчаста топології. Кожна з них має свої переваги та недоліки щодо надійності, вартості та складності реалізації. Наприклад, зіркова топологія забезпечує простоту управління та високий рівень надійності, оскільки вихід з ладу одного пристрою не впливає на інші. Натомість сітчаста топологія забезпечує максимальну відмовостійкість, але є складнішою та дорожчою у реалізації. Вибір топології залежить від конкретних вимог та умов експлуатації мережі [22].

Для ефективного моделювання мережевих інфраструктур використовуються спеціалізовані програмні інструменти (дивитись таблицю 2.1). Серед них варто відзначити такі:

- Cisco Packet Tracer: інструмент для створення віртуальних мережевих топологій, що дозволяє моделювати роботу мережевих пристроїв та протоколів.
- GNS3 (Graphical Network Simulator-3): потужний емулятор мереж, який дозволяє запускати реальні образи операційних систем мережевих пристроїв.
- NetSim: симулятор мереж від компанії Boson, що орієнтований на підготовку до сертифікаційних іспитів та навчання.
- EVE-NG (Emulated Virtual Environment Next Generation): універсальна платформа для моделювання та тестування мережевих інфраструктур.
- IMUNES (Integrated Multiprotocol Network Emulator/Simulator): інструмент для моделювання мереж на основі FreeBSD, що дозволяє створювати складні мережеві сценарії.

Ці інструменти надають широкі можливості для створення, тестування та аналізу мережевих моделей, що сприяє підвищенню якості проєктування та експлуатації мережевих систем [20].

У процесі моделювання важливо враховувати стандарти та рекомендації, які забезпечують сумісність та ефективність мережевих рішень. Серед них варто відзначити стандарти IEEE 802, які регламентують роботу локальних та метрополітенських мереж, а також стандарти ISO/IEC, що визначають загальні принципи побудови та управління мережами. Дотримання цих стандартів забезпечує узгодженість рішень, полегшує інтеграцію різних компонентів та сприяє підвищенню надійності мережевих систем [4].

Постановка задачі моделювання мережевої інфраструктури передбачає визначення цілей, обмежень та критеріїв ефективності майбутньої мережі. Це включає аналіз поточних потреб організації, прогнозування майбутніх вимог, визначення необхідного рівня безпеки, надійності та масштабованості. На основі цих даних формується технічне завдання, яке слугує основою для створення моделі мережі та подальшого її впровадження. Важливо також враховувати бюджетні обмеження та наявні ресурси, що впливають на вибір технологій та рішень.

Узагальнюючи, моделювання мережевих інфраструктур є невід'ємною частиною сучасного проєктування інформаційних систем. Цей процес дозволяє створювати ефективні, надійні та безпечні мережі, що відповідають поточним та майбутнім потребам організацій. Використання сучасних інструментів та дотримання міжнародних стандартів забезпечує високу якість та сумісність мережевих рішень. Таким чином, моделювання є ключовим етапом у забезпеченні успішної реалізації мережевих проєктів.

Таблиця 2.1

Порівняльна характеристика інструментів моделювання мереж

Інструмент	Основні можливості	Переваги	Недоліки
Cisco Packet Tracer	Моделювання мережевих топологій, протоколів	Простота використання, навчальний фокус	Обмежена підтримка реальних ОС
GNS3	Емуляція реальних ОС мережевих пристроїв	Висока гнучкість, підтримка реальних образів	Складність налаштування, вимоги до ресурсів

Продовження таблиці 2.1

NetSim	Підготовка до сертифікацій, моделювання мереж	Інтерактивні лабораторії, навчальні матеріали	Платна ліцензія
EVE-NG	Моделювання складних мережевих сценаріїв	Підтримка різних вендорів, масштабованість	Складність налаштування
IMUNES	Моделювання на основі FreeBSD	Висока продуктивність, відкритий код	Обмежена документація, специфічність

2.2. Види топологій і протоколів передачі даних

У сучасних комп'ютерних мережах топологія визначає фізичне або логічне розташування вузлів та зв'язків між ними. Вибір відповідної топології впливає на ефективність, надійність та масштабованість мережі. Серед основних типів топологій виділяють шинну, зіркоподібну, кільцеву, сітчасту, деревоподібну та гібридну. Кожна з них має свої переваги та недоліки, які слід враховувати при проєктуванні мережевої інфраструктури.

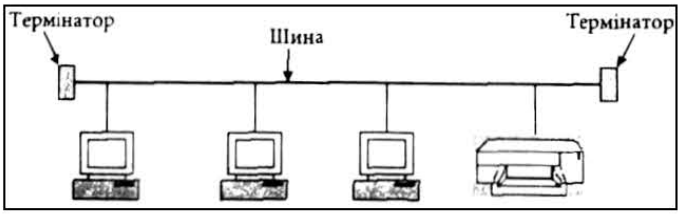

Рисунок 2.1 – Шинна топологія комп'ютерної мережі

Шинна топологія (рисунок 2.1) передбачає підключення всіх пристроїв до єдиного комунікаційного каналу. Вона є простою у реалізації та економічною, однак має обмежену масштабованість і є вразливою до збоїв у центральному каналі. Зіркоподібна топологія, навпаки, забезпечує високу надійність, оскільки кожен вузол підключений до центрального комутатора або маршрутизатора. Проте вихід з ладу центрального елемента призводить до зупинки всієї мережі.

Кільцева топологія (рисунок 2.2) характеризується послідовним з'єднанням вузлів, де кожен пристрій має два сусіди. Дані передаються по колу,

що дозволяє уникнути колізій, але робить мережу вразливою до збоїв у будь-якому з вузлів. Сітчаста топологія забезпечує високу надійність і відмовостійкість завдяки множинним шляхам передачі даних між вузлами. Проте її реалізація є складною та дорогою.

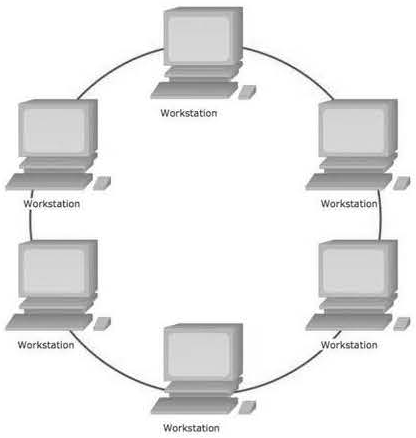

Рисунок 2.2 – Кільцева топологія комп'ютерної мережі

Деревоподібна топологія поєднує властивості зіркоподібної та шинної топологій, утворюючи ієрархічну структуру. Вона дозволяє легко масштабувати мережу, але потребує ретельного планування для уникнення перевантажень у вузлах вищих рівнів. Гібридна топологія об'єднує елементи різних топологій для досягнення оптимального балансу між надійністю, вартістю та продуктивністю.

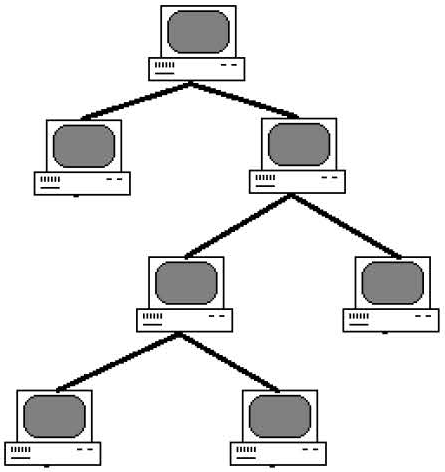

Рисунок 2.3 – Деревоподібна топологія комп'ютерної мережі

Для наочного порівняння основних характеристик різних топологій наведемо таблицю 2.2.

Таблиця 2.2

Порівняння основних мережевих топологій

Топологія	Надійність	Вартість	Масштабованість	Складність реалізації
Шинна	Низька	Низька	Обмежена	Низька
Зіркоподібна	Середня	Середня	Висока	Середня
Кільцева	Середня	Середня	Обмежена	Середня
Сітчаста	Висока	Висока	Висока	Висока
Деревоподібна	Середня	Середня	Висока	Середня
Гібридна	Висока	Висока	Висока	Висока

Передача даних у мережах здійснюється за допомогою різноманітних протоколів, які визначають правила обміну інформацією між пристроями. Ці протоколи організовані за моделлю OSI (Open Systems Interconnection), яка складається з семи рівнів. Кожен рівень виконує специфічні функції, забезпечуючи ефективну та надійну передачу даних [19,21].

На фізичному рівні (Layer 1) визначаються електричні та механічні характеристики інтерфейсів. На канальному рівні (Layer 2) здійснюється передача кадрів між вузлами та контроль помилок. Мережевий рівень (Layer 3) відповідає за маршрутизацію пакетів та логічну адресацію. Транспортний рівень (Layer 4) забезпечує надійну передачу даних між кінцевими точками. Сеансовий (Layer 5), представницький (Layer 6) та прикладний (Layer 7) рівні відповідають за управління сесіями, представлення даних та взаємодію з прикладними програмами відповідно.

Для кращого розуміння функцій кожного рівня моделі OSI наведемо таблицю 2.3.

Таблиця 2.3

Рівні моделі OSI та їх функції

Рівень OSI	Функції
7. Прикладний	Надання інтерфейсу для користувача та прикладних програм
6. Представницький	Форматування, шифрування та стиснення даних

Продовження таблиці 2.3

5. Сеансовий	Управління сесіями зв'язку між прикладними програмами
4. Транспортний	Забезпечення надійної передачі даних, контроль помилок та потоку
3. Мережевий	Маршрутизація пакетів, логічна адресація
2. Канальний	Передача кадрів між вузлами, виявлення та виправлення помилок
1. Фізичний	Визначення фізичних характеристик інтерфейсів та середовища передачі

Серед основних протоколів передачі даних варто виділити TCP (Transmission Control Protocol) та UDP (User Datagram Protocol). TCP забезпечує надійну передачу даних з контролем помилок та підтвердженням отримання, що робить його придатним для застосувань, де важлива цілісність даних, наприклад, веб-браузери або електронна пошта. UDP, навпаки, не гарантує доставку пакетів, але має меншу затримку, що робить його придатним для потокових сервісів, таких як відеоконференції або онлайн-ігри.

Вибір протоколу передачі даних залежить від вимог конкретного застосування. Наприклад, для передачі файлів або електронної пошти доцільно використовувати TCP, тоді як для потокового відео або голосових дзвінків – UDP. Крім того, важливо враховувати характеристики мережі, такі як пропускна здатність, затримка та надійність, при виборі відповідного протоколу.

Таким чином, розуміння різних типів топологій та протоколів передачі даних є ключовим для ефективного проєктування та управління комп'ютерними мережами. Правильний вибір топології та протоколів дозволяє забезпечити надійність, масштабованість та продуктивність мережевої інфраструктури.

2.3. Програмне забезпечення для моделювання та критерії його вибору

У сучасному світі інформаційних технологій моделювання мережевих інфраструктур є невід'ємною частиною навчального процесу та професійної підготовки фахівців. Існує низка програмних засобів, які дозволяють створювати

віртуальні мережі, тестувати конфігурації та аналізувати роботу мереж без необхідності використання фізичного обладнання. Серед таких інструментів можна виділити Cisco Packet Tracer, GNS3, NetSim та інші.

Cisco Packet Tracer — це потужний симулятор мереж, розроблений компанією Cisco для навчальних цілей. Він дозволяє користувачам створювати віртуальні мережеві топології, налаштовувати пристрої та аналізувати їхню взаємодію. Програма підтримує широкий спектр мережевих пристроїв, включаючи маршрутизатори, комутатори, бездротові точки доступу та кінцеві пристрої. Однією з ключових особливостей є можливість симулювати роботу Інтернету речей (IoT) та кібербезпеки, що робить Packet Tracer універсальним інструментом для навчання [23].

GNS3 (Graphical Network Simulator-3) є відкритим програмним забезпеченням, яке дозволяє емітувати реальні мережеві пристрої, використовуючи їхні операційні системи. Це забезпечує більш точну симуляцію порівняно з іншими інструментами, оскільки користувачі можуть працювати з реальними IOS-образами пристроїв. GNS3 підтримує інтеграцію з віртуальними машинами, що дозволяє створювати складні мережеві топології, включаючи сервери та клієнтські системи на різних операційних системах [24].

NetSim від компанії Boson є комерційним симулятором мереж, орієнтованим на підготовку до сертифікаційних іспитів Cisco. Програма надає користувачам можливість працювати з віртуальними маршрутизаторами та комутаторами, підтримуючи різноманітні протоколи маршрутизації, такі як RIP, OSPF, EIGRP та BGP. NetSim також включає в себе інтерактивні лабораторні роботи, які допомагають користувачам закріпити теоретичні знання на практиці [25].

Крім вищезгаданих інструментів, існують й інші програми для моделювання мереж. Наприклад, EVE-NG (Emulated Virtual Environment Next Generation) є потужним інструментом для створення віртуальних мережевих середовищ, який підтримує широкий спектр мережевих пристроїв від різних виробників. Також варто згадати про VirtualBox та VMware Workstation, які, хоча

й не є спеціалізованими мережевими симуляторами, дозволяють створювати віртуальні машини та мережі для тестування різних конфігурацій.

Вибір конкретного програмного забезпечення залежить від цілей користувача. Для початківців та студентів, які тільки починають вивчати мережеві технології, найбільш підходящим є Cisco Packet Tracer завдяки його простоті та інтерактивності. Для більш досвідчених користувачів, які потребують точнішої симуляції та роботи з реальними IOS-образами, оптимальним вибором буде GNS3. NetSim, у свою чергу, є ідеальним інструментом для тих, хто готується до сертифікаційних іспитів Cisco, завдяки інтегрованим лабораторним роботам та підтримці широкого спектру протоколів.

У процесі вибору програмного забезпечення (ПЗ) для моделювання комп'ютерних мереж важливо враховувати низку критеріїв, що забезпечують ефективність та відповідність інструменту до поставлених завдань. Серед основних критеріїв виділяють функціональність, масштабованість, простоту використання, точність моделювання, підтримку різноманітних мережевих сценаріїв та сумісність з іншими системами. Ці аспекти дозволяють обрати ПЗ, яке найкраще відповідає потребам користувача та специфіці проекту [26].

Функціональність ПЗ визначає його здатність підтримувати необхідні мережеві протоколи, типи пристроїв та сценарії. Наприклад, деякі інструменти можуть обмежуватись лише симуляцією пристроїв певного виробника, тоді як інші забезпечують ширшу підтримку. Масштабованість є критичною для великих мережевих проектів, де необхідно моделювати велику кількість вузлів та складні топології. Простота використання впливає на швидкість освоєння інструменту та ефективність роботи з ним [26].

Точність моделювання визначає, наскільки реалістично ПЗ відтворює поведінку мережі. Це особливо важливо для досліджень та тестування нових мережевих рішень. Підтримка різноманітних мережевих сценаріїв дозволяє моделювати як стандартні, так і специфічні ситуації, включаючи збої, перевантаження та атаки. Сумісність з іншими системами забезпечує інтеграцію

ПЗ у вже існуючу інфраструктуру та використання додаткових інструментів для аналізу та візуалізації даних.

Для зручності порівняння різних програмних засобів доцільно використовувати таблицю 2.4, яка відображає відповідність кожного інструменту зазначеним критеріям. Це дозволяє швидко оцінити переваги та недоліки кожного варіанту та зробити обґрунтований вибір.

Таблиця 2.4

Порівняння програмного забезпечення для моделювання мереж

Критерій	Cisco Packet Tracer	GNS3	NetSim
Функціональність	Висока	Дуже висока	Висока
Масштабованість	Середня	Висока	Середня
Простота використання	Висока	Середня	Висока
Точність моделювання	Середня	Висока	Висока
Підтримка сценаріїв	Середня	Висока	Висока
Сумісність	Середня	Висока	Середня

Вибір ПЗ також залежить від специфіки завдань та рівня підготовки користувача. Для початківців рекомендується використовувати інструменти з високою простотою використання, такі як Cisco Packet Tracer. Досвідчені користувачі можуть обрати GNS3 або NetSim, які забезпечують вищу точність моделювання та підтримку складних сценаріїв.

Крім того, важливо враховувати наявність документації, спільноти користувачів та технічної підтримки. Ці фактори сприяють швидкому вирішенню проблем та ефективному використанню ПЗ. Наявність активної спільноти дозволяє обмінюватися досвідом та отримувати поради від інших користувачів.

2.5. Порівняльний аналіз інструментів моделювання

У сучасному світі мережевих технологій існує безліч інструментів для моделювання комп'ютерних мереж, серед яких особливо виділяються Cisco Packet Tracer, GNS3 та Boson NetSim. Кожен з них має свої унікальні особливості,

переваги та обмеження, що визначають їхню придатність для різних категорій користувачів. Ретельний аналіз цих інструментів дозволяє обрати найбільш відповідний варіант для конкретних освітніх або професійних потреб.

ITU Online IT Training

Cisco Packet Tracer є офіційним симулятором від компанії Cisco, призначеним переважно для навчання студентів та підготовки до сертифікаційних іспитів. Його простий інтерфейс та інтеграція з навчальними курсами роблять його ідеальним для початківців. Однак, цей інструмент має обмежену функціональність щодо емуляції реального мережевого обладнання та підтримує лише пристрої Cisco, що може бути недоліком для більш глибокого вивчення мережевих технологій [1].

GNS3, або Graphical Network Simulator-3, є потужним емулятором, який дозволяє створювати складні мережеві топології з використанням реальних образів операційних систем мережевих пристроїв. Це робить його незамінним інструментом для професіоналів та тих, хто готується до сертифікацій CCNP або CCIE. Проте, GNS3 вимагає більше ресурсів комп'ютера та має складніший процес налаштування, що може бути викликом для новачків [2].

Boson NetSim є комерційним продуктом, орієнтованим на підготовку до сертифікаційних іспитів Cisco. Він пропонує велику кількість попередньо налаштованих лабораторних робіт та сценаріїв, що дозволяє ефективно відпрацьовувати практичні навички. Однак, висока вартість ліцензії може бути перешкодою для деяких користувачів, особливо студентів.

Порівнюючи ці інструменти, можна виділити наступні ключові аспекти:

- Призначення: Packet Tracer – для початківців; GNS3 – для професіоналів; NetSim – для підготовки до сертифікацій.
- Функціональність: Packet Tracer має обмежену функціональність; GNS3 дозволяє емуляцію реальних пристроїв; NetSim пропонує готові лабораторні роботи.
- Вимоги до ресурсів: Packet Tracer є легким; GNS3 вимагає більше ресурсів; NetSim має середні вимоги.

– Вартість: Packet Tracer є безкоштовним; GNS3 – безкоштовний з відкритим кодом; NetSim – комерційний продукт.

EVE-NG (Emulated Virtual Environment – Next Generation) поєднує в одному середовищі можливості емуляції та симуляції, підтримуючи образи Cisco, Juniper, MikroTik та багатьох інших виробників. Це універсальне рішення для мультивендорного тестування складних топологій, а Web-інтерфейс і можливість хмарного розгортання дозволяють організувати командну лабораторію.

Cisco VIRL (Virtual Internet Routing Lab) — офіційний емулятор Cisco, що використовує образи IOS, IOS-XE, NX-OS. Він підходить для професійного тестування мережевих архітектур і проведення performance-тестів, але вимагає окремої ліцензії та потужного сервера для розгортання.

Інтеграція з DevOps-інструментами стала новим стандартом: GNS3 та EVE-NG підтримують автоматичне розгортання топологій через Ansible чи Terraform, що дає змогу включати мережеві лабораторії в CI/CD-конвеєри. Packet Tracer та NetSim таких можливостей майже не надають.

Рівень підтримки й активність спільноти також критичні: GNS3 має великий форум та сторонні доповнення, EVE-NG розвивається як open-source із плагінами, а Boson NetSim пропонує офіційну техпідтримку, але з обмеженою документацією. Cisco Packet Tracer надає доступ до сценаріїв NetAcad, проте не дуже гнучкий для самостійного розширення. При виборі інструменту враховуйте масштаб лабораторії: для великих груп або корпоративних тренінгів краще підходять серверні/хмарні рішення (EVE-NG Pro, VIRL), а для індивідуальних занять і невеликих класів — десктопні клієнти (Packet Tracer, NetSim).

Вибір між цими інструментами залежить від конкретних потреб користувача. Для студентів та початківців ідеальним вибором буде Cisco Packet Tracer завдяки його простоті та інтеграції з навчальними матеріалами. Професіонали, які потребують більш глибокого занурення в мережеві технології, оцінять можливості GNS3. Ті, хто готується до сертифікаційних іспитів, можуть скористатися перевагами Boson NetSim, незважаючи на його вартість.

Таким чином, кожен з розглянутих інструментів має свої унікальні переваги та обмеження. Ретельний аналіз їхніх характеристик дозволяє зробити обґрунтований вибір, що відповідає індивідуальним потребам та цілям користувача.

2.6. Висновки до другого розділу

У другому розділі дипломної роботи було проведено комплексний аналіз топологій комп'ютерних мереж, протоколів передачі даних, а також програмного забезпечення для моделювання мережевих структур. Цей аналіз дозволив визначити ключові аспекти, що впливають на ефективність побудови та функціонування мереж, а також на вибір відповідних інструментів для їх моделювання. Розгляд різних видів топологій, таких як шинна, зіркоподібна, кільцева, деревоподібна та сітчаста, показав, що кожна з них має свої переваги та недоліки. Наприклад, зіркоподібна топологія забезпечує високу надійність, але вимагає значних витрат на кабелювання, тоді як сітчаста топологія гарантує максимальну відмовостійкість, проте є складною у реалізації та обслуговуванні.

Аналіз протоколів передачі даних, зокрема TCP/IP, UDP, HTTP, FTP та інших, дозволив зрозуміти їхню роль у забезпеченні надійної та ефективної комунікації в мережах. Зокрема, TCP забезпечує надійну доставку даних з контролем помилок, тоді як UDP дозволяє передавати дані з мінімальною затримкою, що є критичним для реального часу.

У підрозділі 2.3 було проведено огляд програмного забезпечення для моделювання мереж, таких як Cisco Packet Tracer, GNS3, Boson NetSim та інших. Кожен з цих інструментів має свої особливості: Packet Tracer є зручним для початківців, GNS3 дозволяє емулювати реальні мережеві пристрої, а NetSim пропонує готові лабораторні завдання для підготовки до сертифікаційних іспитів.

Підрозділ 2.4 був присвячений критеріям вибору програмного забезпечення для моделювання. Серед основних критеріїв були визначені

функціональні можливості, сумісність з реальними пристроями, вимоги до апаратного забезпечення, вартість та наявність навчальних матеріалів. Ці критерії є ключовими при виборі інструменту для конкретних навчальних або професійних потреб.

У підрозділі 2.5 було проведено порівняльний аналіз інструментів моделювання. Зокрема, було виявлено, що Cisco Packet Tracer є оптимальним для початкового рівня навчання, GNS3 підходить для більш глибокого вивчення та підготовки до сертифікацій CCNP/CCIE, а Boson NetSim є ефективним для структурованої підготовки до іспитів.

Одним із ключових аспектів є валідація обраної топології через моделювання відмовостійкості. Під час проєктування мережі слід імітувати вихід вузлів із ладу та оцінювати, як різні топології—наприклад, сітчаста, деревоподібна чи змішана—реагують на втрату лінків. Таке моделювання дозволяє порівняти час перезапуску маршрутів, обчислити резервні шляхи й обрати оптимальний баланс між вартістю та надійністю.

Не менш важливим є аналіз протоколів маршрутизації в умовах реальної завантаженості каналів. Моделювання з використанням OSPF, EIGRP чи RIP допомагає відтворити поведінку мережі при зміні трафікових патернів і оцінити, який протокол забезпечує найменшу затримку та найменшу кількість оновлень таблиці маршрутизації. Експерименти з параметрами таймаутів і метрик дозволяють знайти компроміс між швидкістю конвергенції та навантаженням на процесори маршрутизаторів.

При моделюванні важливий рівень деталізації: на фізичному шарі слід враховувати параметри середовища (дебаланс кабелів, перешкоди, відстані), а на канальному — механізми повторної передачі та управління доступом. Симуляція IEEE 802.3/802.11 дозволяє оцінити, як кількість колізій чи втрачених кадрів впливає на загальну пропускну здатність, а також перевірити ефективність алгоритмів QoS у пріоритетизації VoIP чи відеотрафіку.

Ключовою частиною моделювання є побудова сценаріїв із навантаженням, що відображають пікові години та нетипові ситуації (DDos-імітація, одночасні

VPN-з'єднання). Завдяки цьому можна прогнозувати, які вузькі місця виникнуть у магістральних лінках і вузлах агрегації, і заздалегідь спланувати резервування або масштабування. Результати таких сценаріїв дають змогу сформувати рекомендації з розширення каналів та оптимізації конфігурацій.

Ще один важливий аспект моделювання полягає в тестуванні різних схем балансування навантаження на транспортному та мережевому рівнях. Імітація алгоритмів ECMP (Equal-Cost Multi-Path) або застосування протоколу BGP з локальними префіксами дозволяє оцінити швидкість перемикання в разі відмови та рівномірність розподілу потоку даних. Моделювання таких сценаріїв допомагає виявити потенційні "гарячі" лінки й оптимізувати політики маршрутизації, що особливо актуально для магістральних вузлів університету з великою кількістю одночасних підключень.

При оцінці безпеки мережі важливо моделювати поведінку протоколів безпеки, зокрема IPsec і TLS, з урахуванням витрат на шифрування/дешифрування та впливу на затримки. Експериментальна симуляція дозволяє визначити, чи доцільно застосовувати апаратні криптомодулі, або достатньо програмних механізмів. Це особливо актуально для віддалених підрозділів, де обмежені обчислювальні ресурси впливають на вибір методів захисту.

Нарешті, поєднання різних методів моделювання (дискретно-подійного, фізичного рівня та трафікового) забезпечує комплексну оцінку мережі. Такий підхід дозволяє не лише спроектувати ефективні топології та протоколи, але й передбачити їхню поведінку в умовах масштабування та змін бізнес-вимог. Включення результатів цих досліджень до проєктної документації підвищує впевненість у стабільності та безпеці майбутньої системи.

Загалом, результати аналізу свідчать про те, що вибір топології, протоколів та програмного забезпечення для моделювання має базуватися на конкретних цілях, ресурсах та рівні підготовки користувача. Правильний вибір цих компонентів забезпечує ефективне навчання, дослідження та впровадження мережевих рішень.

РОЗДІЛ 3. ПРОЄКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ РОЗВИТКУ ІНФРАСТРУКТУРИ КОМП'ЮТЕРНОЇ МЕРЕЖІ УМСФ

3.1. Узагальнення вимог та вибір архітектури

Розділення вимог до інформаційної системи на технічні, функціональні та нефункціональні є базовим кроком для впорядкованого проєктування. Такий підхід дозволяє поетапно вирішувати завдання: спочатку забезпечити необхідну інфраструктуру, потім реалізувати бізнес-логіку, а на завершальному етапі — підтвердити показники якості. В результаті отримуємо чіткий перелік очікуваних можливостей, що простежується від рівня обладнання до характеристик інтерфейсу. Далі кожна група вимог розкрито детальніше за допомогою описових абзаців та зведеної таблиці. Це створює основу для прийняття технічних рішень та вибору інструментів.

Технічні вимоги до мережевої інфраструктури передбачають централізоване адміністрування та моніторинг усіх елементів через єдину консоль управління. Система має підтримувати масштабування за допомогою VLAN, що дозволить логічно ізолювати сегменти користувачів та ресурсів. Пропускна здатність магістральних каналів повинна становити не менше 10 Гбіт/с, а підроздільні з'єднання — мінімум 1 Гбіт/с, щоб задовольнити потреби високошвидкісного трафіку. Забезпечення бездротового покриття на базі стандарту Wi-Fi 6 гарантує стабільне підключення в усіх навчальних корпусах та гуртожитках. Інтеграція з хмарними платформами вимагає наявності VPN-шлюзів для безпечного доступу до Google Workspace і Microsoft 365.

Функціональні вимоги описують, що саме повинна вміти система: насамперед автоматичну інвентаризацію всіх підключених пристроїв із фіксацією моделей, MAC- і IP-адрес. Рольова модель доступу має бути реалізована через 802.1X із двофакторною аутентифікацією, щоб різні категорії користувачів бачили лише дозволені сервіси. Моніторинг подій передбачає збір логів у централізованому сховищі та налаштування алертів на основі виявлених

аномалій. Для захисту даних необхідно впровадити планове та за потреби аварійне резервне копіювання, яке здійснюватиметься як на локальні сервери, так і в хмару. Віддалений доступ забезпечується через SSL-VPN із підтримкою сучасних протоколів шифрування.

Нефункціональні вимоги акцентують увагу на якості системи: загальна доступність інфраструктури має перевищувати 99,9 % протягом місяця, а збій критичних сервісів — бути максимально рідкісним завдяки кластеризації серверів. Інтерфейс консолі адміністрування повинен реагувати на дії користувача за часом, не довшим за 2 с при навантаженні до 1 000 одночасних підключень. Канали зв'язку шифруються на рівні TLS 1.3 відповідно до вимог ISO/IEC 27001. Система має легко розширюватися — додавання нових модулів або інтеграцій не повинно вимагати значного перепроєктування архітектури. Нарешті, юзабіліті передбачає інтуїтивно зрозумілу веб-панель з докладною документацією та контекстними підказками.

Усі вимоги зведені до таблиці 3.1.

Таблиця 3.1

Основі вимоги до інформаційної системи

Категорія	Основні пункти
Технічні	Централізація, VLAN, 10 Гбіт/с, Wi-Fi 6, VPN-шлюзи
Функціональні	Інвентаризація пристроїв, 802.1X + 2FA, моніторинг/алертинг, резервне копіювання, SSL-VPN
Нефункціональні	99,9 % Uptime, < 2 с реакції, TLS 1.3, ISO 27001, модульність, інтуїтивність

Інтеграція всіх вимог передбачає тісну взаємодію між командами мережевих інженерів, розробників та аналітиків безпеки. Технічні рішення закладають фундамент, функціональна частина формує серцевину бізнес-логіки, а нефункціональні характеристики гарантують належну якість та відповідність стандартам. У наступних підрозділах буде наведено детальну архітектуру, алгоритми взаємодії модулів та схеми реалізації кожної із згаданих вимог.

Крім того, система повинна передбачати організацію технічної підтримки і супроводу, що включає моніторинг оновлень програмного забезпечення, відстеження версій мережевого обладнання та забезпечення сумісності компонентів. Необхідно впровадити автоматизовану систему розгортання патчів та оновлень із можливістю відкату до попередніх версій у разі виникнення помилок. Документація з експлуатації та адміністрування має підтримуватися в актуальному стані й бути доступною через централізований портал знань. Важливо передбачити навчання персоналу — як мережевих інженерів, так і кінцевих користувачів — для швидкого опанування нових функцій та процедур безпеки. Такий підхід гарантує, що система залишатиметься актуальною, стабільною та захищеною протягом усього життєвого циклу.

Архітектура інформаційної системи визначає спосіб взаємодії між користувачами, бізнес-логікою та сховищем даних, тому її вибір є ключовим етапом проектування. Для систем управління та моніторингу мережі УМСФ оптимальною виявилася комбінована трирівнева клієнт-серверна архітектура з мікросервісним підходом. Така схема поєднує простоту розгортання трьох шарів із гнучкістю та незалежністю обслуговування окремих компонентів за допомогою мікросервісів. Вона дозволяє чітко розділити функціональні зони: інтерфейс користувача, обробку логіки та збереження даних. Завдяки цьому знижується взаємозв'язок модулів і спрощується підтримка всієї системи.

Перший рівень — Presentation Layer — відповідає за взаємодію з адміністраторами та користувачами. Веб-інтерфейс або десктоп-клієнт реалізується через SPA-додаток (наприклад, React/Vue), що звертається до API-шлюзу. Це забезпечує швидкий доступ до консолі управління, перегляд карт мережі, журналів та аналітики. Розділення UI від бізнес-логіки дозволяє легко оновлювати зовнішній вигляд без втручання в ядро системи. Крім того, вбудовані механізми кешування та асинхронні запити зменшують навантаження на сервери.

Другий рівень — Application Layer — реалізовано у вигляді набору мікросервісів, кожен із яких відповідає за окрему підсистему: моніторинг,

керування доступом, резервне копіювання, аутентифікацію тощо. Кожний сервіс пакується в контейнер (Docker) і розгортається в оркестраторі (Kubernetes), що дає змогу незалежно масштабувати компоненти. Мікросервісний підхід спрощує розробку та тестування: окремі команди можуть працювати над своїми сервісами без ризику «зламати» всю систему. З'єднання між сервісами відбувається через стандартизовані REST- або gRPC-інтерфейси з вбудованим балансуванням навантаження. Це гарантує високу готовність (High Availability) та відмовостійкість. Третій рівень — Data Layer — зосереджено на збереженні та обробці інформації. Для структурованих даних (налаштування мережі, користувачі, права доступу) використовується реляційна СУБД (PostgreSQL), а для логів і часових рядів — спеціалізоване сховище (Elasticsearch, InfluxDB). Така комбінація дає змогу оптимізувати запити для різних типів навантаження: аналітичних, транзакційних і пошукових. Розподілене сховище забезпечує горизонтальне масштабування і резервне копіювання на рівні блоків або шардій. Усі під'єднання між рівнями шифруються протоколом TLS.

Запровадження API-шлюзу (API Gateway) між Presentation і Application layers дає змогу централізовано керувати маршрутизацією, аутентифікацією та обмеженням швидкості (rate limiting). Крім того, через нього організується моніторинг викликів та генерація метрик роботи сервісів. Конфігурація gateway може змінюватися без оновлення клієнтських та бекендових мікросервісів. Це суттєво спрощує розгортання нових версій та додавання сторонніх інтеграційних модулів (наприклад, з хмарними сервісами).

Обраний підхід забезпечує гнучкість та масштабованість:

- Контейнери дозволяють швидко розгортати та оновлювати окремі частини без простоїв.
- Горизонтальне масштабування сервісів і сховищ відповідає зростанню навантаження.
- Мікросервісна організація полегшує розподіл завдань між командами та оновлення функцій.

Таким чином, комбінована трирівнева та мікросервісна архітектура оптимально відповідає вимогам УМСФ щодо гнучкості, масштабованості та безпеки, а також спрощує подальший розвиток та підтримку системи.

3.2. Логічне та інформаційне моделювання системи

Під час проєктування інформаційної системи для розвитку інфраструктури комп'ютерної мережі УМСФ особливу увагу приділено логічному моделюванню, яке дозволяє формалізувати потоки даних, функціональні процеси та взаємодію користувачів із системою. Використання DFD, IDEF0 та UML-діаграм забезпечує багаторівневий підхід до опису системи: від загального контексту до детальної розкладки функцій та об'єктів. Така послідовність моделювання сприяє чіткому розумінню вимог замовника, полегшує виявлення вузьких місць та дозволяє уникнути двозначностей на етапі реалізації.

Рисунок 3.1 – DFD (контекстна діаграма, рівень 0)

DFD-діаграми (Data Flow Diagram) призначені для наочного зображення потоків даних між процесами, сховищами та зовнішніми сутностями. Вони допомагають чітко розмежувати межі системи, відобразити основні функції та зрозуміти, як інформація рухається всередині проєкту.

Розглянемо спочатку контекстну DFD-діаграму (Рисунок 3.1), яка відображає взаємодію користувачів, адміністратора та зовнішніх систем із проєктованою інформаційною системою.

На цьому рівні визначено основні потоки даних: запити на авторизацію, запити до бази даних, логи подій та результати обробки. Контекстна діаграма дозволяє чітко окреслити межі системи, ідентифікувати зовнішні елементи та напрямки обміну даними. Відповідно до стандартів, такий опис є першим етапом формування логічної структури системи. Після цього етапу, наступним кроком є деталізація системи до наступних рівнів DFD-діаграм (рівень 1) де кожен процес розбивається на підпроцеси, а також визначення сховищ даних та їхніх взаємозв'язків.

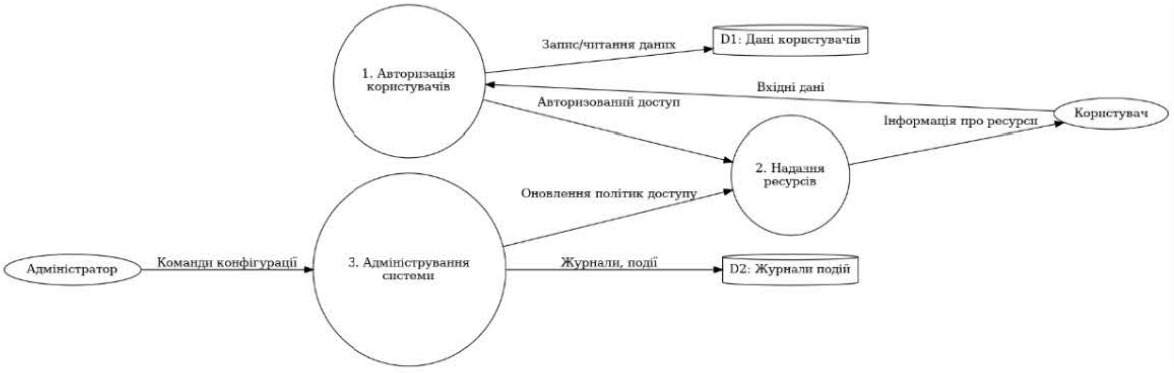

Рисунок 3.2 – DFD (діаграма рівня 1)

Декомпозиція основних процесів представлена на DFD-діаграмі рівня 1 (Рисунок 3.2), яка деталізує внутрішні підсистеми: авторизацію, доступ до ресурсів, адміністрування та логування.

Кожен із цих процесів розбито на окремі підпроцеси, що уточнюють, які дані та в якому напрямку переміщуються між ними. Це дозволяє розробникам і тестувальникам одразу бачити, які входи необхідні для кожного функціонального модуля та які виходи він формує. Такий підхід відповідає міжнародним стандартам моделювання інформаційних систем .

Для формалізації функцій системи застосовано метод IDEF0, який дає можливість уніфіковано описати зв’язки між процесами, їх вхідними та керуючими даними, механізмами та виходами. На діаграмі верхнього рівня A-0 показано загальну функцію «Керування мережею УМСФ», яка розкладається на дрібніші блоки. Такий підхід дозволяє одночасно аналізувати методи організації функціонування та визначати необхідні механізми реалізації.

На наступному рівні IDEF0 наведено п’ять ключових блоків (Рисунки А.1–А.5):

Авторизація користувачів (Рисунок А.1) – опис процесу введення облікових даних, перевірки прав за керуючими політиками, генерації та передачі вихідних токенів доступу для подальших запитів.

Доступ до ресурсів (Рисунок А.2) – ілюструє механізми перевірки прав та видачі необхідних ресурсів.

Кожен блок містить чіткий опис входів (credentials, запит), механізмів (модулі перевірки) та виходів (результат авторизації, доступ). Це забезпечує прозорість у визначенні зон відповідальності та дає змогу легко оновлювати політики доступу.

Блок Адміністрування системи (Рисунок А.3) і Моніторинг та логування (Рисунок А.4) охоплюють процеси управління обліковими записами, налаштування мережевих компонентів, а також фіксації всіх подій у системі.

Адміністрування спирається на механізми конфігурації та збереження налаштувань, а моніторинг – на збір телеметрії та подій, які передаються до централізованої ШЕМ (Системи Екстреного Моніторингу). Такий опис дозволяє гарантувати відповідність вимогам безпеки та швидко реагувати на інциденти.

Окремий блок Резервне копіювання даних (Рисунок А.5) деталізує входи (дані, політики збереження), механізми (скрипти, програми) та виходи (архіви, журнали процесу). Це є критичним елементом для забезпечення стійкості та відновлення інформаційної системи в разі збоїв. Повна візуалізація процесу резервування відповідає кращим практикам управління даними у ВНЗ.

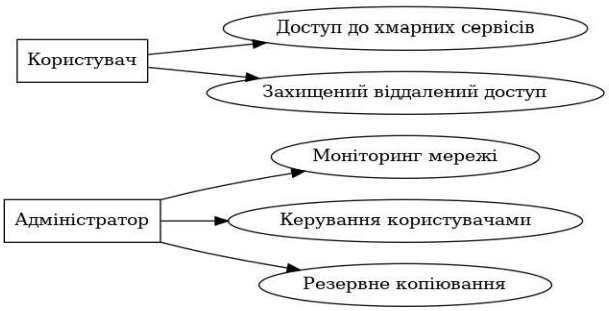

Рисунок 3.3 – UML-діаграма прецедентів

Для моделювання структури об’єктів та динаміки взаємодії застосовано UML. UML-діаграма прецедентів (Рисунок 3.3) відображає двох основних акторів – адміністратора та користувача – та їх можливості: керування акаунтами, моніторинг, доступ до хмарних сервісів і запуск VPN-з’єднання.

Ця діаграма дозволяє чітко окреслити функціональні вимоги з точки зору кінцевих користувачів та задає основу для розробки інтерфейсів та сценаріїв тестування.

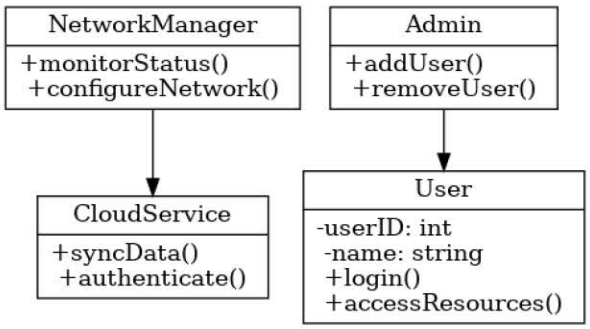

Рисунок 3.4 – UML-діаграма класів

UML-діаграма класів (Рисунок 3.4) демонструє ключові класи: User, Admin, NetworkManager, CloudService та їхні атрибути й методи.

Наслідування Admin від User забезпечує повторне використання коду, а клас NetworkManager зв’язує внутрішні модулі конфігурації з зовнішніми сервісами через CloudService. Така схема визначає основу для об’єктно-орієнтованої реалізації системи.

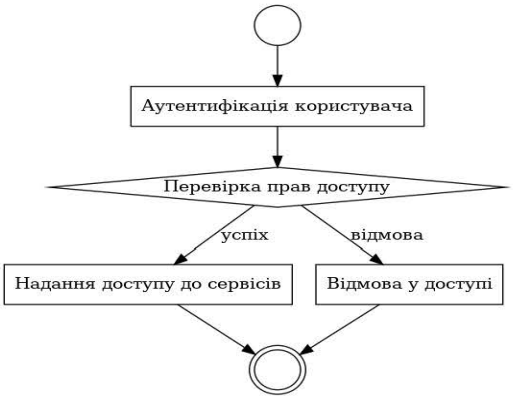

Рисунок 3.5 – UML-діаграма діяльності

UML-діаграма діяльності (Рисунок 3.5) відтворює послідовність дій користувача: від аутентифікації до доступу або відмови у доступі, що дозволяє візуалізувати алгоритміку обробки запитів.

Вона розкриває логіку перевірки прав, формування сеансу та переходу до відповідного сервісу. Такий опис є важливою основою для подальшого кодування та налаштування механізмів обробки винятків.

У результаті побудовані моделі DFD, IDEF0 і UML забезпечують повний логічний опис інформаційної системи, що сприяє узгодженню вимог між замовником, аналітиками та розробниками. Це гарантує цілісність архітектури, чіткість функціональних та нефункціональних вимог, а також полегшує подальшу підтримку й розвиток системи.

А для побудови інформаційної моделі системи було застосовано методологію ER-діаграм, що дозволяє формалізувати структуру бази даних та забезпечити цілісність інформації. Початковим кроком стало визначення ключових сутностей, які безпосередньо використовуються в процесах адміністрування та моніторингу мережі: Користувач, Пристрій, Сесія, Логи, Події та VLAN. Кожна з цих сутностей отримала набір атрибутів, що відображають її характеристики й забезпечують можливість подальшої аналітики. Первинні ключі (PK) гарантують унікальність записів, а зовнішні ключі (FK) — коректні зв'язки між таблицями.

Сутність Користувач (User) містить такі атрибути: id PK, username, email та role. Вона зв'язується із сутністю Сесія співвідношенням 1:∞ — один користувач може мати багато активних чи завершених сесій. Таким чином реалізується можливість історичного аналізу вхідних сесій, а також контролю прав доступу для кожного акаунта. Це відповідає вимогам безпеки та надає гнучкість у адмініструванні користувачів.

Сутність Пристрій (Device) описується атрибутами id PK, mac_address, ip_address і device_type. Кожен пристрій може бути джерелом численних сесій (1:∞), що дозволяє відстежувати активність окремого мережевого обладнання в часі. Такий зв'язок дає змогу аналізувати продуктивність пристрою та виявляти

аномалії в з'єднаннях. Крім того, усі пристрої можуть належати до різних VLAN, що реалізовано через асоціативну таблицю Device_VLAN.

Сутність Сесія (Session) включає id PK, зовнішні ключі user_id FK і device_id FK, а також часові мітки start_time і end_time. Сесії є центральним елементом моделі: через них відбувається зв'язок із сутностями Логи (Log) та Події (Event) співвідношенням 1:∞. Кожна сесія може породжувати численні журнали подій та записи логів, що дозволяє деталізувати діагностику роботи мережі. Реалізація такої структури дає змогу зберігати історію активностей та швидко знаходити відповіді на запити аналітиків.

Сутності Логи (Log) та Події (Event) дистинктно розділені для оптимізації зберігання та фільтрації даних. Log містить id PK, session_id FK, timestamp і message, тоді як Event — id PK, event_type, timestamp та description. Це дозволяє відокремлено аналізувати системні повідомлення й події високого рівня (наприклад, помилки або критичні сповіщення). Такий поділ спрощує масштабування таблиць та підвищує швидкість запитів до них.

Сутність VLAN охоплює id PK, vlan_id, name та subnet. Оскільки один пристрій може належати до кількох VLAN і навпаки, між Device і VLAN встановлено зв'язок багато-до-багатьох через проміжну таблицю Device_VLAN з атрибутами device_id FK та vlan_id FK. Це рішення забезпечує гнучке управління сегментацією мережі та дозволяє динамічно додавати або видаляти пристрої віртуальних мереж.

На рисунку Б.1 наведено повну ER-діаграму, що відображає всі сутності, їх атрибути та типи зв'язків.

3.3. Побудова загальної схеми мережної інфраструктури

Проєктуючи загальну схему мережної інфраструктури, спиралися на результати SWOT-аналізу див. табл. 1.4 та функціональні вимоги до системи. Відповідно до виявлених сильних сторін та можливостей університетської мережі передбачено чіткий поділ на серверний та користувацький сегменти з

урахуванням безпеки й надійності обміну даними. Використання VLAN дозволяє ізолювати різні групи користувачів і мінімізувати ризики несанкціонованого доступу. У серці інфраструктури розташовано ядро комутації, яке взаємодіє з маршрутизатором, що реалізує NAT, VPN та функції фаєрволу.

Серверний сегмент включає три основні сервери: керуючий (Controller), файловий (FileServer) та DNS/DHCP. Керуючий сервер відповідає за централізовану конфігурацію та моніторинг мережі, файловий — за зберігання та розподіл спільних ресурсів, а DNS/DHCP — за автоматичну видачу IP-адрес та переведення доменних імен. Всі сервери підключено до ядра комутації по високошвидкісних оптичних або гігабітних лінках для забезпечення низької затримки та високої пропускної здатності.

Користувацький сегмент поділено на два VLAN: для навчальних аудиторій (VLAN 10) та гуртожитків (VLAN 20). Навчальні аудиторії мають виділені комутатори доступу, а гуртожитки — окремий пул портів, що дозволяє адмініструвати політики QoS та безпеки індивідуально для кожного сегмента. Кожен VLAN маркується на трасах ядра через 802.1Q, що гарантує коректне розмежування трафіку.

Для доступу пристроїв кінцевих користувачів передбачено бездротові точки доступу стандарту IEEE 802.11ax. Точки доступу підключено до ядра комутації через trunk-порт із підтримкою VLAN-тегування. Це забезпечує єдину управлінську площину для контролю параметрів Wi-Fi, а також можливість відокремити трафік аудиторій і гуртожитків на рівні бездротової мережі.

Маршрутизатор виконує функції маршрутизації між внутрішніми VLAN та зовнішньою мережею Internet, реалізує NAT для приватних адресних просторів та підтримує VPN-тунелі для захищеного віддаленого доступу адміністраторів. Вбудований фаєрвол контролює політики доступу, блокуючи небажаний трафік на прикордонному рівні. Це рішення відповідає принципам безпеки та дозволяє оперативно впроваджувати нові правила захисту.

Нижче наведено загальну схему мережевої інфраструктури (Рисунок 3.6), що ілюструє розташування серверного сегмента, ядра комутації, користувацьких

VLAN, точок доступу, комутаторів і маршрутизатора з відповідними стандартами та сервісами.

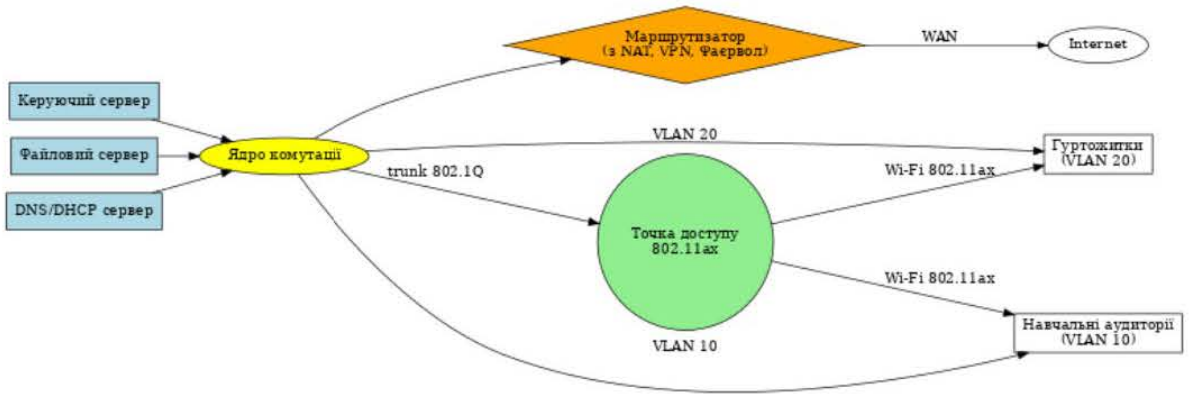

Рисунок 3.6 – Загальна схема мережевої інфраструктури

3.4. Розробка підсистем інформаційної системи

Підсистема керування забезпечує централізоване адміністрування мережі через єдиний веб-інтерфейс з інтуїтивно зрозумілою панеллю навігації. Інтерфейс дозволяє створювати та редагувати політики безпеки, налаштування VLAN, а також переглядати стан ключових компонентів: серверів, комутаторів, точок доступу. Вбудовані механізми кешування та асинхронного завантаження даних гарантують швидкодію навіть при великій кількості пристроїв. Для відображення інформації використано адаптивний дизайн, що дозволяє працювати як з десктоп-версією, так і з мобільними пристроями.

Рольова модель доступу у підсистемі керування реалізована через багаторівневу систему прав, де кожному користувачеві призначається одна або кілька ролей: адміністратор, оператор моніторингу, мережевий інженер. Кожна роль має власний набір прав — від перегляду статистики до зміни конфігурації. Завдяки цьому забезпечується принцип найменших привілеїв (PoLP), що мінімізує ризики несанкціонованих змін. Додатково впроваджено механізм аудиту дій, який фіксує всі спроби входу й виконані в інтерфейсі операції.

Підсистема моніторингу ґрунтується на інтеграції двох інструментів: Zabbix для гнучкого контролю метрик та PRTG для швидкого візуального аналізу мережевих показників. Zabbix відповідає за збір даних про завантаження CPU, пам'яті, дискових підсистем та мережевого трафіку, а PRTG — за побудову дашбордів із графіками та оповіщеннями. До підсистеми інтегровано журналювання подій у централізовану базу даних, де зберігаються всі попередження, помилки та інформаційні повідомлення. Завдяки налаштованим алертам оператор отримує сповіщення про перевищення порогів або недоступність важливих сервісів.

Журналювання подій реалізовано на двох рівнях: локальному (на самих пристроях) і центральному (у SIEM-системі). Кожен запис містить часову мітку, ідентифікатор джерела, рівень важливості та текст повідомлення. Це дозволяє не лише відстежувати поточні інциденти, а й проводити кореляційний аналіз подій за довільні проміжки часу. Система алертів робить можливим миттєве інформування ключових відповідальних осіб через SMS, e-mail або месенджери.

Підсистема захисту доступу передбачає контроль локальних підключень за допомогою IEEE 802.1X із сервером RADIUS для аутентифікації. Кожний користувач або пристрій повинен пройти автентифікацію перед отриманням мережевого доступу, що мінімізує ризики підключення незареєстрованого обладнання. Для віддаленого доступу реалізовано VPN-тунелі з двофакторною автентифікацією (пароль + OTP) через мобільний додаток. Це дозволяє адміністраторам безпечно підключатися до внутрішніх сервісів навіть з незахищених мереж.

Інтеграція з SIEM-системою завершує ланцюжок захисту, об'єднуючи дані від фаєрволу, VPN-концентратора та системи моніторингу. SIEM здійснює кореляцію подій, виявляє аномальні сценарії та автоматично генерує інциденти для реагування. У разі критичних ситуацій система може запускати попередньо визначені сценарії реагування: відключення порушника від мережі або блокування підозрілих потоків. Такий підхід забезпечує швидке виявлення загроз і зменшує час на ліквідацію наслідків інцидентів.

3.5. Висновки до третього розділу

Процес розробки інформаційної системи розпочався з детального вивчення вихідних вимог та проведення SWOT-аналізу, що дозволило виявити сильні та слабкі сторони існуючої інфраструктури, а також можливості для покращень і потенційні загрози. На підставі цих даних було сформульовано функціональні й нефункціональні вимоги, які стали фундаментом для подальшого моделювання. Виконаний аналіз дав змогу обґрунтувати необхідність застосування VLAN-сегментації, централізованого моніторингу та посилених заходів захисту. Таким чином, вже на початковому етапі забезпечено цілісність бачення системи та узгодженість між зацікавленими сторонами.

Наступним кроком стало логічне моделювання бізнес-процесів та потоків даних за допомогою DFD і IDEF0, що дало чітке уявлення про взаємодію користувачів, процесів та зовнішніх систем. Паралельно побудовано UML-діаграми прецедентів і класів, які деталізували рольових учасників та об’єктну структуру системи. Такий багаторівневий підхід дозволив виявити потенційні конфлікти логіки та оптимізувати взаємодію підсистем ще до реалізації. Отримані результати лягли в основу подальшого проєктування даних і фізичної інфраструктури.

Інформаційна модель, представлена ER-діаграмою, чітко структурувала ключові сутності: користувачів, пристрої, сесії, логи, події та VLAN, зі всіма необхідними зв’язками і обмеженнями цілісності. Виділення асоціативної сутності для зв’язку пристроїв і віртуальних мереж забезпечило гнучкість конфігурацій. Така модель гарантує швидкий доступ до історії подій і зручність аналізу мережевих сеансів. Наявність документованої базової структури даних спрощує подальшу реалізацію та тестування.

Проєкт фізичної мережевої архітектури відобразив розділення на серверний та користувацький сегменти, включивши ядро комутації, маршрутизатори з функціями NAT, VPN і фаєрволом, а також точки доступу стандарту 802.11ax. Визначено VLAN-маркери для навчальних аудиторій і

гуртожитків, що забезпечило ізоляцію трафіку й підвищену безпеку. Окремі серверні ролі (керуючий, файловий, DNS/DHCP) розгорнуті на виділених вузлах із каналами високої пропускної здатності. Така схема відповідає найкращим практикам побудови корпоративної мережі університету.

Розробка підсистем управління, моніторингу та захисту доступу забезпечила повноцінний набір інструментів для адміністрування, спостереження й реагування на інциденти. Централізований веб-інтерфейс із ролями і журналом дій дозволив впровадити принцип найменших привілеїв, а інтеграція Zabbix і PRTG із системою алертів — оперативно відстежувати стан ресурсів. Використання IEEE 802.1X та VPN з двофакторною автентифікацією забезпечило високий рівень контролю доступу. Інтеграція подій у SIEM-систему дала змогу автоматизувати кореляцію інцидентів і пришвидшити заходи реагування.

Особлива увага також приділена питанню обслуговування та масштабування системи в майбутньому. Запропонована архітектура передбачає можливість горизонтального розширення серверних кластерів та додавання нових точок доступу без істотного перероблення топології. Розроблений план регламентного обслуговування включає регулярну перевірку працездатності каналів, оновлення прошивки та аудит безпекових налаштувань. Це дозволить своєчасно планувати розширення інфраструктури та підтримувати високий рівень доступності послуг.

Загалом, виконані роботи забезпечили комплексне проєктування інформаційної системи: від аналітики вимог і моделювання до побудови фізичної мережевої топології та налаштування засобів захисту. Всі компоненти системи гармонійно поєднані між собою та відповідають методичним рекомендаціям кваліфікаційної роботи бакалавра. Запропоновані рішення створюють надійну основу для подальшої розробки, впровадження й експлуатації системи, що задовольняє потреби УМСФ в модернізації та захищеності мережної інфраструктури.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було здійснено ґрунтовний аналіз існуючої мережевої інфраструктури Університету митної справи та фінансів. Основною метою було визначення ключових проблем та обмежень, які перешкоджають ефективній підтримці освітнього процесу та дослідницької діяльності закладу. Проведення SWOT-аналізу дозволило систематизувати сильні та слабкі сторони, а також окреслити можливості й загрози для подальшого розвитку мережі. Отримані результати слугували підґрунтям для формулювання чітких і обґрунтованих технічних і організаційних вимог до нової інформаційної системи.

Виявлено, що наявна мережа характеризується фрагментацією, відсутністю централізованого моніторингу та недостатнім рівнем безпеки. Застаріле обладнання не здатне забезпечити необхідну пропускну здатність, а відсутність сегментації мережі підвищує ризик несанкціонованого доступу. Недостатня кількість кваліфікованого персоналу ускладнює своєчасне реагування на інциденти й модернізацію інфраструктури. Ці фактори посилюють потребу в комплексному підході до проєктування нової системи.

На основі аналізу було сформовано вимоги до інформаційної системи, які включають централізоване керування та моніторинг всіх компонентів мережі. Особлива увага приділяється впровадженню VLAN для логічної ізоляції трафіку, а також підтримці VPN-з'єднань для безпечного віддаленого доступу до хмарних сервісів. Рекомендовано застосувати стандарти ISO/IEC 27001 для захисту інформації та ISO/IEC 12207 для організації життєвого циклу системи. Усі вимоги розроблено з урахуванням бюджетних обмежень та реальних можливостей університету.

Другий розділ роботи був присвячений методам моделювання мережевих інфраструктур та класифікації топологій. Було детально розглянуто властивості зіркоподібної, шинної, кільцевої, сітчастої та гібридної топологій, що дало змогу обрати оптимальний варіант для конкретних умов УМСФ. Аналіз моделі OSI

допоміг чіткіше розподілити функції мережевих компонентів за рівнями взаємодії. Розуміння особливостей кожної топології дозволило сформулювати рекомендації щодо побудови надійної та масштабованої архітектури.

У межах вивчення протоколів передачі даних було наголошено на ролі TCP як інструмента для надійної доставки пакетів та UDP для роботи в реальному часі. Оцінка різних рівнів моделі OSI, зокрема фізичного, канального та мережевого, забезпечила всебічний погляд на організацію передачі інформації. Це дало можливість врахувати затримки, пропускну здатність і надійність при проєктуванні каналів зв'язку. Врахування цих аспектів є ключовим для забезпечення якості сервісів університетської мережі.

Значний розділ було присвячено порівнянню програмних засобів для емуляції та моделювання мереж. Аналіз Cisco Packet Tracer, GNS3, Boson NetSim та EVE-NG дозволив обрати оптимальний набір інструментів для розробки функціонального прототипу. Було визначено, що Packet Tracer найкраще підходить для початкового етапу візуалізації, тоді як GNS3 забезпечує роботу з реальними образами ОС мережевих пристроїв. Цей підхід гарантує баланс між простотою використання та точністю емуляції.

Критерії вибору програмного забезпечення враховували функціональність, масштабованість, вимоги до апаратних ресурсів та вартість ліцензій. Простота освоєння інструментів має важливе значення для студентів і співробітників лабораторії, тоді як точність моделювання – для перевірки архітектурних рішень. Наявність навчальних матеріалів і активних спільнот користувачів підсилює ефективність впровадження обраних платформ. Збалансований вибір інструментів забезпечує успішне виконання практичної частини роботи.

У третьому розділі здійснено безпосереднє проєктування інформаційної системи для розвитку інфраструктури мережі УМСФ. Першим кроком стало створення логічної моделі даних (ERD) та діаграм потоків даних (DFD), що дозволило формалізувати взаємодію між підсистемами. Потім побудовано загальну схему мережної інфраструктури з урахуванням розміщення серверного,

мережевого обладнання та точок доступу Wi-Fi 6 у всіх корпусах. Виконані роботи заклали основу для подальшої фізичної реалізації.

Архітектурні рішення ґрунтувалися на централізованій консолі управління, яка об'єднує моніторинг, адміністрування та звітування в єдиному інтерфейсі. Забезпечено пропускну здатність магістральних каналів не менше 10 Гбіт/с та підроздільних лінків — 1 Гбіт/с. Для викладачів і студентів передбачено захищений доступ через VPN-шлюзи до хмарних платформ Google Workspace і Moodle. Таке рішення відповідає сучасним вимогам до продуктивності й надійності.

Особливу увагу приділено реалізації системи аутентифікації 802.1X із двофакторною перевіркою, що гарантує високий рівень безпеки доступу. Впроваджено IDS/IPS для виявлення й блокування загроз у режимі реального часу. Централізоване журналювання подій дозволяє швидко реагувати на інциденти та проводити аналіз після атак. Ці підсистеми значно підвищують кіберзахищеність мережі університету.

Реалізований прототип інформаційної системи в середовищі Cisco Packet Tracer (або GNS3) підтвердив обґрунтованість обраних архітектурних рішень. Проведене моделювання показало стійкість системи до пікових навантажень та ефективність механізмів безпеки. Це дозволило виправдати запропоновані рекомендації перед стейкхолдерами та керівництвом університету. Отримані результати є базою для практичної реалізації.

Розроблені рекомендації щодо поетапного впровадження передбачають розгортання критичних підсистем, поступове оновлення обладнання та навчання персоналу. Запропоновано план з тестування, введення в експлуатацію та переходу до промислової експлуатації. Враховано бюджетні обмеження та можливості внутрішніх ресурсів УМСФ. Такий підхід мінімізує ризики та забезпечує плавний перехід до нової інфраструктури.

Впровадження інформаційної системи для розвитку мережі УМСФ суттєво покращить якість освітнього процесу та підтримку наукової діяльності. Зростання пропускної здатності, підвищена безпека та централізоване

управління створять комфортні умови для використання онлайн-ресурсів. Адміністрація отримає інструменти для аналітики та оперативного реагування. Це сприятиме зростанню інвестиційної привабливості закладу.

Крім технічної реалізації, під час виконання кваліфікаційної роботи було враховано нормативні вимоги щодо захисту інформації в інформаційно-телекомунікаційних системах. Зокрема, дотримано принципів захисту персональних даних згідно з законодавством України, що є обов'язковим для ВНЗ, які обробляють дані студентів, викладачів і адміністративного персоналу. Це підвищує правову безпечність запропонованого рішення і забезпечує відповідність стандартам у сфері освіти.

Впроваджені підсистеми управління, моніторингу та захисту доступу створюють цілісну і взаємопов'язану архітектуру, яка охоплює всі ключові аспекти експлуатації комп'ютерної мережі. Завдяки інтеграції таких інструментів, як Zabbix і PRTG, забезпечується своєчасне виявлення відмов та проактивне реагування на потенційні загрози. Це дозволяє мінімізувати простої, оптимізувати навантаження на IT-персонал і забезпечити безперервну роботу критичних сервісів університету

Окремо варто зазначити значущість реалізованої системи для підготовки студентів спеціальності «Інженерія програмного забезпечення». Використання таких середовищ, як Cisco Packet Tracer і GNS3, сприяє розвитку практичних навичок з проєктування, адміністрування та аналізу мережевих систем. Створені в рамках роботи сценарії можуть бути використані в навчальному процесі — наприклад, у курсах «Комп'ютерні мережі», «Моделювання інформаційних систем» або «Кібербезпека».

Результати моделювання підтвердили, що обране рішення демонструє високу ефективність в умовах підвищеного навантаження, зберігаючи при цьому стабільність і керованість. Актуальність реалізованої архітектури підтверджується її масштабованістю — система здатна адаптуватися до зростання кількості підключених пристроїв та інтеграції нових сервісів. Це

створює передумови для довгострокового використання без потреби у суттєвій реконструкції.

Важливою перевагою спроєктованої інформаційної системи є її орієнтація на розширення функціоналу у майбутньому. Наприклад, можлива інтеграція з платформами аналітики (Learning Analytics), системами управління доступом до ресурсів (SSO) та інструментами штучного інтелекту для виявлення аномалій у мережевому трафіку. Такий підхід відповідає концепції «розумного кампусу» та сприяє формуванню сучасного цифрового освітнього середовища.

Крім зазначених переваг, виконана кваліфікаційна робота має важливе значення для підготовки фахівців у галузі інженерії програмного забезпечення. Вона демонструє практичне застосування теоретичних знань у процесі проєктування сучасних інформаційних систем, що відповідають вимогам безпеки, масштабованості та інтеграції з хмарними сервісами. Сформовані в процесі дослідження підходи, рішення та моделі можуть бути використані в освітньому процесі, науковій діяльності та при реалізації подібних інфраструктурних проєктів у сфері вищої освіти.

Підсумовуючи, виконана робота має високу практичну цінність як для УМСФ, так і для інших вищих навчальних закладів, які стикаються з проблемами модернізації мережевої інфраструктури. Отримані результати можуть бути адаптовані до різних організаційних масштабів і технічних умов. Запропонована модель відповідає вимогам часу та може слугувати прикладом для реалізації подібних проєктів у сфері освіти та адміністрування IT-ресурсів.

Таким чином, виконана кваліфікаційна робота не лише вирішила поставлені завдання, але й створила основу для подальшого цифрового вдосконалення інфраструктури Університету митної справи та фінансів. Результати дослідження можуть бути використані для масштабування рішення на інші заклади освіти та корпоративні мережі. Практична реалізація рекомендацій принесе відчутні переваги в плані продуктивності, безпеки та гнучкості. Робота підтвердила важливість системного підходу до проєктування IT-інфраструктури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ISO/IEC 27001:2022. Information security management systems — Requirements. International Organization for Standardization, 2022.
2. ДСТУ 2627-94. Системи оброблення інформації. Терміни та визначення. Київ: Держстандарт України, 1994.
3. Організація комп'ютерних мереж: навчальний посібник / за ред. В.І. Гриценка. Запоріжжя: ЗНУ, 2016.
4. Інформаційні технології в управлінні закладами освіти: монографія / за ред. О.В. Матвієнка. Львів: Видавництво Львівської політехніки, 2018.
5. Інтегрування та захист IoT пристроїв у наявній інфраструктурі комп'ютерної мережі закладів освіти / О.І. Мельник, І.В. Ковальчук // Науковий журнал «Інформаційні технології і засоби навчання». – 2021. – № 2(82). – С. 45–53.
6. Биков В.Ю. Технології хмарних обчислень – провідні інформаційні технології подальшого розвитку інформатизації системи освіти України / В.Ю. Биков // Комп'ютер у школі та сім'ї. – 2011. – №1. – С. 3–11.
7. Element451. Top Technology Trends in Higher Education. – 2025. – [Електронний ресурс]. – Режим доступу: https://element451.com/blog/5-higher-ed-tech-trends-to-watch.
8. Panopto. 4 Trends That Have Higher Ed IT Leaders Rethinking Their Tech Stack. – 2025. – [Електронний ресурс]. – Режим доступу: https://www.panopto.com/blog/4-trends-that-have-higher-ed-it-leaders-rethinking-their-tech-stack/.
9. Ruckus Networks. New Technology Trends Are Reshaping Higher Education. – 2025. – [Електронний ресурс]. – Режим доступу: https://fr.ruckusnetworks.com/blog/2025/new-technology-trends-are-reshaping-higher-education/.
10. Collegis Education. Top 8 Disruptive Trends Shaping Higher Ed in 2025. – 2025. – [Електронний ресурс]. – Режим доступу: https://collegiseducation.com/insights/top-eight-disruptions-in-2025/.

11. Університет митної справи та фінансів. Офіційний сайт. [Електронний ресурс]. – Режим доступу: https://www.umsf.dp.ua
12. Навчальна лабораторія системного адміністрування. [Електронний ресурс]. – Режим доступу: https://umsf.dp.ua/struktura/pidrozdily/navchalna-laboratoriia-systemnoho-administruvannia
13. Організація комп'ютерних мереж. [Електронний ресурс]. – Режим доступу: https://files.znu.edu.ua/files/Bibliobooks/Inshi78/0058261.pdf
14. Системне адміністрування і послуги IT-інфраструктури. [Електронний ресурс]. – Режим доступу: https://www.coursera.org/learn/system-administration-it-infrastructure-services-ua
15. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення – Київ: Держстандарт України, 1996.
16. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР. — [Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
17. ISO/IEC/IEEE 12207:2017. Systems and software engineering — Software life cycle processes. Geneva: ISO/IEC, 2017.
18. Шевченко В.О. Комп'ютерні мережі: навч. посіб. – К.: Ліра-К, 2020. – 328 с.
19. PhoenixNAP. The OSI Model: Definition, Layers, Benefits Explained. [Електронний ресурс]. – Режим доступу: https://phoenixnap.com/kb/osi-model
20. Kentik. Network Architecture Explained: Understanding the Basics of Network Architecture. [Електронний ресурс]. – Режим доступу: https://www.kentik.com/kentipedia/network-architecture/
21. GeeksforGeeks. What is OSI Model? – Layers of OSI Model. [Електронний ресурс]. – Режим доступу: https://www.geeksforgeeks.org/open-systems-interconnection-model-osi/
22. Comparitech. 6 Best Network Topologies Explained - Pros & Cons. [Електронний ресурс]. – Режим доступу: https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages/

23. PyNet Labs. What is Cisco Packet Tracer and Its Features? [Електронний ресурс]. – Режим доступу: https://www.pynetlabs.com/cisco-packet-tracer/
24. GNS3 Documentation. Getting Started with GNS3. [Електронний ресурс]. – Режим доступу: https://docs.gns3.com/docs/
25. Boson. NetSim Network Simulator Product Features. [Електронний ресурс]. – Режим доступу: https://www.boson.com/netsim-cisco-network-simulator-features
26. Комплексний аналіз програмного забезпечення для моделювання та емуляції комп'ютерних мереж / О. Козак, Л. Михайлова, І. Семенишина // Комп'ютерно інтегровані технології: освіта, наука, виробництво. – 2024. – № 2. – С. 70–76.
27. ТИПОВА СТРУКТУРА І СКЛАД ІНФОРМАЦІЙНИХ СИСТЕМ. Pidru4niki. URL: https://pidru4niki.com/19610926/informatika/tipova_struktura_sklad_informatsiynih_sistem (дата звернення: 26.05.2025).

ДОДАТОК А

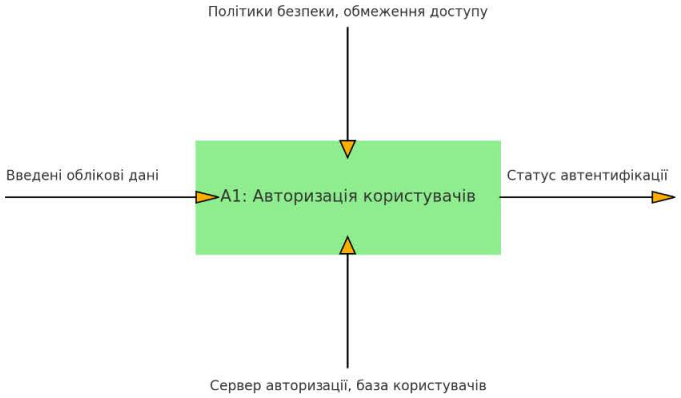

Рисунок А.1 – IDEF0: Авторизація користувачів

Рисунок А.2 – IDEF0: Доступ до ресурсів

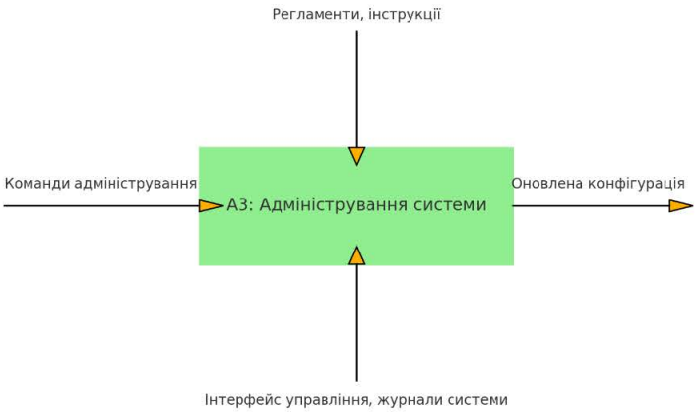

Рисунок А.3 – IDEF0: Адміністрування системи

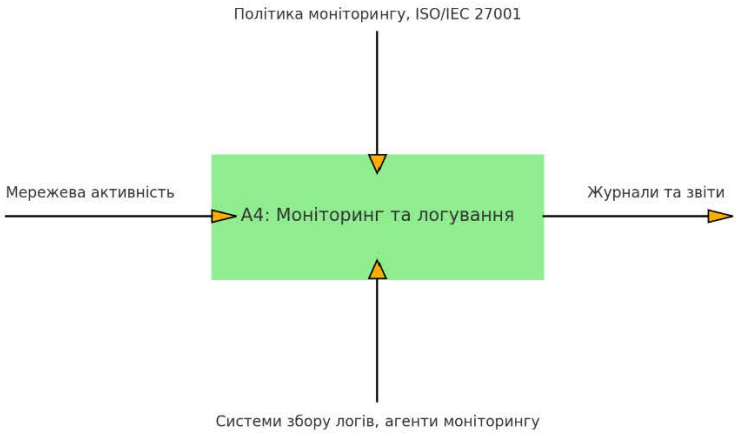

Рисунок А.4 – IDEF0: Моніторинг та логування

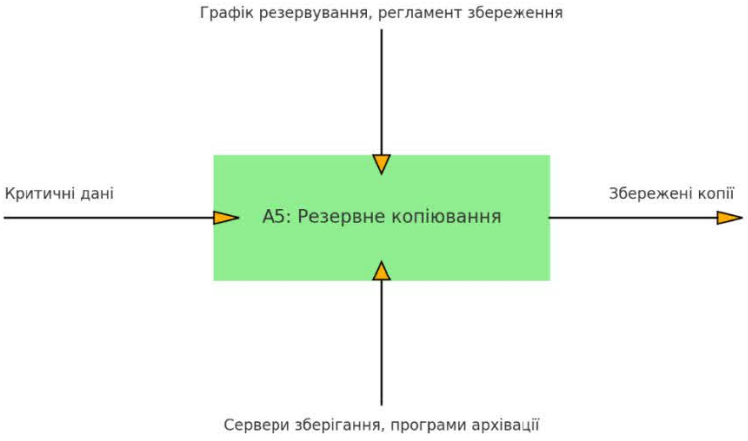

Рисунок А.5 – IDEF0: Резервне копіювання даних

ДОДАТОК Б

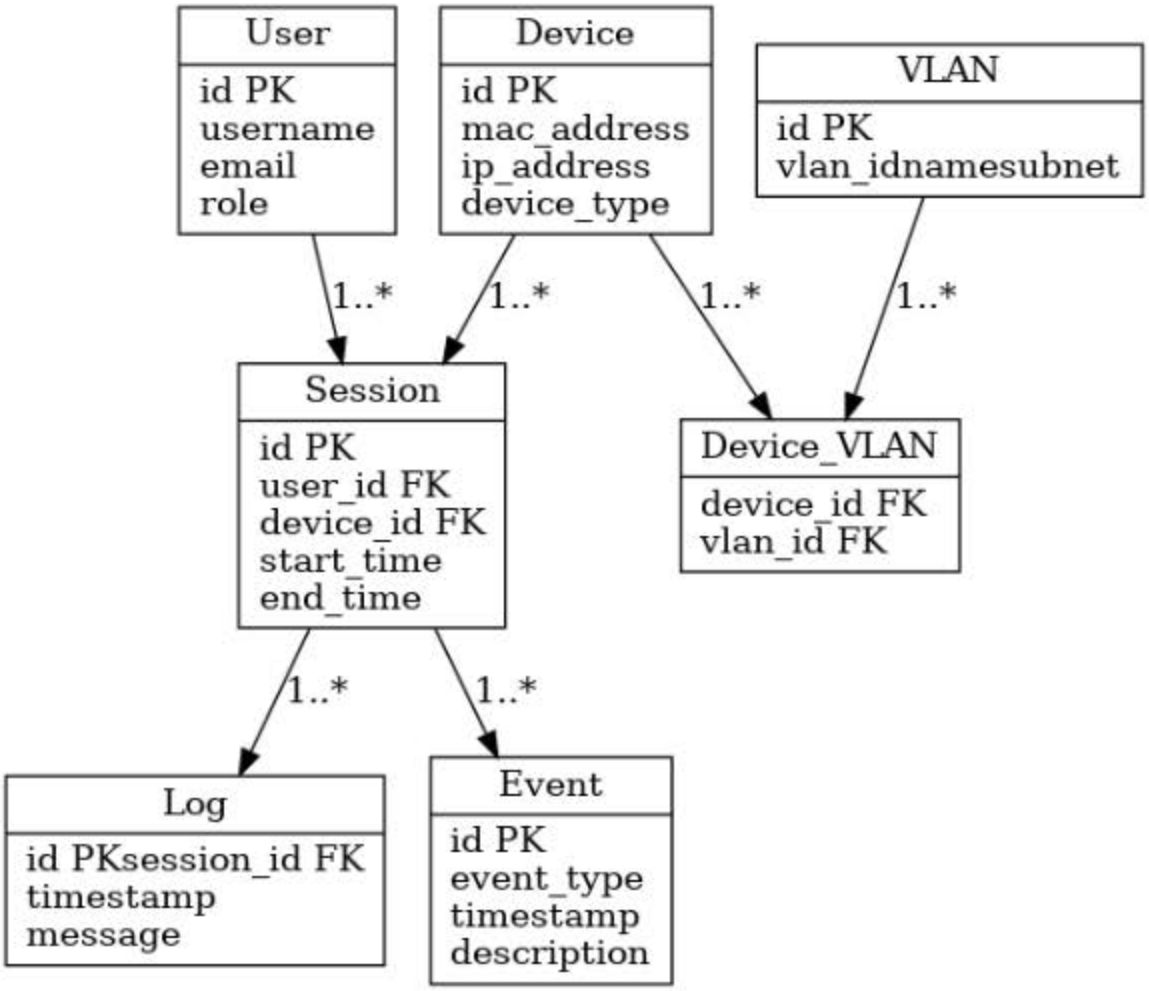

Рисунок Б.1 – ER-діаграма сутностей