Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

**КВАЛІФІКАЦІЙНА РОБОТА**

Ясінського Антона Валерійовича

на здобуття ступеня вищої освіти Бакалавра

Система захисту особової конфіденційної інформації згідно вимог Загального регламенту захисту персональних даних (GDPR) ЄС

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ.220257.22.02.38 ПЗ

Виконав студент 4 курсу група КБ-22-2 Антон ЯСІНСЬКИЙ

Керівник канд. техн. наук, доцент Віктор ЧЕШУН

Нормоконтролер д-р філософії Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

17 06 2026 р.

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій
Кафедра Кібербезпеки
Рівень вищої освіти Бакалавр
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
Юрій КЛЬОЦ
9 січня 2026 р.

**З А В Д А Н Н Я**
**НА КВАЛІФІКАЦІЙНУ РОБОТУ**
Ясінському Антону Валерійовичу

1 Тема роботи Система захисту особової конфіденційної інформації згідно вимог Загального регламенту захисту персональних даних (GDPR) ЄС

Керівник роботи канд. техн. наук, доцент, Чешун Віктор Миколайович
Затверджено наказом ректора університету від 8 січня 2026 р. № 7
2 Строк подання студентом кваліфікаційної роботи на кафедру 27 травня 2026р.
3 Вихідні дані до роботи Аналіз предметної області та вимог законодавства України і GDPR ЄС щодо захисту персональних даних; процеси обробки особової конфіденційної інформації студентів; об'єкт захисту, загрози, ролі користувачів; модель захищеної ІКС із серверною зоною, сегментацією мережі та розмежуванням доступу.
4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Аналіз предметної області та нормативно-правової бази захисту персональних даних. Дослідження процесів обробки персональних даних студентів. Постановка задачі та визначення вимог до захищеної ІКС. Проєктування структури ІКС, серверної зони та мережевих сегментів. Розроблення правил розмежування доступу. Практична реалізація сегментації, IP-адресації та правил доступу. Перевірка працездатності системи й оцінка відповідності вимогам GDPR. Висновки.
5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
План приміщень. Схема сегментації мережі та розмежування доступу. Мережева схема захищеної інформаційно-комунікаційної системи університету.

6 Консультанти розділів кваліфікаційної роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| | | | |

7 Дата видачі завдання 12 січня 2026 р.

## КАЛЕНДАРНИЙ ПЛАН

| Назва етапів (розділів) кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|
| Вибір і затвердження теми кваліфікаційної роботи | Січень-Лютий | |
| Ознайомлення з предметною областю | Лютий | |
| Дослідження існуючих рішень | Лютий | |
| Постановка задачі | Березень | |
| Визначення загальних принципів рішення задачі | Березень | |
| Деталізація принципів рішення задачі | Квітень | |
| Розробка проєктних рішень | Квітень | |
| Апробація проєктних рішень | Травень | |
| Оформлення пояснювальної записки згідно вимог | Травень | |
| Оформлення графічної частини | Травень | |
| Захист КР | Червень | |

Студент Антон ЯСІНСЬКИЙ

Керівник кваліфікаційної роботи Віктор ЧЕШУН

# АНОТАЦІЯ

Тема кваліфікаційної роботи: Система захисту особової конфіденційної інформації згідно вимог Загального регламенту захисту персональних даних (GDPR) ЄС.

Автор роботи: Ясінський Антон Валерійович.

Керівник роботи: канд. техн. наук, доц. Чешун Віктор Миколайович.

Загальний обсяг роботи: 84 сторінки, 11 рисунків, 2 таблиці, 1 додаток, 40 посилань.

Графічна частина: 3 плакати.

Ключові слова: персональні дані, GDPR, особова конфіденційна інформація, інформаційно-комунікаційна система, мережева сегментація, серверна зона, розмежування доступу.

Метою кваліфікаційної роботи є розроблення захищеної інформаційно-комунікаційної системи університетського підрозділу для обробки особової конфіденційної інформації студентів відповідно до вимог законодавства України та GDPR ЄС. У роботі проаналізовано предметну область захисту персональних даних, процеси їх обробки в університетській ІКС та вимоги до захисту інформації. Обґрунтовано технічні рішення захисту, зокрема побудову серверної зони, сегментацію мережі, розмежування доступу між підрозділами та ізоляцію студентського сегмента.

Результати роботи можуть бути використані під час створення або модернізації захищених ІКС закладів вищої освіти.

25.05.2026

# ANNOTATION

Theme of qualification work: System for Protection of Personal Confidential Information According to the Requirements of the General Data Protection Regulation (GDPR) of the EU.

Author of the work: Yasinskyi Anton Valeriiovych

Mentor: Ph.D. Cheshun Viktor Mykolaiovych

Total volume of work: 84 pages, 11 figures, 2 tables, 1 appendice, 40 links.

Graphic part: 3 posters.

Keywords: personal data, GDPR, personal confidential information, information and communication system, network segmentation, server zone, access delimitation.

The purpose of the qualification work is to develop a protected information and communication system for a university department for processing students' personal confidential information in accordance with the requirements of Ukrainian legislation and the EU GDPR. The work analyzes the subject area of personal data protection, the processes of their processing in the university ICS, and information protection requirements. The technical protection solutions are substantiated, in particular the creation of a server zone, network segmentation, access delimitation between departments, and isolation of the student segment.

The results of the work can be used during the creation or modernization of protected ICSs in higher education institutions.

25.05.2026 _____

ЗМІСТ

# ВСТУП

Сучасні заклади вищої освіти активно використовують інформаційно-комунікаційні системи для організації вступу, навчального процесу, обліку студентів, фінансового супроводу, оформлення документів та взаємодії між підрозділами. У таких системах обробляється значний обсяг персональних даних студентів, зокрема ідентифікаційні відомості, контактна інформація, паспортні дані, громадянство, навчальні дані, фінансова інформація та інші відомості, які дозволяють прямо або опосередковано ідентифікувати особу [1, 2].

Захист персональних даних у закладі вищої освіти є не лише юридичним, але й технічним завданням. Якщо персональні дані зберігаються або передаються в мережі без належного розмежування доступу, виникає ризик їх неправомірного перегляду, зміни, втрати або розголошення. Особливої актуальності ця проблема набуває тоді, коли університет надає освітні послуги громадянам країн Європейського Союзу (ЄС), оскільки в такому випадку потрібно враховувати не лише законодавство України, але й принципи Загального регламенту захисту персональних даних ЄС (General Data Protection Regulation – GDPR) [2, 3].

Проблема, що вирішується в роботі, полягає в ризику надмірного доступу до персональних даних студентів у межах університетської інформаційно-компютерної системи (ІКС). Такий ризик може виникати через недостатнє відокремлення серверної зони, відсутність чіткої сегментації мережі, можливість доступу студентського сегмента до внутрішніх ресурсів та неконтрольовану взаємодію між підрозділами. Тому метою кваліфікаційної роботи є розроблення захищеної інформаційно-комунікаційної системи університетського підрозділу для обробки особової конфіденційної інформації студентів відповідно до вимог законодавства України та принципів GDPR [4, 5].

Для досягнення цілей роботи необхідно вирішити такі завдання:

– провести аналіз нормативно-правової бази захисту персональних даних відповідно до законодавства України та вимог GDPR;

– дослідити процеси обробки особової конфіденційної інформації студентів університету під час надання освітніх послуг громадянам ЄС;

– визначити проблеми університетської ІКС, які можуть створювати ризики для конфіденційності персональних даних студентів;

– сформувати вимоги до захищеної ІКС університетського підрозділу;

– розробити концептуальну модель захищеної ІКС;

– спроєктувати мережеву архітектуру із виділенням серверної зони, робочих сегментів підрозділів та студентського сегмента;

– розробити правила розмежування доступу між сегментами мережі відповідно до функцій користувачів;

– реалізувати практичну модель захищеної ІКС із поділом мережі на сегменти, окремою серверною зоною та правилами доступу;

– оцінити відповідність запропонованої ІКС вимогам захисту персональних даних.

Робота включає аналіз нормативно-правових документів, аналіз процесів обробки персональних даних, визначення проблем доступу в університетській ІКС, проєктування інформаційно-комунікаційної системи, побудову мережевої архітектури, розмежування доступу між користувачами та оцінювання відповідності запропонованих рішень вимогам захисту персональних даних.

У першому розділі досліджується нормативно-правова база захисту персональних даних, процеси їх обробки в університеті та вимоги до захищеної ІКС. У другому розділі виконується проєктування захищеної ІКС університетського підрозділу, визначаються її структура, серверна зона, мережеві сегменти та правила доступу. У третьому розділі подано практичну реалізацію розробленої ІКС, налаштування сегментації, IP-адресації, правил доступу та перевірку працездатності запропонованих рішень.

# 1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА ПОСТАНОВКА ЗАДАЧІ

## 1.1 Аналіз нормативно-правової бази захисту персональних даних відповідно до законодавства України та GDPR

Захист персональних даних є важливою складовою інформаційної безпеки сучасних організацій. У закладах вищої освіти персональні дані обробляються під час вступу, навчання, оформлення документів, організації освітнього процесу, обліку студентів та взаємодії між структурними підрозділами. Через це університетська інформаційно-комунікаційна система повинна бути побудована так, щоб забезпечувати захист особової конфіденційної інформації від несанкціонованого доступу, зміни, втрати або розголошення [3, 5].

Персональні дані можна визначити як будь-яку інформацію, яка дає змогу прямо або опосередковано ідентифікувати фізичну особу. У контексті університету до таких даних належать прізвище, ім’я, дата народження, адреса проживання, електронна пошта, номер телефону, паспортні дані, громадянство, відомості про освітню програму, академічний статус, фінансова інформація та інші дані, які використовуються під час надання освітніх послуг [6].

Особливого значення захист персональних даних набуває у випадку, коли університет працює з іноземними студентами, зокрема громадянами країн Європейського Союзу. У такій ситуації обробка персональних даних повинна враховувати не тільки вимоги законодавства України, але й положення Загального регламенту захисту персональних даних ЄС, тобто GDPR. Цей регламент визначає загальні правила обробки персональних даних, права суб’єктів даних та обов’язки організацій, які працюють з такою інформацією.

Основним нормативно-правовим актом Європейського Союзу у сфері захисту персональних даних є Regulation (EU) 2016/679. GDPR встановлює вимоги до законної, справедливої, прозорої та безпечної обробки персональних даних. Для університету це означає, що персональні дані студентів не можуть

оброблятися без визначеної мети, правової підстави та належних засобів захисту [7].

У межах цієї роботи GDPR розглядається як нормативна основа для визначення вимог до захищеної інформаційно-комунікаційної системи університетського підрозділу. Тобто основна увага приділяється не розробленню окремих юридичних документів, а побудові такої ІКС, у якій персональні дані студентів обробляються з урахуванням принципів GDPR. Це дозволяє поєднати правові вимоги до захисту персональних даних із конкретними технічними рішеннями інформаційної безпеки [5, 8].

Водночас GDPR не замінює законодавство України, а використовується в роботі разом із ним. Закон України “Про захист персональних даних” визначає національні правові засади обробки персональних даних, права суб’єктів даних та обов’язки володільців і розпорядників. Закон України “Про захист інформації в інформаційно-комунікаційних системах” визначає необхідність захисту інформації під час її обробки в ІКС. GDPR у межах цієї роботи застосовується як додаткова нормативна основа для обробки персональних даних студентів, які є громадянами країн Європейського Союзу [5].

GDPR ґрунтується на низці основних принципів, які повинні враховуватися під час обробки персональних даних. До них належать законність, справедливість і прозорість обробки, обмеження мети, мінімізація даних, точність, обмеження строків зберігання, цілісність, конфіденційність та підзвітність. Саме ці принципи визначають загальний підхід до побудови системи захисту персональних даних в університетській ІКС.

Принцип законності обробки означає, що університет повинен мати правову підставу для роботи з персональними даними студента. Такою підставою може бути згода особи, виконання договору про надання освітніх послуг, виконання вимог законодавства або інша правова підстава, передбачена GDPR. У практичному розумінні це означає, що студент повинен розуміти, які саме дані збираються, для чого вони потрібні та хто може мати до них доступ.

Принцип прозорості передбачає, що обробка персональних даних не

повинна бути прихованою або незрозумілою для суб'єкта даних. Студент має бути поінформований про мету обробки, категорії даних, строки їх зберігання та загальний порядок використання інформації. Для університету це важливо, тому що персональні дані можуть проходити через різні підрозділи, і студент повинен мати загальне розуміння того, як саме вони використовуються під час освітнього процесу [9].

Принцип обмеження мети означає, що персональні дані повинні використовуватися лише для конкретних і законних цілей. Наприклад, дані, отримані під час вступу, можуть використовуватися для зарахування, формування особової справи, організації навчання або оформлення документів, але не повинні застосовуватися для сторонніх цілей без належної підстави. У межах ІКС це потребує чіткого розподілу доступу між підрозділами університету.

Принцип мінімізації даних означає, що університет повинен обробляти лише ті персональні дані, які є необхідними для конкретної мети. Якщо підрозділу достатньо знати освітню програму, академічну групу та статус студента, він не повинен мати доступу до паспортних або фінансових даних. У цьому випадку мінімізація стосується не тільки кількості зібраної інформації, але й обмеження кола осіб, які можуть працювати з нею.

Для інформаційно-комунікаційної системи принцип мінімізації має безпосереднє технічне значення. Його можна реалізувати через поділ мережі на окремі сегменти, виділення серверної зони та встановлення правил доступу між підрозділами. Наприклад, деканат, міжнародний відділ, фінансовий відділ, адміністратор системи та студентська мережа повинні мати різні можливості доступу до інформаційних ресурсів.

Принцип точності передбачає, що персональні дані повинні бути актуальними та правильними. Університет повинен мати можливість виправляти помилки у персональних даних, наприклад у прізвищі, імені, контактній інформації, громадянстві або навчальному статусі студента. З технічної точки

зору це означає, що змінювати такі дані мають лише уповноважені користувачі, а доступ до відповідних ресурсів повинен бути обмежений [9].

Принцип обмеження строків зберігання означає, що персональні дані не повинні зберігатися довше, ніж це потрібно для досягнення мети обробки або виконання вимог законодавства. Університет може зберігати частину даних протягом навчання, частину після завершення навчання, а частину лише протягом окремого адміністративного процесу. Це потребує розуміння того, де саме в ІКС зберігаються відповідні дані та хто має до них доступ.

Принцип цілісності та конфіденційності є одним із ключових для побудови захищеної ІКС. Він вимагає, щоб персональні дані були захищені від несанкціонованого доступу, випадкової втрати, зміни або розголошення. У межах університетської ІКС це може забезпечуватися через автентифікацію користувачів, розмежування доступу, мережеву сегментацію, серверну зону та обмеження взаємодії між окремими частинами мережі.

Принцип підзвітності означає, що організація повинна мати можливість підтвердити, що обробка персональних даних здійснюється відповідно до встановлених вимог. У межах цієї роботи підзвітність розглядається насамперед через контроль доступу та зрозумілу структуру ІКС. Якщо персональні дані зберігаються в окремій серверній зоні, а доступ до неї мають лише визначені сегменти мережі, це дозволяє більш чітко контролювати обробку інформації.

Окрему увагу GDPR приділяє правам суб’єктів персональних даних. Студент має право отримати інформацію про обробку своїх даних, вимагати виправлення неточних відомостей, обмеження обробки, видалення даних у передбачених випадках та отримання копії своїх даних. Для університету це означає, що персональні дані повинні бути впорядковані, доступні для обробки уповноваженими особами та захищені від доступу сторонніх користувачів.

Право на доступ до персональних даних дає студенту можливість дізнатися, які саме дані про нього обробляються університетом. Водночас реалізація цього права не повинна створювати ризик розкриття інформації

стороннім особам. Тому система має забезпечувати ідентифікацію користувачів і розмежування доступу, щоб кожна особа могла отримати лише ту інформацію, яка стосується її або її службових обов’язків [1, 10].

Право на виправлення даних є важливим для освітнього процесу, оскільки помилки в особовій інформації можуть впливати на документообіг, комунікацію зі студентом та оформлення навчальних документів. Зміни до персональних даних повинні виконуватися лише уповноваженими працівниками. Це ще раз підтверджує необхідність розмежування доступу в ІКС університету.

Для цієї роботи права суб’єктів персональних даних мають значення насамперед тому, що університетська ІКС повинна забезпечувати впорядковане зберігання даних і доступ до них лише для уповноважених користувачів. Тобто технічна структура системи має підтримувати можливість контрольованої обробки персональних даних, а не створювати відкритий доступ до них для всіх користувачів мережі [11].

Поряд із GDPR у роботі необхідно враховувати законодавство України. Закон України "Про захист персональних даних" визначає загальні правові засади обробки персональних даних, права суб’єктів персональних даних та обов’язки володільців і розпорядників таких даних. Для університету цей закон є базовим національним нормативним актом, який регулює роботу з персональними даними студентів [3].

Закон України "Про інформацію" визначає основні принципи інформаційних відносин, права учасників інформаційної діяльності та підходи до захисту інформації. Для цієї роботи він має значення тому, що персональні дані є різновидом інформації, яка потребує належного правового режиму та захисту від неправомірного використання [4].

Особливе значення має Закон України "Про захист інформації в інформаційно-комунікаційних системах". Він визначає вимоги до захисту інформації, яка обробляється в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Оскільки в цій роботі розглядається

саме ІКС університетського підрозділу, цей закон є важливим для обґрунтування необхідності технічного захисту персональних даних [5].

Закон України "Про основні засади забезпечення кібербезпеки України" визначає загальні правові та організаційні основи кібербезпеки. Його положення важливі для розуміння загального підходу до захисту інформаційних ресурсів і безпечного функціонування інформаційно-комунікаційних систем. Для університету це має значення, оскільки порушення роботи ІКС може призвести до втрати, зміни або розкриття персональних даних [6].

Також потрібно враховувати законодавство у сфері освіти. Закон України "Про освіту" та Закон України "Про вищу освіту" визначають правові засади освітньої діяльності, права здобувачів освіти, організацію освітнього процесу та діяльність закладів вищої освіти. Саме в межах освітнього процесу університет отримує, використовує та зберігає персональні дані студентів [7, 8].

Для технічної реалізації вимог захисту персональних даних важливе значення мають підходи інформаційної безпеки та комп’ютерних мереж. У межах ІКС університету персональні дані можуть зберігатися на сервері, передаватися між підрозділами та використовуватися працівниками з різних робочих місць. Тому захист повинен охоплювати не тільки самі дані, але й мережеву інфраструктуру, через яку здійснюється доступ до них.

Одним із основних технічних підходів до захисту персональних даних є мережева сегментація. Її суть полягає в поділі мережі на окремі логічні частини відповідно до функцій користувачів або підрозділів. У межах університету доцільно виділити сегмент деканату, міжнародного відділу, фінансового відділу, адміністратора системи, серверну зону та студентський сегмент [11].

Мережева сегментація дозволяє зменшити кількість користувачів, які можуть безпосередньо взаємодіяти з ресурсами, де зберігаються персональні дані. Наприклад, студентський сегмент не повинен мати доступу до серверної зони, а працівники окремих підрозділів повинні отримувати доступ лише до тих ресурсів, які потрібні їм для виконання службових обов’язків. Такий підхід

відповідає принципу мінімізації доступу [12].

Одним із способів реалізації сегментації є використання VLAN. VLAN дозволяє логічно розділити пристрої в межах однієї мережевої інфраструктури. Завдяки цьому робочі місця різних підрозділів можуть перебувати в окремих логічних мережах, а обмін трафіком між ними може контролюватися за допомогою мережевого обладнання та правил доступу.

Списки контролю доступу ACL дозволяють визначати, які мережеві взаємодії дозволені, а які мають бути заборонені. У межах захищеної ІКС університету ACL можуть застосовуватися для обмеження доступу студентського сегмента до серверної зони, надання доступу уповноваженим підрозділам та заборони непотрібної взаємодії між окремими частинами мережі.

Важливу роль у захисті персональних даних відіграє серверна зона. У ній можуть розміщуватися сервери або інформаційні ресурси, де зберігається особова конфіденційна інформація студентів. Серверна зона повинна бути відокремлена від звичайних робочих сегментів і мати обмежений доступ. Це зменшує ризик випадкового або навмисного втручання в роботу системи.

Фізичне розміщення обладнання також має значення для захисту ІКС. Якщо сервери, комутатори або маршрутизатори розміщені у відкритому приміщенні без обмеження доступу, виникає ризик несанкціонованого втручання, відключення обладнання або пошкодження інформаційних ресурсів. Тому виділення серверної зони та контроль доступу до мережевого обладнання є важливою частиною проєктування захищеної ІКС.

Отже, нормативно-правова база захисту персональних даних у межах цієї роботи розглядається у двох напрямах. Законодавство України визначає загальні правові вимоги до обробки персональних даних і захисту інформації в ІКС, а GDPR деталізує принципи, які мають бути враховані під час обробки персональних даних громадян ЄС. До таких принципів належать мінімізація доступу, конфіденційність, цілісність, підзвітність, захист даних на етапі проєктування та захист даних за замовчуванням.

Для практичної реалізації цих вимог у роботі розглядається захищена інформаційно-комунікаційна система університетського підрозділу. Її технічна основа повинна передбачати серверну зону, мережеву сегментацію, розмежування доступу між підрозділами та ізоляцію студентського сегмента від внутрішніх ресурсів університету. Саме ці рішення надалі використовуються для формування вимог до ІКС та її проєктування.

Отже, аналіз нормативно-правової бази показує, що захист особової конфіденційної інформації студентів повинен базуватися на поєднанні правових вимог і технічних рішень. У подальшому це дозволяє перейти до аналізу процесів обробки персональних даних в університеті та визначити вимоги до захищеної інформаційно-комунікаційної системи університетського підрозділу.

## 1.2 Аналіз процесів обробки персональних даних в інформаційно-комунікаційній системі університету

Під час надання освітніх послуг університет постійно працює з персональними даними студентів. Особливе значення це має у випадку навчання громадян країн Європейського Союзу, оскільки така обробка повинна враховувати вимоги GDPR. Персональні дані використовуються під час вступу, зарахування, організації навчання, оформлення документів, обліку оплати, комунікації зі студентом та роботи структурних підрозділів університету.

До персональних даних, які можуть оброблятися під час надання освітніх послуг, належать прізвище, ім’я, дата народження, громадянство, адреса проживання, електронна пошта, номер телефону, паспортні дані, копії документів, відомості про попередню освіту, освітню програму, академічну групу, форму навчання, статус студента та фінансова інформація. Ці дані дають змогу прямо або опосередковано ідентифікувати особу, тому вони потребують захисту від несанкціонованого доступу або розголошення [12, 13].

Процес обробки персональних даних в університеті не є одноразовою дією. Він починається ще на етапі звернення або вступу студента і триває протягом усього періоду навчання. Після завершення навчання частина даних може зберігатися в архіві, частина може використовуватися для підтвердження факту навчання, а частина має бути видалена або знеособлена відповідно до встановлених строків зберігання.

Першим етапом обробки є отримання персональних даних від студента. Це може відбуватися під час подання документів до університету, заповнення заяв, передачі копій документів, надсилання інформації електронними засобами або під час особистого звернення до відповідального підрозділу. На цьому етапі важливо, щоб університет збирав лише ті дані, які реально потрібні для організації освітнього процесу та виконання законних обов'язків [14].

Під час вступу громадянина ЄС університет може отримувати документи, які підтверджують особу, громадянство, попередню освіту, право на перебування в Україні, контактні дані та інші відомості, необхідні для зарахування. Такі дані зазвичай використовуються приймальною комісією, міжнародним відділом, деканатом та іншими підрозділами, які беруть участь у вступній процедурі.

Після отримання даних відбувається їх перевірка та внесення до інформаційно-комунікаційної системи університету. На цьому етапі працівники перевіряють правильність документів, відповідність даних вимогам вступу, коректність написання прізвища та імені, контактну інформацію, освітню програму і статус студента. Помилки на цьому етапі можуть призвести до неправильного оформлення документів або ускладнення подальшої комунікації зі студентом [15].

У подальшому персональні дані використовуються для організації освітнього процесу. Вони можуть застосовуватися для формування академічних груп, ведення обліку студентів, оформлення наказів, підготовки довідок, контролю успішності, організації доступу до навчальних ресурсів та взаємодії

між студентом і підрозділами університету. Через це персональні дані повинні бути доступні уповноваженим працівникам, але не повинні відкриватися всім користувачам ІКС.

Обробка персональних даних у закладі вищої освіти відбувається за участю кількох підрозділів. Деканат зазвичай працює з навчальними даними студентів, міжнародний відділ - з документами іноземних студентів, фінансовий відділ - з інформацією щодо оплати, адміністратор системи - з технічними параметрами облікових записів і мережевої інфраструктури. Такий розподіл функцій потребує чіткого розмежування доступу [14].

Розмежування доступу є важливою умовою безпечної обробки персональних даних. Працівник одного підрозділу не повинен мати доступ до всіх даних студента, якщо ці дані не потрібні йому для виконання службових обов’язків. Наприклад, фінансовому відділу може бути потрібна інформація про оплату навчання, але не обов’язково потрібен доступ до всіх навчальних документів. Так само студентський сегмент мережі не повинен мати доступу до внутрішніх ресурсів, де зберігаються персональні дані [16].

У межах ІКС університету персональні дані можуть зберігатися на сервері або в окремій серверній зоні. Це дозволяє централізувати обробку інформації та обмежити доступ до неї з боку користувачів, яким вона не потрібна. Серверна зона повинна бути відокремлена від звичайних робочих сегментів мережі, оскільки саме в ній розміщуються ресурси, що мають найбільше значення для захисту особової конфіденційної інформації.

Важливим процесом є передача персональних даних між підрозділами університету. У реальній роботі дані студента можуть використовуватися деканатом, міжнародним відділом, фінансовим відділом, навчальним відділом або іншими службами. Така передача повинна здійснюватися тільки в межах службової необхідності. Якщо дані передаються без обмежень або стають доступними зайвим користувачам, зростає ризик їх неправомірного використання.

Для зменшення таких ризиків інформаційно-комунікаційна система повинна мати поділ на окремі сегменти. Окремо можуть бути виділені сегмент деканату, сегмент міжнародного відділу, фінансовий сегмент, адміністративний сегмент, серверна зона та студентський сегмент. Завдяки цьому кожна група користувачів працює у своїй частині мережі, а доступ до інших частин може бути обмежений відповідно до функцій підрозділу.

Сегментація мережі дозволяє не тільки впорядкувати роботу користувачів, але й реалізувати принцип мінімізації доступу. Якщо підрозділ не потребує доступу до певного ресурсу, такий доступ не повинен надаватися. У разі помилки користувача або спроби несанкціонованого доступу поділ мережі зменшує ймовірність того, що сторонній користувач отримає доступ до серверної зони або інших важливих ресурсів [17].

Студентський сегмент мережі потребує окремої уваги. Студенти можуть користуватися навчальними або інформаційними ресурсами університету, але вони не повинні мати прямого доступу до внутрішніх ресурсів підрозділів і серверів, де обробляються персональні дані. Тому студентська мережа має бути ізольована від адміністративних сегментів і серверної зони [18].

У результаті аналізу процесів обробки персональних даних в університетській ІКС можна визначити кілька основних проблем, які можуть впливати на відповідність принципам захисту персональних даних. До таких проблем належать ризик надмірного доступу між підрозділами, можливість доступу студентського сегмента до внутрішніх ресурсів, недостатнє відокремлення серверної зони та відсутність чітких технічних правил взаємодії між мережевими сегментами. Якщо такі обмеження не реалізовані на рівні ІКС, то персональні дані можуть бути доступні ширшому колу користувачів, ніж це потрібно для виконання службових функцій.

З погляду GDPR такі проблеми пов’язані насамперед із принципами мінімізації доступу, конфіденційності та захисту даних за замовчуванням. Надмірний доступ між підрозділами може призводити до обробки даних без

службової необхідності, відсутність окремої серверної зони ускладнює контроль доступу до персональних даних, а відкритий доступ студентського сегмента до внутрішньої мережі створює ризик несанкціонованої взаємодії з ресурсами ІКС. Тому для подальшого проєктування необхідно передбачити технічні рішення, які усувають ці недоліки.

Для вирішення виявлених проблем у подальших розділах роботи передбачається розроблення захищеної ІКС із виділенням окремої серверної зони, поділом мережі на логічні сегменти, розмежуванням доступу між підрозділами та ізоляцією студентського сегмента. Такий підхід дозволяє перейти від загального аналізу процесів обробки персональних даних до формування конкретних вимог до мережевої інфраструктури університетського підрозділу.

Адміністративний сегмент також повинен мати обмеження. Адміністратор системи виконує технічні функції, пов’язані з підтримкою працездатності ІКС, налаштуванням мережевого обладнання, облікових записів і доступу. Проте це не означає, що адміністратор повинен мати необмежений доступ до змісту всіх персональних даних. Його повноваження мають відповідати технічним завданням і не створювати зайвих ризиків для конфіденційності.

Окремим етапом обробки є зберігання персональних даних. Дані можуть перебувати в активному використанні під час навчання, після чого частина з них переходить до архівного зберігання. Важливо визначити, які дані потрібні для поточної роботи, які мають зберігатися після завершення навчання, а які можуть бути видалені або знеособлені після завершення мети обробки.

Обмеження строків зберігання є одним із принципів GDPR. Університет не повинен зберігати персональні дані безстроково лише через те, що вони були отримані раніше. Наприклад, частина документів може бути необхідною для підтвердження факту навчання, а інша частина може втратити актуальність після завершення конкретного адміністративного процесу. Тому під час проєктування ІКС потрібно враховувати місце зберігання таких даних і порядок доступу до них.

Під час дистанційної або змішаної форми навчання кількість процесів обробки персональних даних збільшується. Студент може використовувати електронні сервіси, навчальні платформи, електронну пошту та інші засоби взаємодії з університетом. Це збільшує кількість точок доступу до інформації, тому в ІКС необхідно передбачити захист облікових записів, обмеження доступу до внутрішніх ресурсів і захист каналів передавання даних [19].

Важливим елементом обробки є автентифікація користувачів. Кожен працівник або студент, який отримує доступ до ресурсів ІКС, повинен бути ідентифікований. Це дозволяє відокремити права студентів, працівників деканату, міжнародного відділу, фінансового відділу та адміністратора системи. Без цього неможливо правильно організувати доступ до персональних даних [20].

Після автентифікації важливо правильно організувати авторизацію. Авторизація визначає, які саме ресурси доступні користувачу і які дії він може виконувати. Наприклад, студент може мати доступ лише до власних даних і навчальних сервісів, деканат – до навчальних відомостей, міжнародний відділ – до документів іноземних студентів, фінансовий відділ – до інформації щодо оплати, а адміністратор – до технічних налаштувань системи.

У процесах обробки персональних даних важливо враховувати різний рівень чутливості інформації. Контактні дані, копії паспортних документів, фінансові відомості, дані про громадянство та навчальний статус мають різний рівень ризику у випадку розголошення. Тому до різних категорій даних можуть застосовуватися різні рівні доступу та різні технічні обмеження [20].

Персональні дані можуть використовуватися не тільки для поточних освітніх процесів, але й для формування звітності, статистики або підтвердження факту навчання. У таких випадках доцільно застосовувати знеособлення, коли інформація більше не дозволяє ідентифікувати конкретну особу. Наприклад, університет може використовувати узагальнені дані про кількість іноземних студентів або освітні програми без зазначення імен, паспортних даних чи контактної інформації [21].

Узагальнено процес обробки персональних даних під час надання освітніх послуг громадянам ЄС можна подати як послідовність етапів: отримання даних, перевірка, внесення до ІКС, використання під час навчання, передача між уповноваженими підрозділами, зберігання, архівування, видалення або знеособлення. На кожному з цих етапів повинні бути визначені користувачі, які мають право працювати з відповідними даними.

Для наочного подання процесу обробки персональних даних студентів в університетській ІКС доцільно відобразити його у вигляді життєвого циклу (рисунок 1.1). Такий підхід дозволяє показати, що захист персональних даних повинен забезпечуватися не лише на етапі їх зберігання, а протягом усього процесу роботи з інформацією від моменту отримання даних до їх архівування, видалення або знеособлення.


Рисунок 1.1 – Життєвий цикл обробки персональних даних студентів в університетській ІКС

Як видно з рисунка 1.1, персональні дані студентів проходять кілька послідовних етапів обробки. На кожному з них виникають окремі вимоги до захисту інформації. Під час збору та перевірки даних важливо не отримувати надмірну інформацію, під час зберігання розміщувати її у захищеній серверній зоні, під час використання надавати доступ лише уповноваженим підрозділам, а на етапах архівування та видалення обмежувати подальше використання даних

відповідно до визначеної мети обробки.

Проведений аналіз показує, що обробка персональних даних в університеті є постійним організаційно-технічним процесом. Він охоплює різні підрозділи, різні категорії даних, різні ролі користувачів і різні етапи життєвого циклу інформації. Саме тому для забезпечення вимог GDPR потрібна не окрема дія, а цілісна захищена інформаційно-комунікаційна система.

Таким чином, процеси обробки персональних даних під час надання освітніх послуг громадянам ЄС повинні бути побудовані на принципах законності, мінімізації даних, обмеження доступу, конфіденційності та безпечної роботи ІКС. У подальшому це дозволяє сформувати вимоги до захищеної інформаційно-комунікаційної системи університетського підрозділу, які будуть розглянуті в наступному підрозділі.

## 1.3 Визначення вимог до захищеної інформаційно-комунікаційної системи університету та постановка задачі

Після аналізу нормативно-правової бази та процесів обробки персональних даних можна визначити основні вимоги до захищеної інформаційно-комунікаційної системи університету. У межах цієї роботи така система розглядається як сукупність мережевого обладнання, серверної зони, робочих місць підрозділів, студентського сегмента та правил доступу, які забезпечують контрольовану обробку особової конфіденційної інформації студентів відповідно до вимог GDPR.

Під час формування вимог до ІКС у роботі враховуються як положення законодавства України, так і принципи GDPR. Закон України “Про захист персональних даних” визначає загальні вимоги до законної та цільової обробки персональних даних, Закон України “Про захист інформації в інформаційно-комунікаційних системах” обґрунтовує необхідність захисту інформації під час її

обробки в ІКС, а GDPR деталізує принципи мінімізації доступу, конфіденційності, цілісності та захисту даних за замовчуванням [22].

Основна ідея побудови захищеної ІКС полягає в тому, що персональні дані студентів не повинні бути доступні всім користувачам внутрішньої мережі університету. Доступ до них має надаватися лише тим підрозділам і користувачам, яким це необхідно для виконання службових обов'язків. Такий підхід відповідає принципам мінімізації даних, конфіденційності та захисту персональних даних за замовчуванням [2,23].

На основі аналізу процесів обробки персональних даних було визначено основні проблеми, які повинна усунути захищена ІКС. До них належать ризик надмірного доступу між підрозділами, можливість доступу студентського сегмента до внутрішніх ресурсів, недостатнє відокремлення серверної зони та відсутність чітких технічних правил взаємодії між частинами мережі. Такі недоліки можуть призводити до того, що персональні дані стають доступними користувачам, які не мають службової необхідності працювати з ними [24].

З погляду GDPR зазначені проблеми пов'язані насамперед із порушенням принципів мінімізації доступу, конфіденційності та захисту даних за замовчуванням. Якщо підрозділи мають однаковий або надмірний доступ до ресурсів, це суперечить ідеї обробки лише необхідних даних. Якщо студентський сегмент не ізольований від внутрішньої мережі, виникає ризик несанкціонованої взаємодії з ресурсами, де обробляються персональні дані інших осіб [2].

Для усунення ризику надмірного доступу між підрозділами необхідно передбачити поділ мережі університетського підрозділу на окремі логічні сегменти. Кожен сегмент повинен відповідати певній групі користувачів або функціональній зоні ІКС. Зокрема, доцільно виділити сегмент деканату, міжнародного відділу, фінансового відділу, адміністративний сегмент, серверну зону та студентський сегмент. Такий поділ дозволяє обмежити взаємодію між підрозділами та зменшити кількість користувачів, які можуть отримати доступ

до ресурсів із персональними даними [18].

Проблема доступу студентського сегмента до внутрішніх ресурсів вирішується через його ізоляцію від серверної зони та робочих сегментів підрозділів. Студенти можуть користуватися дозволеними навчальними або інформаційними ресурсами, однак не повинні мати прямого доступу до серверів, робочих місць деканату, міжнародного відділу, фінансового сегмента або адміністративної частини ІКС. Це відповідає принципу захисту даних за замовчуванням, оскільки непотрібні напрями доступу блокуються ще на рівні побудови системи [23].

Недостатнє відокремлення персональних даних усувається шляхом виділення окремої серверної зони. У цій зоні повинні розміщуватися основні ресурси, на яких зберігається або обробляється особова конфіденційна інформація студентів. Винесення таких ресурсів в окремий сегмент дозволяє централізувати захист, обмежити доступ до даних і спростити контроль взаємодії між користувачами та серверними ресурсами [24].

Для вирішення проблеми вільної взаємодії між частинами мережі необхідно встановити правила розмежування доступу. Такі правила повинні визначати, які сегменти можуть звертатися до серверної зони, які з'єднання між підрозділами дозволені, а які мають бути заборонені. Це дозволяє реалізувати принцип найменших привілеїв, коли кожен підрозділ отримує лише той рівень доступу, який потрібен для виконання його службових функцій.

Окремою вимогою є захист мережевого обладнання та контроль його розміщення. Сервери, комутатори, маршрутизатори та інші критичні компоненти ІКС не повинні розміщуватися у відкритому доступі для всіх користувачів. Їх необхідно розміщувати в контрольованій зоні, оскільки фізичний доступ до обладнання може створювати ризики несанкціонованого підключення, зміни налаштувань або порушення роботи системи.

Першою вимогою до захищеної ІКС є наявність окремої серверної зони. У цій зоні повинні розміщуватися ресурси, на яких зберігаються або обробляються

персональні дані студентів. Серверна зона має бути відокремлена від звичайних робочих сегментів мережі, а доступ до неї повинен бути обмежений відповідно до функцій користувачів. Це дозволяє зменшити ризик несанкціонованого доступу до особової конфіденційної інформації [25].

Другою важливою вимогою є поділ мережі на окремі сегменти. Університетський підрозділ може включати деканат, міжнародний відділ, фінансовий відділ, адміністратора системи, серверну зону та студентську мережу. Кожен із цих сегментів має власне призначення і повинен мати різні права доступу до інформаційних ресурсів. Завдяки цьому користувачі не отримують доступ до даних, які не потрібні їм для роботи.

Третьою вимогою є розмежування доступу між мережевими сегментами. Для цього в ІКС повинні бути визначені правила, які дозволяють або забороняють взаємодію між окремими частинами мережі. Такий підхід дає змогу реалізувати принцип найменших привілеїв, коли кожен користувач або підрозділ отримує лише той доступ, який потрібен для виконання його функцій.

Особливо важливо обмежити доступ студентського сегмента. Студенти можуть користуватися навчальними або інформаційними ресурсами, але не повинні мати прямого доступу до серверів і внутрішніх сегментів підрозділів, у яких обробляються персональні дані. Ізоляція студентського сегмента зменшує ризик випадкового або навмисного доступу до конфіденційної інформації [25].

Окрему увагу потрібно приділити сегменту адміністратора системи. Адміністратор повинен мати можливість налаштовувати мережеве обладнання, підтримувати роботу ІКС і контролювати доступ до ресурсів. Водночас його права повинні бути пов’язані саме з технічним обслуговуванням системи, а не з необмеженим доступом до змісту всіх персональних даних. Це дозволяє зменшити ризик надмірних привілеїв.

Наступною вимогою є захист мережевого обладнання та правильне його розміщення. Комутатори, маршрутизатори, сервери та інші важливі компоненти ІКС повинні розміщуватися в контрольованій зоні, доступ до якої мають лише

уповноважені особи. Якщо обладнання розташоване у відкритому приміщенні, це створює ризик несанкціонованого підключення, відключення або зміни налаштувань.

Важливою вимогою є визначення IP-адресації та логічної структури мережі. Кожен сегмент ІКС повинен мати окремий адресний простір, що дозволяє простіше контролювати взаємодію між підрозділами. Такий підхід полегшує налаштування правил доступу і допомагає відокремити серверну зону, робочі місця працівників та студентську мережу [26].

Для контролю взаємодії між сегментами доцільно використовувати правила доступу. Вони повинні визначати, які підрозділи можуть звертатися до серверної зони, які з'єднання потрібно заборонити, а які дозволити. Наприклад, студентський сегмент не повинен мати доступу до сервера персональних даних, а доступ до нього мають отримувати лише визначені підрозділи університету.

Вимоги GDPR також передбачають забезпечення конфіденційності та цілісності персональних даних. У контексті ІКС це означає, що персональні дані повинні бути захищені від перегляду або зміни неуповноваженими користувачами. Для цього необхідно поєднувати організаційне визначення ролей користувачів із технічними обмеженнями доступу на рівні мережевої інфраструктури [26].

Ще однією вимогою є доступність основних інформаційних ресурсів для уповноважених користувачів. Захист системи не повинен повністю блокувати роботу підрозділів. Працівники деканату, міжнародного та фінансового відділів повинні мати можливість виконувати свої функції, але в межах чітко визначених прав доступу. Тому захищена ІКС має поєднувати безпеку та працездатність [27].

Для відповідності принципу мінімізації доступу необхідно визначити, які підрозділи працюють з певними категоріями персональних даних. Такий розподіл повинен бути врахований під час проєктування ІКС.

Захищена ІКС також повинна враховувати життєвий цикл персональних даних. Дані надходять до університету, перевіряються, вносяться до системи,

використовуються під час навчання, зберігаються, архівуються або видаляються. На кожному з цих етапів необхідно визначити, які користувачі мають доступ до даних і які технічні обмеження повинні діяти [28].

Сформовані вимоги повинні забезпечити зв’язок між нормативними положеннями та практичною структурою ІКС. Законодавство України визначає необхідність захисту персональних даних та інформації, що обробляється в інформаційно-комунікаційній системі, а принципи GDPR конкретизують, як саме має бути організована така обробка з погляду мінімізації доступу, конфіденційності та захисту даних за замовчуванням. Тому вимоги до ІКС у цій роботі розглядаються не як загальні рекомендації, а як основа для подальшого проєктування конкретної мережевої структури університетського підрозділу.

Важливо, що захищена ІКС повинна не лише обмежувати небажаний доступ, але й забезпечувати нормальну роботу підрозділів університету. Деканат, міжнародний відділ і фінансовий відділ повинні мати можливість працювати з необхідними ресурсами серверної зони, однак їхня взаємодія з іншими сегментами має бути обмежена відповідно до службових функцій. Такий підхід дозволяє поєднати вимоги безпеки з практичними потребами освітнього процесу та підготувати основу для подальшого проєктування захищеної ІКС.

На основі проведеного аналізу постановка задачі полягає в розробленні захищеної інформаційно-комунікаційної системи університетського підрозділу, у якій персональні дані студентів зберігаються в окремій серверній зоні, робочі місця підрозділів поділені на окремі мережеві сегменти, а доступ між ними обмежений відповідно до функцій користувачів. Така система повинна усунути ризики надмірного доступу, відкритої взаємодії студентського сегмента з внутрішніми ресурсами та неконтрольованого доступу до серверної зони.

У межах постановки задачі потрібно передбачити структуру ІКС, яка включає серверну зону, сегмент деканату, сегмент міжнародного відділу, фінансовий сегмент, адміністративний сегмент і студентський сегмент. Для кожного з них необхідно визначити призначення, склад користувачів і допустимий рівень

доступу до персональних даних або інших інформаційних ресурсів [27].

Також потрібно визначити правила взаємодії між сегментами. Основним обмеженням є заборона прямого доступу студентського сегмента до серверної зони та внутрішніх сегментів підрозділів. Доступ до сервера персональних даних мають отримувати лише ті підрозділи, які беруть участь в обробці відповідної інформації. Це дозволяє реалізувати принцип мінімізації доступу.

У результаті виконання поставленої задачі повинна бути отримана захищена ІКС університетського підрозділу, яка відповідає основним принципам GDPR. Вона повинна забезпечувати розмежування доступу між користувачами, ізоляцію студентського сегмента, захист серверної зони, контроль взаємодії між частинами мережі та безпечну обробку особової конфіденційної інформації.

Таким чином, у підрозділі було сформовано вимоги до захищеної інформаційно-комунікаційної системи університетського підрозділу та визначено постановку задачі. Основними вимогами є виділення серверної зони, поділ мережі на окремі сегменти, розмежування доступу між підрозділами, ізоляція студентської мережі, захист мережевого обладнання та контроль взаємодії між частинами ІКС. Ці вимоги враховують положення законодавства України щодо захисту персональних даних та інформації в ІКС, а також принципи GDPR щодо мінімізації доступу, конфіденційності та захисту даних за замовчуванням.

# 2 ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ УНІВЕРСИТЕТУ

## 2.1 Концептуальне проєктування

Концептуальне проєктування є початковим етапом розроблення захищеної інформаційно-комунікаційної системи університету. На цьому етапі визначається загальна структура системи, її основні складові, користувачі, підрозділи, інформаційні ресурси та принципи доступу до персональних даних. Концептуальна модель не передбачає детального опису всіх технічних налаштувань, але дає змогу визначити, як саме має бути організована ІКС для безпечної обробки особової конфіденційної інформації студентів [29, 30].

У межах даної роботи захищена ІКС розглядається як сукупність мережевого обладнання, серверної зони, робочих місць працівників університетського підрозділу, студентського сегмента та правил доступу між окремими частинами системи. Основним призначенням такої ІКС є забезпечення контрольованої обробки персональних даних студентів відповідно до принципів GDPR, зокрема мінімізації доступу, конфіденційності, цілісності та захисту даних за замовчуванням.

Перед проєктуванням захищеної ІКС було проаналізовано наявну інформаційно-комунікаційну систему університетського підрозділу. Вона забезпечувала базове підключення робочих місць працівників, серверних ресурсів і студентського доступу до мережевої інфраструктури. У такій системі вже були наявні основні елементи для виконання робочих процесів: комп’ютери працівників підрозділів, серверні ресурси, мережеве обладнання та можливість підключення студентів до окремих інформаційних або навчальних ресурсів [31].

Наявна ІКС дозволяла виконувати основні завдання університетського підрозділу, зокрема обробку навчальних даних студентів, роботу з документами іноземних студентів, фінансовий супровід освітніх послуг і технічне обслуговування мережевої інфраструктури. Водночас така система потребувала вдосконалення,

оскільки її структура не забезпечувала достатньо чіткого розмежування доступу між підрозділами, студентським сегментом і серверними ресурсами.

Основним недоліком наявної ІКС був ризик надмірного доступу до персональних даних. Якщо робочі місця деканату, міжнародного відділу, фінансового відділу, адміністратора системи та студентський сегмент не розмежовані на достатньому рівні, користувачі можуть отримувати доступ до ресурсів, які не потрібні їм для виконання службових функцій. Така ситуація не відповідає принципу мінімізації доступу, оскільки персональні дані мають бути доступні лише тим користувачам, яким вони необхідні для виконання конкретних завдань [31].

Окремою проблемою була недостатня ізоляція студентського сегмента. Студенти можуть бути користувачами навчальних або інформаційних сервісів, однак вони не повинні мати доступу до серверної зони, робочих місць деканату, міжнародного відділу, фінансового відділу або адміністративного сегмента. За відсутності чітких технічних обмежень студентська мережа може створювати додатковий ризик для конфіденційності персональних даних, що суперечить принципу захисту даних за замовчуванням [32].

Також було визначено, що серверна зона потребує чіткого відокремлення від робочих і студентських сегментів. Серверні ресурси, на яких зберігаються або обробляються персональні дані студентів, повинні бути розміщені в окремій захищеній частині ІКС. Це дозволяє контролювати доступ до них, обмежити кількість можливих напрямів взаємодії та зменшити ризик випадкового або навмисного розкриття особової конфіденційної інформації.

Отже, аналіз наявної ІКС показав, що для приведення її до вимог захисту персональних даних необхідно виконати кілька проєктних змін: виділити окрему серверну зону, розділити мережу на функціональні сегменти, ізолювати студентський сегмент від внутрішніх ресурсів та запровадити правила розмежування доступу між підрозділами. Саме ці недоліки стали основою для подальшого концептуального проєктування захищеної ІКС.

Об’єктом проєктування є університетський підрозділ, у якому здійснюється обробка персональних даних студентів, зокрема громадян країн Європейського Союзу. У структурі такого підрозділу доцільно виділити деканат, міжнародний відділ, фінансовий відділ, адміністратора системи, серверну зону та студентський сегмент мережі. Кожен із цих елементів виконує окрему функцію та має різний рівень доступу до інформаційних ресурсів.

Деканат у проєктованій ІКС виконує функції, пов’язані з організацією освітнього процесу. Працівники деканату можуть працювати з даними про академічні групи, освітні програми, навчальний статус студентів, заяви, довідки та інші документи, необхідні для супроводу навчання. При цьому доступ деканату повинен бути обмежений лише тими даними, які потрібні для виконання його службових обов’язків.

Міжнародний відділ працює з персональними даними іноземних студентів. До таких даних можуть належати документи, що підтверджують особу, громадянство, попередню освіту, право на перебування в Україні, контактні відомості та інша інформація, необхідна для супроводу громадян ЄС під час вступу та навчання. Оскільки ці дані можуть мати підвищену чутливість, доступ до них повинен бути обмежений лише для уповноважених працівників [33].

Фінансовий відділ обробляє інформацію, пов’язану з оплатою освітніх послуг. Йому можуть бути потрібні дані про студента, договір, форму навчання, суму оплати та стан фінансових зобов’язань. Водночас фінансовий відділ не повинен мати доступу до всіх навчальних або паспортних даних, якщо вони не потрібні для виконання його функцій. Такий підхід відповідає принципу мінімізації доступу.

Адміністратор системи відповідає за технічну працездатність ІКС, підтримку мережевої інфраструктури, налаштування доступу до окремих сегментів та обслуговування серверної зони. Його функції повинні бути пов’язані насамперед із технічним забезпеченням роботи системи. Надання адміністратору необмеженого доступу до змісту всіх персональних даних є

небажаним, оскільки це створює додаткові ризики для конфіденційності [34].

Серверна зона є центральним елементом захищеної ІКС. У ній розміщуються інформаційні ресурси, на яких зберігаються або обробляються персональні дані студентів. Саме до цієї зони мають застосовуватися найбільш суворі обмеження доступу. Серверна зона повинна бути відокремлена від робочих сегментів підрозділів і студентської мережі, а доступ до неї має надаватися лише визначеним користувачам.

Студентський сегмент призначений для підключення студентів до дозволених навчальних або інформаційних ресурсів. Проте цей сегмент не повинен мати прямого доступу до серверної зони та внутрішніх робочих сегментів підрозділів. Ізоляція студентського сегмента є важливою умовою захисту персональних даних, оскільки зменшує ризик несанкціонованого доступу до внутрішніх ресурсів університету.

Концептуальна модель ІКС передбачає поділ мережі на окремі логічні частини відповідно до функцій користувачів. Такий поділ дозволяє відокремити робочі місця деканату, міжнародного відділу, фінансового відділу, адміністратора системи, серверну зону та студентський сегмент. У результаті кожна група користувачів працює у власному сегменті, а взаємодія між сегментами контролюється відповідно до визначених правил доступу [35].

Такий підхід відповідає принципу мінімізації доступу, який є одним із важливих принципів GDPR. Користувачі не повинні отримувати доступ до всіх ресурсів ІКС лише через факт підключення до внутрішньої мережі університету. Доступ має надаватися відповідно до ролі користувача, функцій підрозділу та необхідності роботи з певними категоріями персональних даних.

У проєктованій ІКС персональні дані студентів повинні зберігатися централізовано в серверній зоні, а не на окремих робочих місцях працівників. Це дозволяє краще контролювати доступ до даних і зменшити ризик їх випадкового розповсюдження між користувачами. Робочі місця повинні отримувати доступ до відповідних ресурсів лише в межах дозволених правил взаємодії.

Важливим елементом концептуального проєктування є визначення інформаційних потоків. У межах університетського підрозділу персональні дані можуть надходити від студента до міжнародного відділу або деканату, після чого використовуватися для організації навчання, фінансового обліку та адміністративного супроводу. Передача даних між підрозділами повинна бути обмежена службовою необхідністю.

Наприклад, міжнародний відділ може працювати з документами іноземного студента, деканат – з навчальними відомостями, фінансовий відділ – з інформацією щодо оплати, а адміністратор – з технічними параметрами роботи системи. Такий розподіл дозволяє уникнути ситуації, коли всі підрозділи мають однаковий доступ до всіх персональних даних.

Концептуальна модель також передбачає фізичне розміщення основних компонентів ІКС. Сервери та основне мережеве обладнання доцільно розміщувати в окремому приміщенні або контрольованій зоні. Робочі місця працівників розташовуються у відповідних кабінетах підрозділів, а студентський доступ організовується окремо від внутрішньої адміністративної мережі. Це дозволяє поєднати логічний і фізичний рівні захисту.

Для наочного відображення фізичного розміщення основних зон захищеної ІКС доцільно використати план приміщень університетського підрозділу. У плані (рисунок 2.1) студентська зона розміщується біля входу і відокремлюється від службових кабінетів, у яких працюють працівники деканату, міжнародного та фінансового відділів. Серверна зона розміщується окремо від студентської частини, що дозволяє обмежити фізичний доступ до обладнання та ресурсів, у яких обробляються персональні дані студентів.

Як видно з рисунка 2.1, студентська зона відокремлена від службових приміщень університетського підрозділу. Такий підхід є важливим, оскільки студенти можуть користуватися дозволеними навчальними або інформаційними ресурсами, але не повинні мати прямого доступу до внутрішніх робочих зон і серверної. Розміщення серверної зони в окремому приміщенні дозволяє

додатково захистити обладнання, на якому зберігаються або обробляються персональні дані студентів.

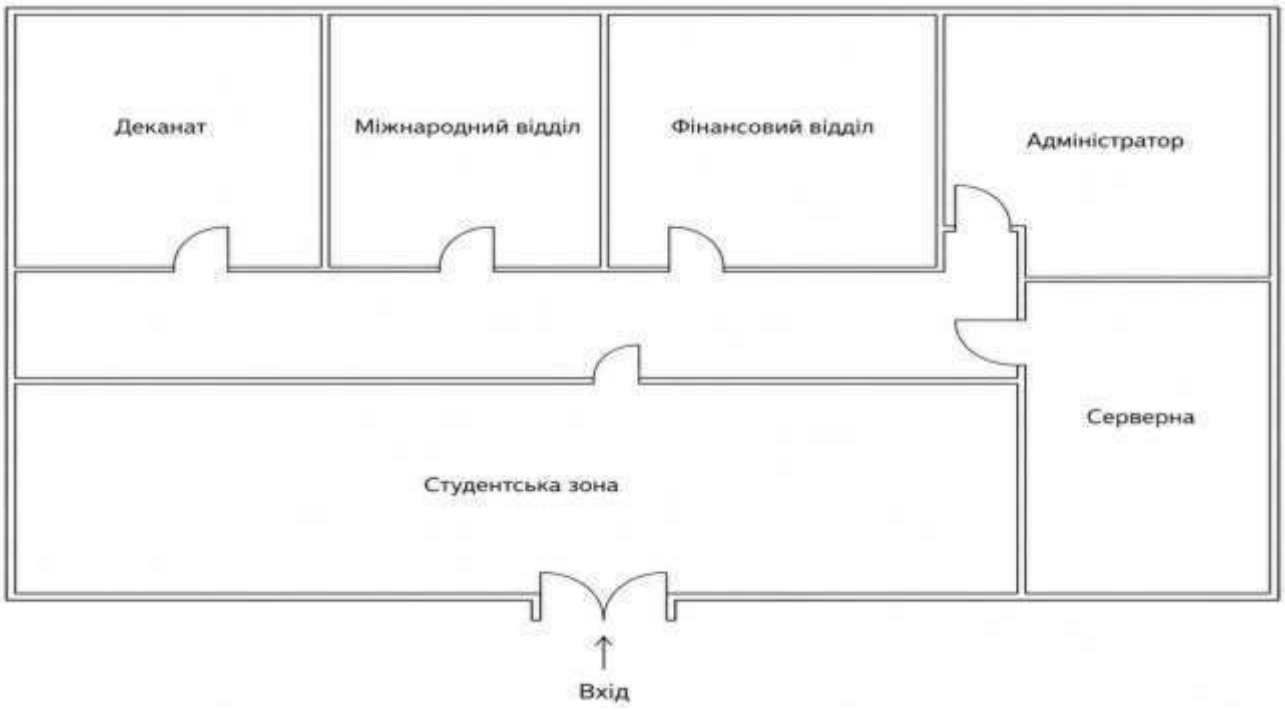



Рисунок 2.1 – План приміщень університетського підрозділу з виділенням основних зон ІКС

Під час концептуального проєктування потрібно враховувати не лише обмеження доступу, але й працездатність системи. Захист не повинен повністю блокувати нормальну роботу університетських підрозділів. Працівники деканату, міжнародного та фінансового відділів повинні мати можливість виконувати свої функції, але тільки в межах чітко визначених прав доступу. Тому проєктована ІКС має поєднувати безпеку, стабільність роботи та зручність використання.

З точки зору GDPR запропонована концептуальна модель дозволяє реалізувати кілька важливих принципів. Мінімізація проявляється в тому, що кожен підрозділ отримує доступ лише до необхідних ресурсів. Конфіденційність забезпечується через ізоляцію серверної зони та обмеження взаємодії між сегментами. Захист даних за замовчуванням реалізується через те, що

студентський сегмент не має доступу до внутрішніх ресурсів університету.

Таким чином, концептуальне проєктування захищеної ІКС університету передбачає визначення основних підрозділів, інформаційних ресурсів, серверної зони, студентського сегмента та принципів розмежування доступу. Запропонована структура створює основу для подальшого проєктування мережевої архітектури, визначення адресації, сегментації мережі та правил взаємодії між окремими частинами системи.

## 2.2 Проєктування мережевої архітектури

Проєктування мережевої архітектури є важливим етапом створення захищеної інформаційно-комунікаційної системи університету. На цьому етапі визначається склад мережевого обладнання, розміщення серверної зони, підключення робочих місць підрозділів, студентський сегмент та загальна логіка взаємодії між частинами системи. Мережева архітектура повинна бути побудована так, щоб забезпечити доступність ресурсів для уповноважених користувачів і водночас обмежити доступ до персональних даних студентів [35].

У межах даної роботи мережа університетського підрозділу розглядається як локальна інформаційно-комунікаційна система, у якій обробляється особова конфіденційна інформація студентів. До складу такої системи входять робочі станції працівників деканату, міжнародного відділу, фінансового відділу, адміністратора системи, серверна зона, мережеве обладнання та студентський сегмент доступу. Кожен із цих елементів має власне призначення і повинен бути підключений до мережі відповідно до визначених вимог безпеки [36].

З урахуванням недоліків наявної ІКС мережева архітектура повинна забезпечити чіткіший поділ між серверними ресурсами, робочими місцями підрозділів і студентським сегментом. Основна увага приділяється тому, щоб усунути ризик надмірного доступу, відокремити ресурси з персональними

даними від загальної мережі та створити основу для подальшого налаштування правил розмежування доступу між сегментами.

Центральним елементом мережевої архітектури є серверна зона. У ній розміщуються ресурси, на яких зберігаються або обробляються персональні дані студентів. До таких ресурсів може належати сервер персональних даних, сервер внутрішніх сервісів або інший інформаційний ресурс, який використовується підрозділами університету. Серверна зона повинна бути відокремлена від робочих сегментів і студентської мережі, оскільки саме вона містить найбільш важливу для захисту інформацію.

Для забезпечення доступу до серверної зони передбачається використання мережевого обладнання, яке дозволяє об’єднати всі компоненти ІКС в єдину систему. До такого обладнання належать комутатор, маршрутизатор або пристрій, що виконує функції маршрутизації між сегментами мережі. Комутатор забезпечує підключення робочих місць і серверів, а маршрутизатор дає змогу організувати взаємодію між окремими сегментами відповідно до встановлених правил доступу [37].

Робочі місця працівників університетського підрозділу розміщуються відповідно до функцій окремих структурних одиниць. Такий розподіл дозволяє врахувати принцип мінімізації доступу, передбачений GDPR.

Мережева архітектура повинна враховувати, що різні підрозділи університету не повинні мати однаковий рівень доступу до персональних даних. Якщо всі робочі місця підключені до однієї спільної мережі без логічного поділу, це створює ризик надмірного доступу до інформаційних ресурсів. Тому під час проєктування передбачається поділ мережі на окремі функціональні частини, що відповідають основним підрозділам і типам користувачів.

У проєктованій ІКС доцільно передбачити окремі сегменти для деканату, міжнародного відділу, фінансового відділу, адміністратора системи, серверної зони та студентської мережі. Такий поділ дозволяє обмежити доступ між частинами мережі та забезпечити більш контрольовану обробку персональних

даних. Кожен сегмент виконує власну функцію і має взаємодіяти з іншими сегментами лише в межах службової необхідності.

Сегмент деканату призначений для робочих місць працівників, які організовують навчальний процес і працюють з даними студентів. У цьому сегменті можуть розміщуватися комп'ютери працівників, які використовуються для перегляду навчальної інформації, оформлення довідок, підготовки наказів або роботи з академічними групами. Доступ цього сегмента до серверної зони має бути дозволений лише до тих ресурсів, які потрібні для виконання функцій деканату.

Сегмент міжнародного відділу призначений для роботи з персональними даними іноземних студентів. Працівники цього відділу можуть обробляти копії документів, дані про громадянство, попередню освіту, контактну інформацію та інші відомості, необхідні для супроводу громадян ЄС. Оскільки ці дані можуть бути конфіденційними, доступ до них повинен бути обмежений, а сам сегмент має бути відокремлений від інших частин мережі [38].

Фінансовий сегмент використовується для роботи з інформацією щодо оплати освітніх послуг. У цьому сегменті можуть розміщуватися робочі місця працівників, які виконують фінансовий облік, перевіряють стан оплати або працюють з договорами. Фінансовий відділ повинен мати доступ лише до тих даних, які потрібні для виконання фінансових функцій, і не повинен отримувати необмежений доступ до всіх навчальних або паспортних даних студентів.

Адміністративний сегмент призначений для роботи адміністратора системи. Він використовується для технічного обслуговування мережевої інфраструктури, контролю працездатності обладнання, налаштування доступу та підтримки серверної зони. Цей сегмент повинен мати окремий рівень доступу, оскільки від нього залежить стабільність роботи всієї ІКС. Водночас права адміністратора повинні бути обмежені функціями технічного обслуговування [39].

Студентський сегмент призначений для підключення студентів до дозволених освітніх або інформаційних ресурсів. Він може використовуватися для доступу до навчальних матеріалів, загальних сервісів або мережевих послуг,

які не містять конфіденційної інформації. Водночас студентський сегмент не повинен мати прямого доступу до серверної зони, робочих місць працівників деканату, міжнародного або фінансового відділів.

Ізоляція студентського сегмента є важливою вимогою до мережевої архітектури. Студенти є окремою групою користувачів і не виконують службових функцій з обробки персональних даних інших осіб. Тому їхній доступ до внутрішньої мережі університетського підрозділу повинен бути обмеженим. Такий підхід відповідає принципу захисту даних за замовчуванням, коли користувач не отримує зайвих прав доступу без необхідності.

Мережеве обладнання в проєктованій ІКС повинно забезпечувати об’єднання сегментів у єдину керовану структуру. Комутатор використовується для підключення робочих станцій і серверів, а маршрутизатор або інший пристрій рівня маршрутизації забезпечує обмін даними між сегментами. При цьому взаємодія між сегментами не повинна бути вільною, а має визначатися відповідно до ролей користувачів і потреб підрозділів.

Для серверної зони доцільно передбачити окреме підключення до мережевого обладнання. Це дозволяє відокремити сервери від робочих місць користувачів і контролювати доступ до них через правила взаємодії між сегментами. Такий підхід зменшує ризик випадкового або навмисного доступу до персональних даних з боку користувачів, які не беруть участі в їх обробці.

Під час проєктування мережевої архітектури також потрібно врахувати фізичне розміщення обладнання. Сервери, маршрутизатор і основний комутатор доцільно розміщувати в окремій серверній зоні або приміщенні з обмеженим доступом. Робочі місця працівників повинні бути розташовані в кабінетах відповідних підрозділів, а студентський доступ має бути організований окремо від адміністративної частини мережі.

Фізичне розділення приміщень доповнює логічне розмежування мережі. Якщо серверна зона розташована окремо, це зменшує ризик прямого доступу сторонніх осіб до обладнання. Якщо ж робочі місця різних підрозділів

підключені до відповідних сегментів, це допомагає підтримувати впорядковану структуру ІКС і спрощує подальше налаштування правил доступу.

У проєктованій архітектурі важливо забезпечити баланс між захистом і працездатністю системи. Надмірні обмеження можуть ускладнити роботу підрозділів, а надто відкритий доступ створює ризики для персональних даних. Тому архітектура повинна передбачати такий рівень доступу, який дозволяє працівникам виконувати службові завдання, але не відкриває їм зайві ресурси.

З точки зору GDPR така мережева архітектура дозволяє реалізувати кілька важливих принципів. Мінімізація проявляється у тому, що підрозділи мають доступ лише до необхідних ресурсів. Конфіденційність забезпечується через обмеження доступу до серверної зони. Цілісність підтримується тим, що змінювати або використовувати персональні дані можуть лише уповноважені користувачі відповідних сегментів.

У межах цієї архітектури імплементується не окремий програмний сервіс, а захищена мережева структура ІКС. Її основними елементами є фізичне підключення робочих місць і серверів, логічне відокремлення функціональних зон, централізоване розміщення ресурсів із персональними даними та контрольована взаємодія між сегментами. Саме ці рішення надалі деталізуються через сегментацію мережі, IP-адресацію та правила доступу.

У межах подальшого проєктування на основі визначеної архітектури необхідно деталізувати логічний поділ мережі, визначити адресацію для кожного сегмента та сформувати правила доступу між ними. Це дозволить перейти від загального опису архітектури до практичного проєктування сегментації мережі та розмежування взаємодії між підрозділами університету.

Отже, мережева архітектура захищеної ІКС університету повинна включати серверну зону, робочі сегменти основних підрозділів, адміністративний сегмент, студентську мережу та мережеве обладнання, яке забезпечує контрольовану взаємодію між ними. Така архітектура створює основу для безпечної обробки персональних даних студентів і дозволяє поєднати

вимоги законодавства України щодо захисту інформації в ІКС із принципами GDPR щодо мінімізації доступу, конфіденційності та захисту даних за замовчуванням.

## 2.3 Проєктування сегментації мережі та правил розмежування доступу

Сегментація мережі є одним із основних елементів проєктування захищеної інформаційно-комунікаційної системи університету. Якщо загальна мережева архітектура визначає склад системи та взаємне розміщення її компонентів, то сегментація дає змогу розділити мережу на окремі логічні частини відповідно до функцій користувачів і підрозділів. Для системи, у якій обробляються персональні дані студентів, такий поділ має важливе значення, оскільки дозволяє обмежити доступ до конфіденційної інформації та зменшити ризик її несанкціонованого використання.

У межах цієї роботи сегментація мережі розглядається як технічний спосіб реалізації вимог захисту персональних даних в ІКС. Законодавство України обґрунтовує необхідність захисту інформації, що обробляється в інформаційно-комунікаційній системі, а GDPR деталізує принципи мінімізації, конфіденційності та захисту даних за замовчуванням. У практичному вигляді це означає, що користувачі не повинні мати доступу до всіх ресурсів системи лише через факт підключення до мережі. Доступ має надаватися відповідно до ролі користувача, функцій підрозділу та необхідності роботи з певними даними [40].

Основна мета сегментації полягає в тому, щоб відокремити робочі місця різних груп користувачів, серверну зону та студентську мережу. Університетський підрозділ обробляє різні категорії персональних даних: навчальні відомості, документи іноземних студентів, контактні дані, фінансову інформацію та технічні дані облікових записів. Оскільки ці дані використовуються різними підрозділами, мережа не повинна бути єдиним

відкритим середовищем без обмежень.

У проєктованій ІКС доцільно виділити кілька основних сегментів: сегмент деканату, сегмент міжнародного відділу, фінансовий сегмент, адміністративний сегмент, серверну зону та студентський сегмент. Кожен із цих сегментів має окреме призначення і повинен мати власні правила взаємодії з іншими частинами системи. Такий підхід дозволяє побудувати більш контрольовану мережеву інфраструктуру та зменшити кількість користувачів, які можуть отримати доступ до ресурсів із персональними даними.

Сегмент деканату призначений для працівників, які забезпечують організацію освітнього процесу. У цьому сегменті можуть розміщуватися робочі станції працівників, які працюють з навчальними даними студентів, академічними групами, заявами, довідками та іншими документами, пов’язаними з навчанням. Деканат може мати доступ до окремих ресурсів серверної зони, але лише до тих, які потрібні для виконання його функцій. Це відповідає принципу мінімізації доступу, оскільки працівники деканату не повинні отримувати необмежений доступ до всієї інформації про студента.

Сегмент міжнародного відділу використовується для роботи з даними іноземних студентів, зокрема громадян країн Європейського Союзу. У цьому сегменті можуть оброблятися копії документів, відомості про громадянство, попередню освіту, контактні дані та інформація, необхідна для адміністративного супроводу іноземного студента. Оскільки такі дані можуть бути чутливими, доступ до них повинен бути обмежений лише працівниками, які безпосередньо виконують відповідні функції.

Фінансовий сегмент призначений для працівників, які обробляють інформацію щодо оплати освітніх послуг. У цьому сегменті можуть використовуватися дані про студента, договір, форму навчання, стан оплати та фінансові зобов’язання. При цьому фінансовий відділ не повинен мати доступу до всіх навчальних або паспортних даних студента, якщо вони не потрібні для фінансового обліку. Таке розмежування дозволяє зменшити надмірну обробку

персональних даних і краще узгоджується з вимогами GDPR.

Адміністративний сегмент призначений для адміністратора системи, який відповідає за технічну працездатність ІКС. Через цей сегмент можуть виконуватися налаштування мережевого обладнання, контроль роботи серверної зони, підтримка доступності ресурсів та технічне обслуговування системи. Водночас адміністративний сегмент не повинен розглядатися як зона повного необмеженого доступу до всього змісту персональних даних. Повноваження адміністратора мають бути пов’язані насамперед із технічною підтримкою ІКС.

Серверна зона є найбільш важливою частиною проєктованої системи. У ній розміщуються сервери або інформаційні ресурси, на яких зберігаються персональні дані студентів. Саме ця зона повинна бути найбільш захищеною, оскільки порушення доступу до неї може призвести до розкриття або зміни особової конфіденційної інформації. Серверна зона повинна бути відокремлена від усіх робочих сегментів, а доступ до неї має надаватися лише через визначені правила.

Студентський сегмент призначений для підключення студентів до дозволених навчальних або інформаційних ресурсів. Студенти можуть використовувати мережу для доступу до навчальних матеріалів, загальних сервісів або інших ресурсів, які не містять конфіденційної інформації інших осіб. Однак студентський сегмент не повинен мати прямого доступу до серверної зони, робочих місць деканату, міжнародного відділу, фінансового відділу або адміністративного сегмента.

Ізоляція студентського сегмента є однією з ключових вимог до захищеної ІКС. Студенти є користувачами освітніх сервісів, але вони не виконують службових функцій з обробки персональних даних інших студентів. Тому доступ студентської мережі до внутрішніх ресурсів університетського підрозділу повинен бути заборонений або суттєво обмежений. Такий підхід відповідає принципу захисту даних за замовчуванням, оскільки небезпечні або непотрібні з’єднання не дозволяються з самого початку.

Для реалізації логічного поділу мережі доцільно використовувати VLAN. Такий підхід дозволяє розділити пристрої різних підрозділів на окремі логічні мережі навіть у межах однієї фізичної інфраструктури. Наприклад, робочі станції деканату можуть належати до одного VLAN, міжнародного відділу – до іншого, фінансового відділу – до третього, а серверна зона і студентський сегмент можуть бути винесені в окремі VLAN. Це спрощує подальше налаштування правил доступу між частинами системи [29].

Використання VLAN дозволяє зробити структуру мережі більш впорядкованою. Кожен сегмент отримує власну логічну область, у межах якої працюють пристрої відповідної групи користувачів. Завдяки цьому зменшується кількість непотрібних з'єднань між пристроями різних підрозділів, а доступ до серверної зони може контролюватися централізовано. Для ІКС, у якій обробляються персональні дані, це є важливою умовою безпечної роботи.

Водночас сам поділ мережі на VLAN не є повним механізмом захисту персональних даних. VLAN лише створює логічні межі між групами пристроїв, але для реального контролю доступу необхідно визначити правила обміну трафіком між цими логічними частинами. Якщо всі VLAN можуть вільно взаємодіяти між собою, то ризик надмірного доступу фактично зберігається. Тому сегментація повинна поєднуватися з правилами розмежування доступу, які дозволяють службові з'єднання та блокують непотрібні напрями взаємодії [28].

Для наочного відображення логічного поділу мережі та правил взаємодії між сегментами доцільно подати схему сегментації захищеної ІКС університету. На такій схемі окремо виділяються сегменти адміністратора, деканату, міжнародного відділу, фінансового відділу, серверної зони та студентської мережі. Також показується, які напрями доступу дозволені, які обмежені, а які повинні бути заборонені відповідно до принципів GDPR.

Перед поданням схеми доцільно уточнити, що вона відображає не фізичне розміщення пристроїв, а логічну модель доступу між частинами ІКС. Основний зміст такої моделі полягає у визначенні дозволених і заборонених напрямів

взаємодії між сегментами. Тому на схемі важливо показати не лише сам факт поділу мережі на окремі частини, а й те, які сегменти можуть звертатися до серверної зони, які мають обмежений доступ, а які повинні бути ізольовані від внутрішніх ресурсів університету.

У подальшій практичній реалізації логічна схема (рисунок 2.2) використовується як основа для налаштування мережевої сегментації та правил доступу. Тобто спочатку визначається проєктна логіка взаємодії між підрозділами, а вже потім вона відображається у конкретних технічних рішеннях: окремих сегментах мережі, адресації та правилах фільтрації трафіку. Це дозволяє перейти від загальних вимог захисту персональних даних до побудови конкретної захищеної ІКС університетського підрозділу.

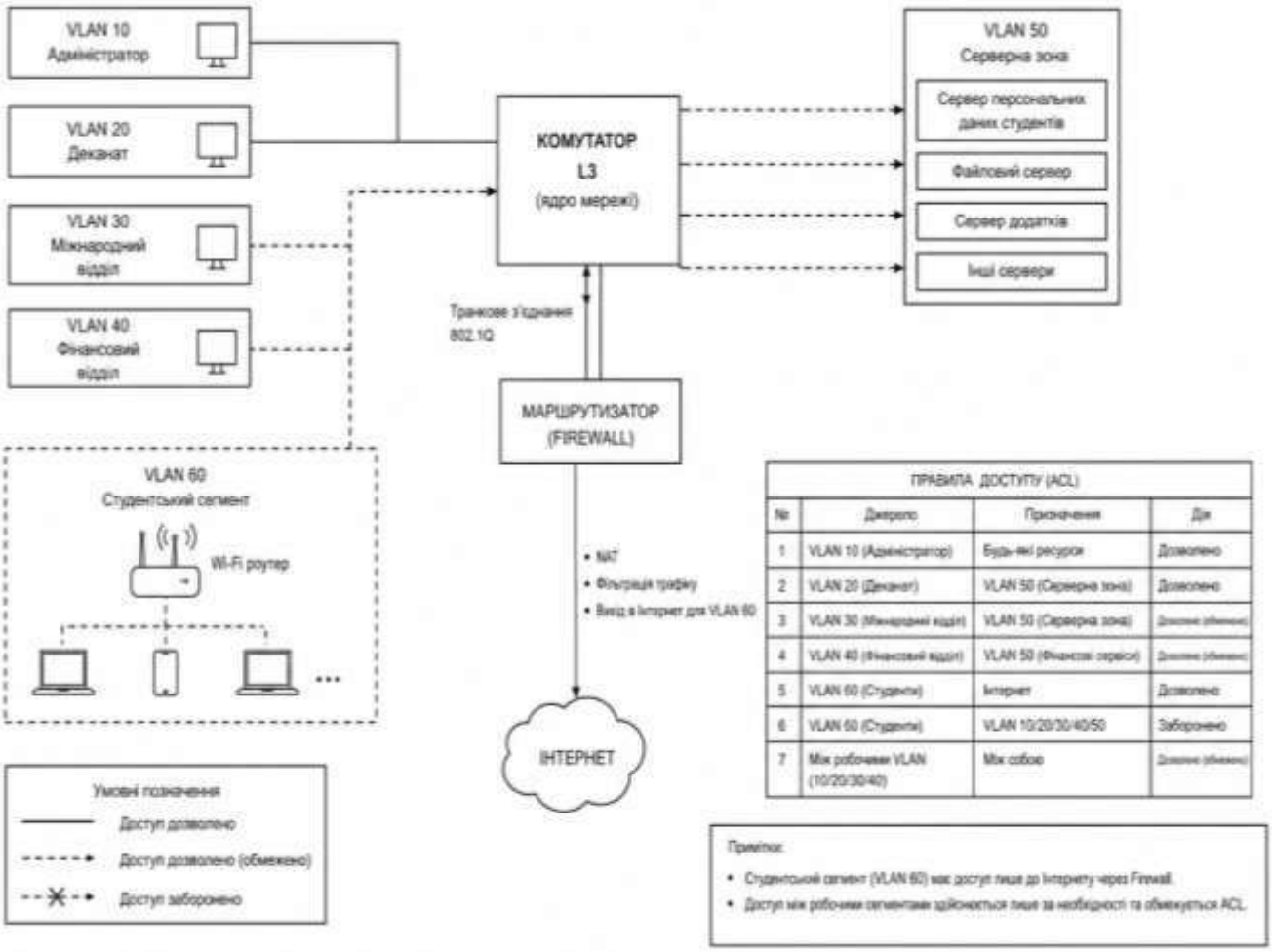



Рисунок 2.2 – Схема сегментації мереж та розмежування доступу в захищеній ІКС університету

Як видно з рисунка 2.2, серверна зона виділена в окремий сегмент і є центральним ресурсом, до якого звертаються лише визначені підрозділи. Адміністратор має доступ до мережевого обладнання та службових ресурсів для технічного обслуговування ІКС. Деканат, міжнародний відділ і фінансовий відділ отримують доступ до серверної зони лише в межах своїх службових функцій. Студентський сегмент має доступ до Інтернету, але не має доступу до серверної зони та внутрішніх робочих сегментів університету.

Списки контролю доступу ACL можуть використовуватися для обмеження взаємодії між мережевими сегментами. Вони дозволяють визначити, з яких сегментів дозволено звертатися до певних ресурсів, а з яких доступ має бути заборонений. Наприклад, студентський сегмент не повинен мати доступу до серверної зони, а сегмент деканату може мати доступ лише до необхідних серверних ресурсів. Це дозволяє реалізувати принцип найменших привілеїв на мережевому рівні [30, 35].

Для сегмента деканату доцільно дозволити доступ до тих серверних ресурсів, які використовуються для обліку навчальних даних студентів. При цьому доступ до ресурсів фінансового відділу або технічних ресурсів адміністратора має бути обмежений. Такий підхід дозволяє деканату виконувати свої функції, але не створює надмірного доступу до інформації, яка не потрібна для організації освітнього процесу.

Для сегмента міжнародного відділу потрібно передбачити доступ до ресурсів, пов’язаних з обробкою даних іноземних студентів. Це можуть бути документи, контактні відомості, інформація про громадянство та освітній супровід. Водночас міжнародний відділ не повинен отримувати необмежений доступ до фінансових або технічних ресурсів системи, якщо такі дані не потрібні для виконання його службових функцій.

Для фінансового сегмента доцільно дозволити доступ лише до ресурсів, пов’язаних з оплатою освітніх послуг. Такий сегмент не повинен мати повного доступу до документів іноземних студентів або навчальних даних, якщо це не

обґрунтовано його функціями. Завдяки цьому зменшується ризик зайвої обробки персональних даних і забезпечується більш чітке розмежування відповідальності між підрозділами.

Адміністративний сегмент повинен мати доступ до мережевого обладнання та технічних ресурсів, необхідних для підтримки працездатності ІКС. Водночас доступ адміністратора до змісту персональних даних має бути обмежений настільки, наскільки це можливо в межах технічної моделі. Такий підхід важливий, тому що адміністратор має високий рівень технічних прав, і неправильне визначення його доступу може створити додаткові ризики.

Серверна зона повинна приймати з’єднання лише від тих сегментів, яким це необхідно для роботи. Будь-які непотрібні з’єднання до серверної зони повинні бути заборонені. Особливо це стосується студентського сегмента, який не повинен мати прямої взаємодії з сервером персональних даних. Такий підхід дозволяє зменшити поверхню атаки та обмежити можливість випадкового доступу до конфіденційної інформації.

Для студентського сегмента основним правилом має бути ізоляція від внутрішніх ресурсів університетського підрозділу. Студентська мережа може мати доступ до загальних навчальних або зовнішніх ресурсів, але не до внутрішніх сегментів деканату, міжнародного відділу, фінансового відділу та серверної зони. Таке обмеження є логічним, оскільки студенти не повинні взаємодіяти з ресурсами, у яких обробляються персональні дані інших осіб.

Проєктування правил доступу повинно враховувати не лише заборони, але й дозволені потоки даних. Повна ізоляція всіх сегментів зробила б систему непрацездатною, оскільки підрозділи не змогли б виконувати свої функції. Тому правила доступу мають бути побудовані так, щоб дозволяти необхідну службову взаємодію і водночас блокувати зайві або небезпечні з’єднання. Це забезпечує баланс між безпекою та працездатністю ІКС.

З погляду GDPR такий підхід дозволяє реалізувати принцип мінімізації доступу. Кожен підрозділ отримує лише ті можливості, які потрібні для

виконання його функцій. Конфіденційність забезпечується за рахунок того, що персональні дані розміщуються в серверній зоні, а доступ до них контролюється. Захист даних за замовчуванням проявляється в тому, що студентський сегмент і непотрібні взаємодії між підрозділами спочатку обмежуються, а не залишаються відкритими.

Сегментація також зменшує ризики у випадку помилки користувача або компрометації окремого робочого місця. Якщо один пристрій у студентському або робочому сегменті буде використаний неправильно, сегментація ускладнює доступ до інших частин мережі. Це особливо важливо для серверної зони, оскільки саме там розміщуються ресурси з персональними даними студентів.

У проєктованій ІКС важливо передбачити логічний порядок взаємодії між сегментами. Робочі сегменти підрозділів повинні звертатися до серверної зони лише в межах своїх службових потреб. Взаємодія між робочими сегментами має бути обмеженою, оскільки більшість процесів обробки персональних даних повинна проходити через централізовані ресурси, а не через прямий обмін між робочими станціями різних підрозділів.

Загальна логіка розмежування доступу в ІКС може бути сформульована так: серверна зона є центральним захищеним ресурсом; деканат, міжнародний відділ і фінансовий відділ отримують доступ лише до потрібних їм ресурсів; адміністратор має доступ до технічної частини системи; студентський сегмент ізольований від внутрішніх ресурсів. Саме така модель відповідає практичному завданню роботи і дозволяє пов’язати мережеву архітектуру з вимогами GDPR.

Важливо, що проєктування сегментації мережі не є окремою технічною дією, відірваною від теми захисту персональних даних. Навпаки, саме через сегментацію та правила доступу вимоги GDPR набувають практичної реалізації в ІКС. Якщо GDPR визначає необхідність обмежити обробку персональних даних, то сегментація мережі показує, як це може бути виконано на рівні інфраструктури університету.

У результаті проєктування сегментації має бути сформована логічна

структура мережі, у якій кожен сегмент має власне призначення і власні обмеження доступу. Така структура буде використана під час подальшої практичної реалізації ІКС, де необхідно буде визначити адресацію, створити мережеві сегменти та налаштувати правила взаємодії між ними. Це дозволить перейти від концептуальної моделі до практичної побудови захищеної системи.

Таким чином, сегментація мережі та правила розмежування доступу є ключовими елементами захищеної ІКС університету. Вони дозволяють відокремити серверну зону, обмежити доступ студентського сегмента, розподілити права між підрозділами та забезпечити більш безпечну обробку персональних даних. Саме ці рішення створюють технічну основу для реалізації принципів GDPR у межах інформаційно-комунікаційної системи університетського підрозділу.

## 2.4 Висновки

У другому розділі було виконано проєктування захищеної інформаційно-комунікаційної системи університетського підрозділу для обробки особової конфіденційної інформації студентів. На основі аналізу наявної ІКС визначено, що вона потребує вдосконалення через ризик надмірного доступу між підрозділами, недостатнє відокремлення серверної зони та потребу в ізоляції студентського сегмента від внутрішніх ресурсів університету.

Визначено основні складові проєктованої ІКС: серверну зону, сегмент деканату, сегмент міжнародного відділу, фінансовий сегмент, адміністративний сегмент і студентський сегмент. Кожен із цих елементів має власне призначення і різний рівень доступу до інформаційних ресурсів. Такий поділ дозволяє уникнути ситуації, коли всі користувачі внутрішньої мережі мають однаковий доступ до персональних даних студентів.

Серверну зону було визначено як центральний захищений елемент ІКС. У

ній передбачається розміщення ресурсів, на яких зберігається або обробляється особова конфіденційна інформація студентів. Відокремлення серверної зони від робочих сегментів і студентської мережі дозволяє зменшити ризик несанкціонованого доступу до персональних даних і створює основу для подальшого контролю взаємодії між частинами системи.

Під час проєктування мережевої архітектури визначено логіку взаємодії між основними частинами ІКС. Робочі сегменти деканату, міжнародного та фінансового відділів повинні мати доступ до серверної зони лише в межах службової необхідності. Адміністративний сегмент використовується для технічного обслуговування системи, а студентський сегмент має бути відокремлений від внутрішніх ресурсів підрозділу.

Важливим результатом розділу стало обґрунтування сегментації мережі та правил розмежування доступу. Поділ мережі на окремі логічні сегменти дозволяє обмежити надмірну взаємодію між підрозділами, зменшити кількість користувачів, які можуть звертатися до ресурсів із персональними даними, і реалізувати доступ відповідно до функцій користувачів. При цьому показано, що сама сегментація має доповнюватися правилами доступу між сегментами.

Окремо було обґрунтовано необхідність ізоляції студентського сегмента. Студенти можуть користуватися дозволеними навчальними або інформаційними ресурсами, однак не повинні мати прямого доступу до серверної зони, робочих місць підрозділів та адміністративної частини ІКС.

Таким чином, у другому розділі сформовано проєктні рішення для усунення недоліків наявної ІКС. Надмірний доступ між підрозділами обмежується через сегментацію мережі та правила доступу, студентський сегмент ізолюється від внутрішніх ресурсів, а персональні дані розміщуються в окремій серверній зоні. Запропонована структура створює основу для практичної реалізації захищеної ІКС у третьому розділі, зокрема для побудови мережевої моделі, визначення IP-адресації, створення логічних сегментів і налаштування правил доступу.

# 3 РЕАЛІЗАЦІЯ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ВІДПОВІДНО ДО ВИМОГ GDPR

## 3.1 Розроблення мережевої моделі та структури захищеної інформаційно-комунікаційної системи університету

Після виконання концептуального проєктування та визначення мережевої архітектури необхідно перейти до практичної побудови захищеної інформаційно-комунікаційної системи університету. У межах даної роботи практична частина спрямована на створення мережевої моделі ІКС, у якій персональні дані студентів обробляються в окремій серверній зоні, а доступ до них розмежовується між підрозділами відповідно до їхніх функцій. Такий підхід дозволяє показати, як вимоги законодавства України та принципи GDPR щодо захисту персональних даних можуть бути враховані не лише на теоретичному рівні, але й під час побудови конкретної мережевої інфраструктури [2, 18].

Основою практичної реалізації є модель університетського підрозділу, у якому працюють деканат, міжнародний відділ, фінансовий відділ, адміністратор системи та студентський сегмент. Кожен із цих елементів виконує окрему роль у процесі обробки інформації. Деканат працює з навчальними даними студентів, міжнародний відділ з документами іноземних студентів, фінансовий відділ з інформацією щодо оплати, адміністратор забезпечує технічну працездатність системи, а студентський сегмент використовується лише для доступу до дозволених навчальних або загальних ресурсів.

Практична модель ІКС повинна відображати не просто набір підключених пристроїв, а логіку захисту персональних даних. Тому під час її розроблення основну увагу приділено серверній зоні, розподілу робочих місць за підрозділами, створенню окремих мережевих сегментів та обмеженню доступу між ними. У такій моделі персональні дані не повинні зберігатися на робочих комп’ютерах працівників або бути доступними для всіх користувачів мережі. Вони мають розміщуватися в окремій зоні ІКС, доступ до якої контролюється.

Для побудови мережевої моделі передбачається використання типових елементів локальної мережі: маршрутизатора, комутатора, серверів, робочих станцій працівників, точки доступу або окремого пристрою для студентського сегмента. Маршрутизатор використовується для організації взаємодії між мережевими сегментами, комутатор забезпечує підключення пристроїв, сервери використовуються для розміщення інформаційних ресурсів, а робочі станції представляють користувачів різних підрозділів університету.

У практичній частині роботи модель захищеної ІКС будується в середовищі моделювання мережевої інфраструктури. Це дає можливість наочно відобразити структуру університетського підрозділу, розміщення пристроїв, логічний поділ мережі, IP-адресацію та правила доступу між сегментами. Використання такого підходу є доцільним на етапі практичної реалізації, оскільки дозволяє перевірити працездатність запропонованої архітектури без розгортання фізичної мережі.

Для наочного подання практичної реалізації захищеної ІКС було побудовано мережеву модель університетського підрозділу (рисунок 3.1).

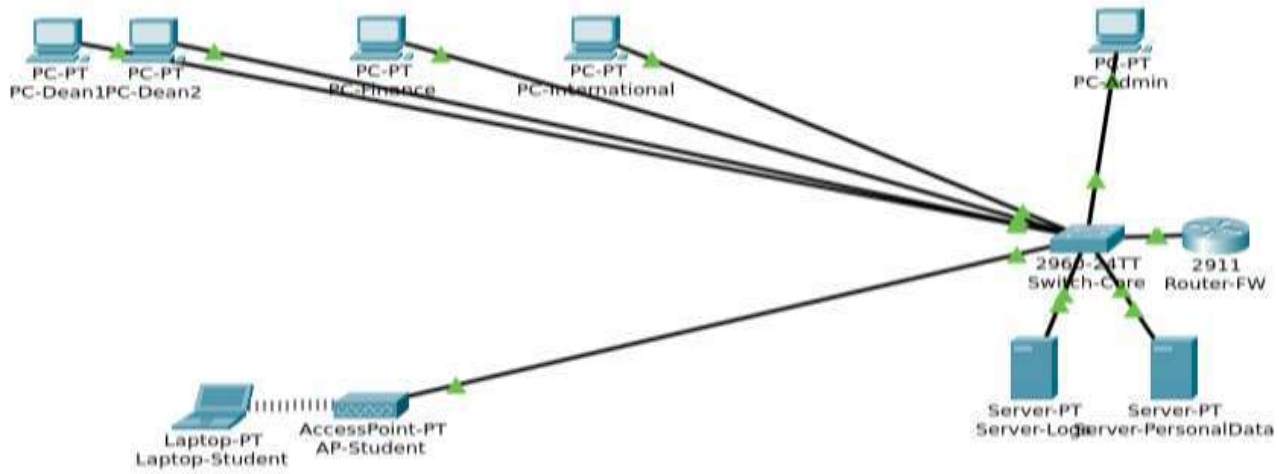



Рисунок 3.1 – Захищена мережева модель ІКС університету

У моделі відображено робочі місця деканату, міжнародного та фінансового відділів, адміністративний сегмент, серверну зону, студентський сегмент, центральний комутатор і маршрутизатор. Така структура дозволяє показати, як

проєктні рішення другого розділу реалізуються у вигляді конкретної мережевої інфраструктури.

Розміщення пристроїв у практичній моделі відповідає логіці фізичного поділу університетського підрозділу на окремі зони. Робочі станції працівників розміщуються відповідно до їхніх функцій, сервери та мережеве обладнання зосереджені в серверній зоні, а студентський сегмент винесений окремо. Це дозволяє поєднати фізичне розміщення компонентів ІКС із логічною сегментацією мережі та подальшим налаштуванням правил доступу.

У моделі передбачається використання однієї центральної мережевої інфраструктури, до якої підключаються всі сегменти ІКС. При цьому кожен сегмент має власне призначення. Окремо виділяється сегмент деканату, сегмент міжнародного відділу, фінансовий сегмент, адміністративний сегмент, серверна зона та студентський сегмент. Такий поділ відповідає попередньо визначеним вимогам до захищеної ІКС і дозволяє реалізувати принцип мінімізації доступу.

Серверна зона є центральною частиною практичної моделі. У ній розміщується сервер персональних даних, який умовно представляє інформаційний ресурс, де зберігаються або обробляються дані студентів. Також у цій зоні може бути передбачений додатковий сервер для службових або допоміжних функцій, наприклад для зберігання технічної інформації чи контролю подій у системі. Основне завдання серверної зони полягає в тому, щоб відокремити ресурси з персональними даними від звичайних робочих місць і студентської мережі.

Сегмент деканату включає робочі станції працівників, які виконують функції, пов’язані з організацією навчального процесу. У практичній моделі цей сегмент повинен мати обмежений доступ до серверної зони, оскільки деканат працює з навчальними даними студентів. Водночас він не повинен мати необмеженого доступу до всіх інших сегментів мережі. Такий підхід дозволяє забезпечити роботу підрозділу без надання зайвих прав доступу.

Сегмент міжнародного відділу призначений для роботи з інформацією

іноземних студентів, зокрема громадян ЄС. До таких даних можуть належати документи, відомості про громадянство, попередню освіту, контактна інформація та інші дані, необхідні для адміністративного супроводу. У мережевій моделі цей сегмент також повинен мати доступ до необхідних ресурсів серверної зони, але не до фінансового чи студентського сегмента без потреби.

Фінансовий сегмент використовується для робочого місця або робочих місць працівників, які обробляють інформацію щодо оплати освітніх послуг. Йому може бути потрібний доступ до окремих даних студента, пов’язаних із договором, оплатою або фінансовим обліком. Водночас фінансовий відділ не повинен отримувати повний доступ до навчальних документів або всіх матеріалів міжнародного відділу. Це дозволяє відобразити в моделі принцип розмежування доступу між підрозділами.

Адміністративний сегмент призначений для адміністратора системи. У практичній моделі він використовується для технічного управління мережею, перевірки працездатності підключень, контролю серверної зони та налаштування правил доступу. Цей сегмент має особливе значення, оскільки адміністратор забезпечує роботу ІКС. Водночас його доступ також повинен бути обґрунтованим і пов’язаним саме з технічним обслуговуванням системи.

Студентський сегмент є окремою частиною мережі, яка призначена для підключення студентів до дозволених ресурсів. У практичній моделі він може бути представлений окремим комп’ютером, ноутбуком або бездротовою точкою доступу. Головна вимога до цього сегмента полягає в тому, що він не повинен мати прямого доступу до серверної зони та робочих сегментів підрозділів. Це дозволяє показати реалізацію принципу захисту даних за замовчуванням.

Під час побудови мережевої моделі важливо правильно визначити склад пристроїв. Для відображення роботи захищеної ІКС достатньо передбачити один маршрутизатор, один керований комутатор, сервер персональних даних, за потреби додатковий сервер, робочі станції для деканату, міжнародного відділу, фінансового відділу, адміністратора системи та пристрій студентського

сегмента. Така кількість пристроїв дозволяє показати основну логіку системи без зайвого ускладнення моделі.

Маршрутизатор у цій моделі виконує функцію зв’язку між окремими сегментами мережі. Саме через нього може здійснюватися маршрутизація трафіку між деканатом, міжнародним відділом, фінансовим сегментом, адміністративним сегментом, серверною зоною та студентською мережею. Крім того, на рівні маршрутизатора можуть бути реалізовані правила доступу, які дозволяють або забороняють взаємодію між сегментами.

Комутатор використовується для фізичного підключення робочих станцій, серверів та інших мережевих пристроїв. У межах практичної моделі він також потрібний для розподілу портів за окремими логічними сегментами. Наприклад, порти, до яких підключені комп’ютери деканату, належать до одного сегмента, порти міжнародного відділу до іншого, порти серверної зони до окремого сегмента. Такий підхід дозволяє впорядкувати мережу та підготувати її до подальшого налаштування доступу.

Для побудови захищеної ІКС важливо, щоб кожен сегмент мав власну логічну адресацію. Окремий адресний простір дозволяє чітко відокремити підрозділи один від одного і спростити налаштування правил доступу. Наприклад, сегмент деканату, міжнародного відділу, фінансового відділу, серверної зони та студентської мережі можуть мати різні підмережі. Це дає змогу контролювати взаємодію між ними на рівні мережевої інфраструктури.

Розроблена структура ІКС повинна забезпечувати виконання кількох основних умов. По-перше, персональні дані студентів повинні бути зосереджені в серверній зоні. По-друге, доступ до цієї зони повинні мати лише ті сегменти, яким це потрібно для виконання службових функцій. По-третє, студентський сегмент повинен бути ізольований від внутрішніх ресурсів університету. По-четверте, взаємодія між підрозділами повинна бути обмежена службовою необхідністю.

У практичній моделі також потрібно врахувати фізичну логіку розміщення

пристроїв. Робочі місця деканату, міжнародного відділу та фінансового відділу умовно розміщуються в окремих кабінетах або робочих зонах. Сервери та основне мережеве обладнання розміщуються в серверній зоні. Студентський доступ організовується окремо від адміністративної частини мережі. Таке розміщення допомагає показати, що захист персональних даних забезпечується не тільки логічним, але й фізичним розмежуванням.

Особливість запропонованої моделі полягає в тому, що вона не надає всім користувачам однаковий доступ до ресурсів. Кожен підрозділ отримує власну частину мережі, а доступ до персональних даних обмежується відповідно до його функцій. Це дозволяє уникнути ситуації, коли будь-який користувач внутрішньої мережі може звернутися до сервера з персональними даними або до робочих станцій інших підрозділів.

З погляду вимог захисту персональних даних така структура дозволяє реалізувати принципи мінімізації, конфіденційності та захисту даних за замовчуванням. Мінімізація проявляється в обмеженні доступу до ресурсів за функціями підрозділів. Конфіденційність забезпечується через виділення серверної зони та заборону прямого доступу з непотрібних сегментів. Захист за замовчуванням полягає в тому, що студентський сегмент і непотрібні з’єднання між підрозділами не відкриваються без потреби.

Практична побудова мережевої моделі створює основу для наступного етапу роботи налаштування сегментації та правил доступу. Після визначення структури ІКС необхідно призначити адреси пристроям, створити логічні сегменти, налаштувати взаємодію між ними та перевірити, чи виконуються обмеження доступу. Саме ці дії дозволяють перейти від загального проєкту до працюючої моделі захищеної ІКС.

Отже, у межах підрозділу було визначено практичну структуру захищеної інформаційно-комунікаційної системи університету. Запропонована модель включає серверну зону, робочі сегменти деканату, міжнародного та фінансового відділів, адміністративний сегмент і студентську мережу. Така структура дає

змогу реалізувати вимоги захисту персональних даних на рівні мережевої інфраструктури та створює основу для подальшого налаштування сегментації, IP-адресації та правил розмежування доступу.

## 3.2 Налаштування сегментації, IP-адресації та правил доступу

Після розроблення мережевої моделі захищеної інформаційно-комунікаційної системи університету необхідно перейти до її практичного налаштування. На цьому етапі визначається логічна сегментація мережі, IP-адресація пристроїв, налаштування взаємодії між сегментами та правила доступу до серверної зони. Саме ці налаштування дозволяють перетворити загальну структуру ІКС на працюючу модель, у якій персональні дані студентів захищаються не лише організаційно, але й технічними засобами.

У межах даної роботи практичне налаштування захищеної ІКС виконується з урахуванням вимог законодавства України щодо захисту персональних даних та інформації в ІКС, а також принципів GDPR. Це означає, що технічна структура мережі повинна підтримувати мінімізацію доступу, конфіденційність, цілісність та захист даних за замовчуванням.

Основою налаштування є поділ мережі на окремі сегменти відповідно до функцій підрозділів університету. У моделі виділяються адміністративний сегмент, сегмент деканату, сегмент міжнародного відділу, фінансовий сегмент, серверна зона та студентський сегмент. Така структура відповідає раніше визначеній архітектурі ІКС і дозволяє обмежити доступ до персональних даних студентів залежно від службової необхідності.

Для практичної реалізації такого поділу доцільно використовувати VLAN. VLAN дозволяє розділити одну фізичну мережеву інфраструктуру на кілька окремих логічних мереж. Це означає, що пристрої різних підрозділів можуть бути підключені до одного комутатора, але при цьому належати до різних

сегментів і не мати вільного доступу один до одного. Для захищеної ІКС університету це є важливим, оскільки дозволяє відокремити серверну зону і студентську мережу від робочих сегментів підрозділів [27-29].

У проєктованій ІКС доцільно передбачити шість основних VLAN. Адміністративний сегмент використовується для робочого місця адміністратора системи. Сегмент деканату призначений для працівників, які працюють з навчальними даними студентів. Сегмент міжнародного відділу використовується для обробки даних іноземних студентів, зокрема громадян ЄС. Фінансовий сегмент призначений для роботи з інформацією щодо оплати освітніх послуг. Серверна зона використовується для розміщення ресурсів із персональними даними. Студентський сегмент призначений для підключення студентів до дозволених ресурсів.

Для зручності налаштування кожному сегменту надається окремий номер VLAN і окрема IP-підмережа. Такий підхід дозволяє чітко відокремити пристрої різних підрозділів і спростити подальше налаштування правил доступу. Крім того, окрема адресація допомагає швидко визначати, до якого сегмента належить певний пристрій, і контролювати маршрутизацію між частинами ІКС.

У практичній моделі можна використати таку структуру VLAN: VLAN 10 - адміністративний сегмент, VLAN 20 - сегмент деканату, VLAN 30 - сегмент міжнародного відділу, VLAN 40 - фінансовий сегмент, VLAN 50 - серверна зона, VLAN 60 - студентський сегмент. Такий поділ є достатнім для демонстрації роботи захищеної ІКС університетського підрозділу і водночас не ускладнює модель зайвими елементами.

Для кожного VLAN також визначається власна IP-підмережа. Адміністративний сегмент може використовувати мережу 192.168.10.0/24, сегмент деканату - 192.168.20.0/24, сегмент міжнародного відділу - 192.168.30.0/24, фінансовий сегмент - 192.168.40.0/24, серверна зона - 192.168.50.0/24, студентський сегмент - 192.168.60.0/24. Така адресація є зрозумілою і дозволяє логічно пов’язати номер VLAN з адресним простором

відповідного сегмента.

Для кожного сегмента також визначається шлюз за замовчуванням. Наприклад, для VLAN 10 шлюзом може бути адреса 192.168.10.1, для VLAN 20 - 192.168.20.1, для VLAN 30 - 192.168.30.1, для VLAN 40 - 192.168.40.1, для VLAN 50 - 192.168.50.1, для VLAN 60 - 192.168.60.1. Наявність окремих шлюзів дозволяє організувати маршрутизацію між сегментами та одночасно контролювати, які з'єднання між ними дозволені.

У серверній зоні доцільно розмістити сервер персональних даних і, за потреби, додатковий сервер службових або технічних функцій. Сервер персональних даних може мати адресу 192.168.50.10, а додатковий сервер - 192.168.50.20. Саме серверна зона є основним ресурсом, до якого повинні застосовуватися найсуворіші правила доступу, оскільки в ній зберігається або обробляється особова конфіденційна інформація студентів.

Робоче місце адміністратора системи може бути розміщене в адміністративному сегменті з адресою 192.168.10.10. Цей пристрій використовується для технічного обслуговування ІКС, перевірки підключень, налаштування обладнання та контролю роботи серверної зони. Водночас доступ адміністратора також повинен бути обґрунтованим і не повинен означати необмежене використання персональних даних без службової необхідності.

У сегменті деканату можна розмістити дві робочі станції, наприклад PC-Dean-1 з адресою 192.168.20.10 та PC-Dean-2 з адресою 192.168.20.11. Ці пристрої умовно представляють працівників, які працюють з навчальними даними студентів. Для них має бути дозволений доступ до необхідних ресурсів серверної зони, але не до студентського сегмента або технічних ресурсів адміністратора без потреби.

У сегменті міжнародного відділу можна розмістити робочу станцію PC-International з адресою 192.168.30.10. Цей пристрій представляє працівника, який працює з документами іноземних студентів, контактними даними, інформацією про громадянство та іншими відомостями, необхідними для супроводу громадян

ЄС. Доступ цього сегмента до серверної зони повинен бути обмежений лише тими ресурсами, які потрібні для виконання функцій міжнародного відділу.

У фінансовому сегменті можна розмістити робочу станцію PC-Finance з адресою 192.168.40.10. Вона використовується для роботи з даними щодо оплати освітніх послуг, договорів та фінансових зобов'язань студентів. При цьому фінансовий сегмент не повинен мати необмеженого доступу до навчальних даних, документів міжнародного відділу або студентської мережі.

Студентський сегмент може бути представлений окремим пристроєм Laptop-Student з адресою 192.168.60.10 або підключенням через точку доступу. Цей сегмент використовується для демонстрації доступу студентів до дозволених ресурсів. Основне правило для нього полягає в тому, що студентський сегмент не повинен мати доступу до серверної зони, адміністративного сегмента та робочих сегментів підрозділів. Це є одним із ключових обмежень у проєктованій ІКС.

Для наочності логіку IP-адресації подано у вигляді таблиці 3.1.

Таблиця 3.1 – IP-адресація сегментів захищеної ІКС університету

| Сегмент мережі | VLAN | Підмережа | Шлюз |
|---|---|---|---|
| Адміністративний сегмент | 10 | 192.168.10.0/24 | 192.168.10.1 |
| Сегмент деканату | 20 | 192.168.20.0/24 | 192.168.20.1 |
| Сегмент міжнародного відділу | 30 | 192.168.30.0/24 | 192.168.30.1 |
| Фінансовий сегмент | 40 | 192.168.40.0/24 | 192.168.40.1 |
| Серверна зона | 50 | 192.168.50.0/24 | 192.168.50.1 |
| Студентський сегмент | 60 | 192.168.60.0/24 | 192.168.60.1 |

Наведена адресація дозволяє впорядкувати структуру мережі та забезпечити зрозумілий поділ між підрозділами. Кожен сегмент має власний діапазон адрес, що спрощує налаштування маршрутизації, перевірку підключень

і створення правил доступу. Крім того, така структура дозволяє швидко визначити, з якого саме сегмента надходить мережевий трафік.

Окремо доцільно визначити адреси основних пристроїв у моделі (таблиця 3.2).

Таблиця 3.2 – IP-адресація основних пристроїв захищеної ІКС університету

| Пристрій | Сегмент | IP-адреса | Призначення |
|---|---|---|---|
| PC-Admin | Адміністративний сегмент | 192.168.10.10 | Технічне адміністрування ІКС |
| PC-Dean-1 | Сегмент деканату | 192.168.20.10 | Робоче місце деканату |
| PC-Dean-2 | Сегмент деканату | 192.168.20.11 | Робоче місце деканату |
| PC-International | Міжнародний відділ | 192.168.30.10 | Робота з даними іноземних студентів |
| PC-Finance | Фінансовий сегмент | 192.168.40.10 | Робота з фінансовою інформацією |
| Server-PersonalData | Серверна зона | 192.168.50.10 | Сервер персональних даних студентів |
| Server-Logs | Серверна зона | 192.168.50.20 | Допоміжний службовий сервер |
| Laptop-Student | Студентський сегмент | 192.168.60.10 | Пристрій студентської мережі |

Наведена структура адресації показує, що кожен пристрій належить до визначеного сегмента ІКС. Це дозволяє чітко розмежувати робочі місця

підрозділів, серверну зону та студентську мережу, а також підготувати основу для подальшого налаштування правил доступу між ними.

Після визначення VLAN та IP-адресації наступним етапом є формування правил доступу між сегментами. Основна логіка полягає в тому, що службові сегменти деканату, міжнародного та фінансового відділів можуть звертатися до серверної зони, але не повинні мати вільної прямої взаємодії між собою. Студентський сегмент повинен бути ізольований від серверної зони, адміністративного сегмента та робочих місць підрозділів.

Під час налаштування ACL основну увагу потрібно приділити забороні доступу студентського сегмента до внутрішніх ресурсів. Якщо студентський сегмент матиме можливість звертатися до серверної зони або робочих станцій підрозділів, це створить ризик несанкціонованого доступу до персональних даних. Тому в моделі студентська мережа повинна бути відокремлена від внутрішньої адміністративної частини ІКС.

Також потрібно обмежити доступ між робочими сегментами підрозділів. Деканат, міжнародний відділ і фінансовий відділ можуть працювати з різними категоріями персональних даних, але це не означає, що вони повинні мати прямий доступ до робочих станцій один одного. Більш безпечним є підхід, за якого основна робота з даними відбувається через серверну зону, а прямий обмін між робочими сегментами обмежується.

Для практичного розмежування доступу між VLAN у моделі ІКС були налаштовані списки контролю доступу ACL на маршрутизаторі Router-FW (рисунки 3.2-3.5). ACL застосовуються до відповідних підінтерфейсів маршрутизатора, через які проходить трафік окремих сегментів. Окремі правила було створено для сегмента деканату, фінансового сегмента, сегмента міжнародного відділу та студентського сегмента. Адміністративний сегмент не обмежувався окремою ACL, оскільки він використовується для технічного обслуговування ІКС.

```
Router(config)#ip access-list extended DEAN_ACCESS
Router(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 192.168.50.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.20.0 0.0.0.255 192.168.60.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 any
Router(config-ext-nacl)#exit
```

Рисунок 3.2 – Налаштування ACL для сегмента деканату

```
Router(config)#ip access-list extended FINANCE_ACCESS
Router(config-ext-nacl)#permit ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.40.0 0.0.0.255 192.168.60.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.40.0 0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#interface g0/0.40
Router(config-subif)#ip access-group FINANCE_ACCESS in
Router(config-subif)#exit
```

Рисунок 3.3 – Налаштування ACL для фінансового сегменту

```
Router(config)#ip access-list extended INTERNATIONAL_ACCESS
Router(config-ext-nacl)# permit ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.30.0 0.0.0.255 192.168.60.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.30.0 0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#interface g0/0.30
Router(config-subif)#ip access-group INTE
Router(config-subif)#ip access-group INTERNATIONAL_ACCESS in
Router(config-subif)#exit
```

Рисунок 3.4 – Налаштування ACL для сегмента міжнародного відділу

```
Router(config)#ip access-list extended STUDENTS_BLOCK
Router(config-ext-nacl)#deny ip 192.168.60.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.60.0 0.0.0.255 192.168.20.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.60.0 0.0.0.255 192.168.30.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.60.0 0.0.0.255 192.168.40.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.60.0 0.0.0.255 192.168.50.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.60.0 0.0.0.255 any
Router(config-ext-nacl)#
Router(config-ext-nacl)#exit
Router(config)#interface g0/0.60
Router(config-subif)#ip access-group STUDENTS_BLOCK in
Router(config-subif)#exit
```

Рисунок 3.5 – Налаштування ACL для ізоляції студентського сегмента

Наведені налаштування показують, що доступ між сегментами ІКС не є відкритим для всіх користувачів. Для деканату, міжнародного та фінансового відділів дозволено доступ до серверної зони, але обмежено пряму взаємодію з

іншими службовими сегментами. Студентський сегмент ізольовано від серверної зони, адміністративного сегмента та робочих сегментів підрозділів. Це дозволяє реалізувати технічне розмежування доступу відповідно до функцій користувачів і зменшити ризик несанкціонованого доступу до персональних даних студентів.

Після налаштування сегментації та правил доступу необхідно перевірити, чи відповідає модель поставленим вимогам. Для цього можна виконати перевірку доступності між пристроями різних сегментів. Наприклад, робочі станції деканату, міжнародного відділу і фінансового сегмента повинні мати доступ до дозволених ресурсів серверної зони. Водночас студентський пристрій не повинен мати доступу до сервера персональних даних або робочих станцій підрозділів.

Якщо перевірка показує, що студентський сегмент має доступ до серверної зони, це означає, що правила доступу налаштовані неправильно і потребують виправлення. Якщо ж робочі сегменти підрозділів не можуть отримати доступ до необхідних ресурсів, це також є помилкою, оскільки система повинна бути не тільки захищеною, але й працездатною. Тому налаштування доступу повинно забезпечувати баланс між безпекою та нормальною роботою підрозділу.

З технічної точки зору налаштування сегментації, адресації та правил доступу є основою практичної реалізації захищеної ІКС. Саме на цьому етапі визначається, які пристрої належать до певних сегментів, які підмережі використовуються, які шлюзи забезпечують маршрутизацію і які обмеження застосовуються до мережевого трафіку. Без цих налаштувань мережа залишалася б звичайною локальною мережею без достатнього рівня контролю.

З погляду GDPR такі технічні налаштування мають безпосереднє значення для захисту персональних даних. Сегментація дозволяє обмежити доступ до даних відповідно до функцій користувачів. ACL дозволяють заборонити непотрібні або небезпечні з’єднання. Окрема серверна зона дозволяє централізувати обробку персональних даних. Ізоляція студентської мережі дозволяє зменшити ризик доступу до внутрішніх ресурсів з боку користувачів, які не виконують службових функцій.

Отже, у межах підрозділу було визначено порядок налаштування сегментації, IP-адресації та правил доступу в захищеній інформаційно-комунікаційній системі університету. Запропонована структура VLAN, окрема адресація для кожного сегмента, виділення серверної зони та ізоляція студентської мережі створюють технічну основу для безпечної обробки персональних даних студентів. Такі рішення відповідають вимогам законодавства України щодо захисту інформації в ІКС і підтримують принципи GDPR щодо мінімізації доступу, конфіденційності та захисту даних за замовчуванням.

## 3.3 Оцінка працездатності системи та відповідності вимогам

Перевірка працездатності захищеної інформаційно-комунікаційної системи та оцінка її відповідності вимогам захисту персональних даних є завершальним етапом практичної частини роботи. На цьому етапі потрібно показати, що розроблена мережева модель не лише має правильну структуру, але й реально забезпечує обмеження доступу до персональних даних студентів. Тому оцінка виконується не як повний юридичний аудит, а як перевірка того, чи реалізовані в побудованій ІКС основні технічні вимоги, пов’язані з конфіденційністю, мінімізацією доступу, ізоляцією сегментів та захистом даних за замовчуванням.

У межах даної роботи захищена ІКС університету розглядається як практична мережева модель, у якій виділено серверну зону, робочі сегменти підрозділів, адміністративний сегмент та студентську мережу. Персональні дані студентів умовно розміщуються в серверній зоні, а доступ до цієї зони надається лише тим підрозділам, яким він потрібний для виконання службових функцій. Такий підхід дозволяє пов’язати вимоги законодавства України щодо захисту інформації в ІКС та принципи GDPR із конкретними мережевими рішеннями, які були реалізовані в практичній частині роботи.

Фінальна мережева модель захищеної ІКС університетського підрозділу після налаштування VLAN, IP-адресації та правил ACL подана на рисунку 3.6. У моделі відображено робочі сегменти деканату, міжнародного та фінансового відділів, адміністративний сегмент, серверну зону, студентський сегмент, центральний комутатор, маршрутизатор Router-FW та умовне підключення до зовнішніх ресурсів через Internet.

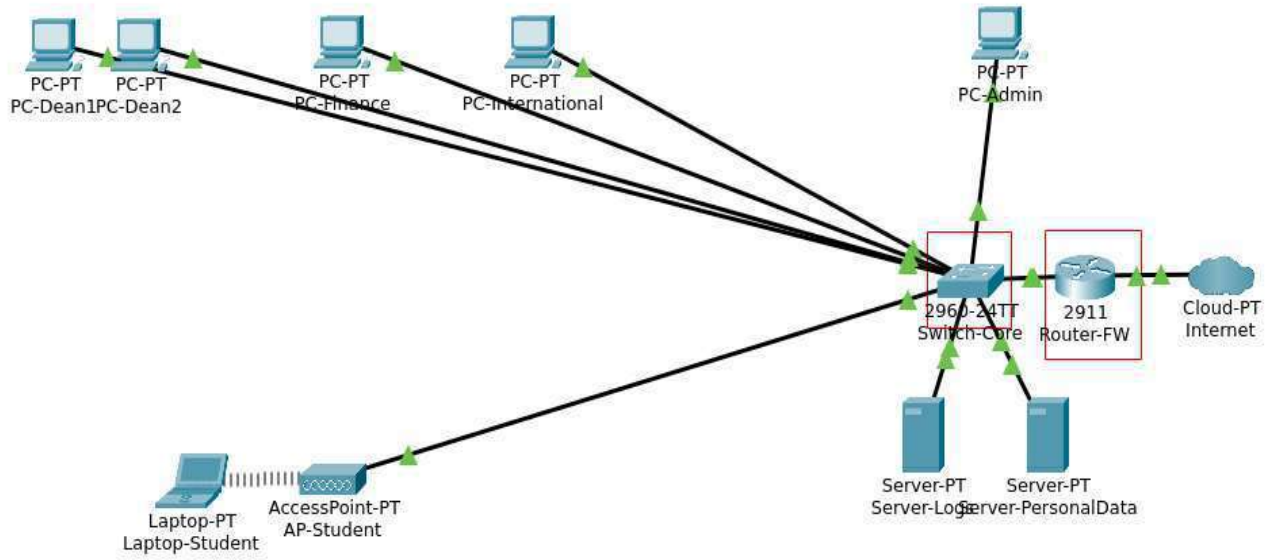



Рисунок 3.6 – Фінальна захищена мережева модель ІКС університету

Під час перевірки насамперед було оцінено працездатність внутрішньої мережевої структури. Після налаштування VLAN, IP-адресації, шлюзів і правил ACL було перевірено, чи відповідає фактична взаємодія між сегментами проєктній логіці доступу. Робочі станції деканату, фінансового та міжнародного відділів повинні мати доступ до дозволених ресурсів серверної зони, оскільки ці підрозділи виконують службові функції з обробки персональних даних студентів. Водночас студентський сегмент повинен бути ізольований від серверної зони та внутрішніх робочих сегментів університету.

Як видно з рисунка 3.6, усі внутрішні сегменти ІКС підключені до центрального комутатора, а взаємодія між VLAN здійснюється через маршрутизатор Router-FW. Комутатор використовується для підключення

пристроїв і розподілу портів між VLAN, а маршрутизатор виконує міжVLAN-маршрутизацію та фільтрацію трафіку за допомогою ACL. Сервери розміщені в окремій серверній зоні, студентський сегмент винесений окремо та відокремлений від внутрішніх ресурсів університету.

Практична перевірка моделі передбачає послідовне тестування підключень між окремими сегментами мережі. Для цього в середовищі моделювання мережевої інфраструктури використовується перевірка доступності пристроїв за допомогою команд ping або простих мережевих запитів до серверів. Основна мета такої перевірки полягає в тому, щоб переконатися, що дозволені з'єднання працюють, а заборонені з'єднання блокуються відповідно до розроблених правил доступу.

У межах перевірки основну увагу було зосереджено не на загальній доступності всіх пристроїв, а саме на відповідності мережевої взаємодії налаштованим правилам доступу. Тому результати перевірки повинні показати дві умови: по-перше, уповноважені службові сегменти можуть звертатися до дозволених ресурсів серверної зони; по-друге, студентський сегмент і прямі зайві з'єднання між робочими сегментами обмежуються правилами ACL.

Для підтвердження працездатності налаштованих правил доступу було виконано перевірку мережевої взаємодії з основних сегментів ІКС. Окремо перевірено доступ із сегмента деканату, фінансового сегмента, сегмента міжнародного відділу та студентського сегмента. Така перевірка дозволяє показати, що службові підрозділи мають доступ до дозволених ресурсів, а студентська мережа ізольована від внутрішніх ресурсів університету.

На рисунку 3.7 показано перевірку доступу з робочих сегментів деканату та міжнародного відділу. Результати перевірки підтверджують, що ці підрозділи можуть звертатися до дозволених ресурсів серверної зони, оскільки їхня діяльність пов'язана з обробкою навчальних даних студентів та даних іноземних студентів. Водночас доступ таких сегментів до інших робочих сегментів має бути обмежений відповідно до налаштованих ACL, щоб уникнути надмірного доступу до персональних даних.

```
C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.40.10

Pinging 192.168.40.10 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.40.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.60.10

Pinging 192.168.60.10 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.60.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.50.10

Pinging 192.168.50.10 with 32 bytes of data:

Reply from 192.168.50.10: bytes=32 time<1ms TTL=127
Reply from 192.168.50.10: bytes=32 time=8ms TTL=127
Reply from 192.168.50.10: bytes=32 time<1ms TTL=127
```

```
C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.40.10

Pinging 192.168.40.10 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.40.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.50.10

Pinging 192.168.50.10 with 32 bytes of data:

Reply from 192.168.50.10: bytes=32 time<1ms TTL=127
Reply from 192.168.50.10: bytes=32 time<1ms TTL=127
Reply from 192.168.50.10: bytes=32 time=3ms TTL=127
Reply from 192.168.50.10: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.50.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>ping 192.168.60.10

Pinging 192.168.60.10 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
```

Рисунок 3.7 – Перевірка доступу з сегментів деканату та міжнародного відділу

На рисунку 3.8 показано перевірку доступу зі студентського сегмента та фінансового відділу.

Результати перевірки підтверджують різну логіку доступу для цих груп

користувачів. Фінансовий сегмент має доступ до дозволених ресурсів серверної зони, оскільки він використовується для роботи з інформацією щодо оплати освітніх послуг. Студентський сегмент, навпаки, ізольований від серверної зони та внутрішніх робочих сегментів університету, оскільки студенти не виконують службових функцій з обробки персональних даних інших осіб.


Рисунок 3.8 – Перевірка доступу з сегментів студентів та фінансового відділу

Якщо пристрій не може звернутися до власного шлюзу, це означає, що є помилка в адресації, налаштуванні VLAN або підключенні порту комутатора. Тому на початковому етапі важливо перевірити саме базову працездатність кожного сегмента окремо. Така перевірка показує, що логічний поділ мережі виконано правильно і кожен сегмент ІКС функціонує як окрема частина загальної мережевої інфраструктури.

Другим напрямом є перевірка доступу робочих сегментів до серверної зони. У проєктованій ІКС серверна зона є центральним елементом, у якому розміщуються ресурси з персональними даними студентів. Тому потрібно перевірити, чи можуть дозволені підрозділи звертатися до сервера персональних даних. До таких підрозділів належать деканат, міжнародний відділ і фінансовий відділ, оскільки вони виконують службові функції, пов’язані з обробкою різних категорій даних студентів.

Сегмент деканату повинен мати доступ до серверної зони в межах роботи з навчальними даними студентів. Це відповідає функціям деканату, який організовує освітній процес, працює з академічними групами, заявами, довідками та іншими навчальними відомостями. Якщо робочі станції деканату можуть звертатися до дозволеного серверного ресурсу, це означає, що система забезпечує працездатність цього підрозділу без надання йому повного доступу до всіх частин ІКС.

Сегмент міжнародного відділу також повинен мати доступ до визначених ресурсів серверної зони, оскільки цей підрозділ працює з даними іноземних студентів, зокрема громадян Європейського Союзу. У практичній моделі це означає, що робоча станція міжнародного відділу повинна мати можливість звертатися до сервера персональних даних або до окремого ресурсу, призначеного для супроводу іноземних студентів. При цьому доступ до інших робочих сегментів без потреби має бути обмежений.

Фінансовий сегмент повинен мати доступ лише до тих ресурсів, які пов’язані з оплатою освітніх послуг або фінансовим супроводом студента. У

практичній моделі це можна перевірити через доступ робочої станції фінансового відділу до серверної зони. Водночас фінансовий сегмент не повинен отримувати вільний доступ до робочих станцій деканату, міжнародного відділу або студентського сегмента. Такий підхід дозволяє обмежити обробку персональних даних тільки необхідними функціями.

Третім напрямом перевірки є ізоляція студентського сегмента. Це один із найбільш важливих елементів захищеної ІКС, оскільки студенти не повинні мати прямого доступу до серверної зони та внутрішніх робочих сегментів університетського підрозділу. У моделі потрібно перевірити, що пристрій студентського сегмента не може звернутися до сервера персональних даних, робочих станцій деканату, міжнародного відділу, фінансового відділу та адміністративного сегмента.

Якщо студентський пристрій не має доступу до внутрішніх ресурсів, це підтверджує правильність налаштування правил розмежування доступу. Така ізоляція відповідає принципу захисту даних за замовчуванням, оскільки студентський сегмент від початку не отримує зайвих прав. Студенти можуть користуватися лише дозволеними навчальними або загальними ресурсами, але не можуть взаємодіяти з ресурсами, у яких обробляються персональні дані інших осіб.

Четвертим напрямом є перевірка обмеження доступу між робочими сегментами підрозділів. Деканат, міжнародний відділ і фінансовий відділ працюють з різними категоріями персональних даних, однак це не означає, що вони повинні мати прямий доступ до робочих станцій один одного. Більш безпечною є модель, за якої основна робота з даними відбувається через серверну зону, а прямі з’єднання між робочими сегментами обмежуються.

Перевірка такого обмеження дозволяє показати, що мережа не є відкритою для всіх внутрішніх користувачів. Якщо комп’ютер деканату не має прямого доступу до комп’ютера фінансового відділу або міжнародного відділу без службової необхідності, це зменшує ризик поширення помилок, несанкціонованого доступу або випадкового розкриття інформації. Така логіка

відповідає принципу мінімізації доступу.

П’ятим напрямом перевірки є доступ адміністративного сегмента до технічних ресурсів системи. Адміністратор повинен мати можливість виконувати технічне обслуговування ІКС, перевіряти працездатність мережі, контролювати роботу серверної зони та налаштовувати мережеве обладнання. Водночас адміністративний сегмент не повинен розглядатися як неконтрольована зона повного доступу до всієї інформації. Його функція полягає насамперед у підтримці працездатності системи.

У практичній моделі це означає, що адміністративний сегмент може мати розширений технічний доступ, але такий доступ повинен бути обґрунтований. Наприклад, адміністратор може перевіряти доступність серверної зони або налаштовувати правила маршрутизації, але модель не повинна передбачати, що всі персональні дані відкриті для довільного перегляду без потреби. Такий підхід зменшує ризики, пов’язані з надмірними правами адміністратора.

Оцінка відповідності вимогам GDPR у межах цієї роботи виконується через зіставлення реалізованих технічних рішень з основними принципами обробки персональних даних. Першим таким принципом є мінімізація доступу. У розробленій ІКС цей принцип реалізується через поділ мережі на окремі сегменти та надання доступу до серверної зони лише тим підрозділам, які виконують відповідні функції. Це зменшує кількість користувачів, які можуть взаємодіяти з персональними даними студентів.

Принцип конфіденційності реалізується через виділення серверної зони, ізоляцію студентського сегмента та обмеження доступу між підрозділами. Персональні дані не розміщуються у відкритій загальній мережі, а зберігаються в окремому сегменті, доступ до якого контролюється. Завдяки цьому зменшується ризик несанкціонованого доступу, випадкового перегляду або розкриття інформації користувачами, які не мають службової потреби працювати з такими даними.

Принцип цілісності підтримується тим, що змінювати або використовувати персональні дані можуть лише визначені сегменти та користувачі. Якщо доступ

до серверної зони відкритий тільки для уповноважених підрозділів, знижується ймовірність неправомірної зміни даних або впливу з боку сторонніх користувачів. У практичній моделі це забезпечується поєднанням VLAN, окремої IP-адресації та правил контролю доступу.

Принцип захисту даних за замовчуванням проявляється в тому, що небажані або непотрібні з'єднання між сегментами спочатку забороняються. Особливо це стосується студентської мережі, яка не повинна мати доступу до внутрішніх ресурсів університету. Такий підхід є важливим, тому що система не очікує від користувача правильних дій для забезпечення безпеки, а сама обмежує потенційно небезпечну взаємодію.

Принцип підзвітності у межах цієї роботи розглядається через можливість пояснити, чому кожен сегмент має саме такий рівень доступу. Наприклад, деканат отримує доступ до навчальних ресурсів, міжнародний відділ — до даних іноземних студентів, фінансовий відділ — до інформації, пов'язаної з оплатою, а студентський сегмент ізолюється від внутрішньої мережі. Така структура робить рішення щодо доступу зрозумілими та обґрунтованими.

Важливо зазначити, що розроблена модель не є повним впровадженням усіх юридичних і організаційних вимог GDPR. У межах цієї кваліфікаційної роботи основний акцент зроблено саме на технічному рівні реалізації захищеної ІКС. Тому такі питання, як повний юридичний аудит, офіційні політики, строки зберігання документів або порядок обробки запитів суб'єктів даних, не є головним результатом практичної частини. Вони можуть бути враховані в діяльності університету додатково, але основна увага роботи зосереджена на мережевій інфраструктурі.

Разом з тим технічна модель безпосередньо підтримує виконання основних вимог захисту персональних даних. Вона показує, що доступ до інформації можна обмежити не тільки на рівні правил для працівників, але й на рівні самої мережі. Якщо користувач фізично або логічно підключений до студентського сегмента, він не може звернутися до серверної зони. Якщо працівник належить

до певного підрозділу, його доступ визначається функцією цього підрозділу, а не фактом перебування у внутрішній мережі університету.

Під час оцінки працездатності також важливо перевірити, що обмеження доступу не порушують нормальну роботу підрозділів. Захищена ІКС не повинна повністю блокувати роботу деканату, міжнародного чи фінансового відділу. Якщо працівники не можуть звернутися до необхідних серверних ресурсів, система буде формально захищеною, але непридатною для практичного використання. Тому правильним результатом є такий стан, коли дозволені службові з'єднання працюють, а зайві або небезпечні з'єднання блокуються.

Результати перевірки можна описати через кілька основних умов. По-перше, усі пристрої повинні мати коректну IP-адресацію відповідно до свого сегмента. По-друге, кожен сегмент повинен мати доступ до власного шлюзу. По-третє, робочі сегменти підрозділів повинні мати доступ до дозволених ресурсів серверної зони. По-четверте, студентський сегмент не повинен мати доступу до серверної зони та внутрішніх робочих сегментів. По-п'яте, прямий доступ між підрозділами повинен бути обмежений.

Якщо всі ці умови виконуються, можна зробити висновок, що мережева модель захищеної ІКС побудована правильно. Вона забезпечує працездатність основних підрозділів, підтримує централізоване розміщення персональних даних у серверній зоні та реалізує обмеження доступу між сегментами. Це дозволяє використовувати модель як основу для демонстрації захисту персональних даних студентів у межах університетського підрозділу.

Окремо потрібно зазначити значення студентського сегмента в оцінці відповідності. Саме ізоляція студентської мережі є одним із найбільш наочних доказів того, що в ІКС враховано вимоги захисту персональних даних. Студенти можуть бути законними користувачами окремих освітніх сервісів, але вони не є працівниками, які обробляють персональні дані інших осіб. Тому їхній доступ до внутрішньої адміністративної частини ІКС повинен бути заборонений.

Також важливим результатом є відокремлення серверної зони. У

незахищеній або слабо структурованій мережі сервери можуть бути доступні для всіх користувачів внутрішньої мережі. У запропонованій моделі серверна зона виділена окремо, має власну підмережу і приймає з'єднання лише від визначених сегментів. Це дозволяє зменшити поверхню атаки та краще контролювати доступ до ресурсів із персональними даними студентів.

Розмежування доступу між деканатом, міжнародним відділом і фінансовим відділом також має значення для відповідності GDPR. Кожен із цих підрозділів працює з різними видами інформації, тому однаковий доступ для всіх працівників був би надмірним. У запропонованій ІКС доступ визначається функціями підрозділу. Це дозволяє зменшити надмірну обробку персональних даних і краще реалізувати принцип мінімізації.

Практична перевірка в середовищі моделювання мережевої інфраструктури дозволяє підтвердити логіку запропонованої архітектури. Якщо після налаштування VLAN, шлюзів і правил доступу дозволені з'єднання працюють, а заборонені блокуються, це означає, що запропонована модель може використовуватися як демонстраційний приклад захищеної ІКС університету. Така перевірка показує не лише теоретичну правильність рішення, а й його працездатність.

Таким чином, оцінка розробленої ІКС показує, що запропоновані технічні рішення відповідають основній меті роботи. Система забезпечує поділ мережі на окремі сегменти, централізоване розміщення персональних даних у серверній зоні, обмеження доступу між підрозділами, ізоляцію студентської мережі та контрольовану взаємодію між частинами ІКС. Це дозволяє зменшити ризик несанкціонованого доступу до особової конфіденційної інформації студентів.

Отже, розроблена захищена інформаційно-комунікаційна система університетського підрозділу відповідає основним вимогам захисту персональних даних на рівні проєктних і технічних рішень. Вона не замінює повний комплекс юридичних та організаційних заходів, але створює практичну технічну основу для безпечної обробки персональних даних студентів. Найбільш

важливими результатами є виділення серверної зони, сегментація мережі, налаштування правил доступу та ізоляція студентського сегмента від внутрішніх ресурсів університету.

## 3.4 Висновки

У третьому розділі було виконано практичну реалізацію захищеної інформаційно-комунікаційної системи університетського підрозділу відповідно до вимог захисту персональних даних. Було побудовано мережеву модель ІКС, визначено її основні елементи, налаштовано сегментацію, IP-адресацію, правила доступу та виконано перевірку працездатності запропонованої системи. Це дозволило перейти від проєктної моделі до практичного відображення контрольованої обробки персональних даних студентів у мережевому середовищі.

У межах практичної реалізації було визначено основні сегменти захищеної ІКС: серверну зону, сегмент деканату, сегмент міжнародного відділу, фінансовий сегмент, адміністративний сегмент і студентську мережу. Кожен сегмент отримав власне функціональне призначення та окремий рівень доступу до інформаційних ресурсів. Така структура дозволяє уникнути ситуації, коли всі користувачі внутрішньої мережі мають однаковий доступ до персональних даних студентів.

Серверну зону було визначено як центральний захищений елемент практичної моделі. У ній передбачено розміщення ресурсів, на яких зберігається або обробляється особова конфіденційна інформація студентів. Виділення серверної зони в окремий мережевий сегмент дозволяє контролювати доступ до персональних даних і обмежити взаємодію з боку непотрібних сегментів.

Під час налаштування мережі було використано поділ на VLAN, окрему IP-адресацію для кожного сегмента та правила контролю доступу ACL. Комутатор забезпечує підключення пристроїв і розподіл портів між VLAN, а

маршрутизатор Router-FW виконує маршрутизацію між VLAN та фільтрацію трафіку. Завдяки цьому службові сегменти отримують доступ лише до дозволених ресурсів серверної зони, а студентський сегмент ізолюється від внутрішніх ресурсів університетського підрозділу.

Перевірка працездатності підтвердила, що реалізована модель відповідає проєктній логіці розмежування доступу. Сегменти деканату, міжнародного та фінансового відділів мають доступ до дозволених ресурсів серверної зони, оскільки виконують службові функції з обробки персональних даних студентів. Водночас студентський сегмент не має доступу до серверної зони, адміністративного сегмента та робочих місць підрозділів.

Оцінка відповідності розробленої ІКС вимогам захисту персональних даних показала, що запропоновані технічні рішення узгоджуються із законодавством України та принципами GDPR. Мінімізація доступу реалізується через поділ мережі на сегменти та надання прав відповідно до функцій підрозділів. Конфіденційність підтримується виділенням серверної зони й обмеженням доступу до неї. Захист даних за замовчуванням забезпечується ізоляцією студентського сегмента та блокуванням непотрібних напрямів взаємодії.

Практична реалізація також показала, що розроблена ІКС є керованою та придатною для подальшого розширення. За потреби до неї можна додавати нові робочі місця, додаткові серверні ресурси або нові сегменти для інших підрозділів університету без зміни загальної логіки захисту. Нові елементи повинні підключатися відповідно до вже визначених принципів: окрема адресація, належність до певного сегмента та доступ лише до необхідних ресурсів.

Розроблена модель має технічний характер і не замінює повний комплекс юридичних та організаційних заходів, необхідних для впровадження вимог захисту персональних даних у діяльність університету. У межах цієї роботи основний акцент зроблено саме на практичній реалізації захищеної ІКС. Такі питання, як повний аудит відповідності, політики обробки персональних даних, строки зберігання документів або порядок роботи із запитами суб’єктів даних,

можуть бути розглянуті як подальші напрями розвитку системи.

Окремим результатом практичної реалізації є підтвердження того, що правила доступу мають бути пов’язані не з самим фактом підключення користувача до внутрішньої мережі, а з його роллю в університетському підрозділі. Деканат, міжнародний відділ, фінансовий відділ, адміністратор системи та студентський сегмент виконують різні функції, тому повинні мати різний рівень взаємодії з інформаційними ресурсами. Такий підхід дозволяє уникнути надмірного доступу та краще контролювати обробку персональних даних.

Практична модель також демонструє зв’язок між проєктними рішеннями другого розділу та їх технічною реалізацією. Виділення серверної зони, поділ мережі на сегменти, визначення IP-адресації та налаштування ACL не є окремими діями, а утворюють єдину систему захисту. Саме поєднання цих рішень дозволяє забезпечити контрольовану взаємодію між підрозділами, ізоляцію студентської мережі та захист ресурсів, у яких обробляються персональні дані студентів.

Таким чином, у третьому розділі було сформовано практичну частину захищеної інформаційно-комунікаційної системи університетського підрозділу. Запропоновані рішення дозволяють організувати серверну зону, поділити мережу на логічні сегменти, визначити IP-адресацію, налаштувати контроль доступу та перевірити працездатність моделі. Це створює технічну основу для безпечної обробки особової конфіденційної інформації студентів відповідно до вимог законодавства України та принципів GDPR.

# ВИСНОВКИ

У кваліфікаційній роботі було розглянуто питання розроблення захищеної інформаційно-комунікаційної системи університетського підрозділу для обробки особової конфіденційної інформації студентів відповідно до вимог законодавства України та принципів GDPR. Основну увагу було приділено побудові ІКС, у якій персональні дані студентів обробляються в контрольованому мережевому середовищі, а доступ до них надається відповідно до функцій користувачів і підрозділів.

У першому розділі було досліджено нормативно-правову базу захисту персональних даних і процеси їх обробки в університеті. Було визначено, що законодавство України встановлює загальні правові засади обробки персональних даних та захисту інформації в ІКС, а GDPR деталізує принципи безпечної обробки персональних даних громадян Європейського Союзу.

У процесі аналізу було встановлено, що основними ризиками університетської ІКС є надмірний доступ між підрозділами, недостатнє відокремлення серверної зони, можливість доступу студентського сегмента до внутрішніх ресурсів та відсутність чітких технічних правил взаємодії між частинами мережі. На основі цього було сформовано вимоги до захищеної ІКС: виділення серверної зони, поділ мережі на сегменти, розмежування доступу між підрозділами, ізоляція студентського сегмента та контрольована взаємодія між частинами системи.

У другому розділі було виконано проєктування захищеної ІКС університетського підрозділу. Було визначено концептуальну модель системи, її основні складові, серверну зону, робочі сегменти деканату, міжнародного та фінансового відділів, адміністративний сегмент і студентську мережу. Запропонована структура передбачає, що персональні дані студентів розміщуються в окремій серверній зоні, а доступ до них надається лише тим підрозділам, які виконують відповідні службові функції.

Під час проєктування було обґрунтовано необхідність мережевої сегментації та правил розмежування доступу. Поділ мережі на окремі логічні сегменти дозволяє обмежити зайву взаємодію між підрозділами, зменшити кількість користувачів, які можуть звертатися до ресурсів із персональними даними, та ізолювати студентський сегмент від внутрішніх ресурсів університетського підрозділу.

У третьому розділі було виконано практичну реалізацію запропонованої ІКС. Було побудовано мережеву модель, визначено VLAN, IP-адресацію, шлюзи для сегментів, склад основних пристроїв і правила доступу. На комутаторі було передбачено поділ пристроїв за VLAN, а на маршрутизаторі Router-FW — маршрутизацію між VLAN та списки контролю доступу ACL.

Практична перевірка підтвердила, що службові сегменти деканату, міжнародного та фінансового відділів мають доступ до дозволених ресурсів серверної зони, тоді як студентський сегмент не має доступу до серверної зони та внутрішніх робочих сегментів. Це показує, що реалізована модель відповідає проєктній логіці розмежування доступу.

Оцінка розробленої ІКС показала, що запропоновані рішення підтримують вимоги законодавства України щодо захисту персональних даних та інформації в ІКС, а також принципи GDPR щодо мінімізації доступу, конфіденційності, цілісності й захисту даних за замовчуванням. Розроблена модель не замінює повний комплекс юридичних та організаційних заходів, однак створює практичну технічну основу для безпечної обробки персональних даних .

Таким чином, мету кваліфікаційної роботи було досягнуто. У роботі розроблено захищену інформаційно-комунікаційну систему університетського підрозділу для обробки особової конфіденційної інформації студентів. Запропонований підхід дозволяє поєднати правові вимоги до захисту персональних даних із конкретними технічними рішеннями: серверною зоною, мережевою сегментацією, IP-адресацією, ACL та ізоляцією студентського сегмента.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ


1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 25.04.2026).
2. General Data Protection Regulation (GDPR). URL: https://gdpr.eu/ (дата звернення: 25.04.2026).
3. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 25.04.2026).
4. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 25.04.2026).
5. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://tinyurl.com/3n7zj68y (дата звернення: 25.04.2026).
6. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 25.04.2026).
7. Про освіту : Закон України від 05.09.2017 № 2145-VIII. URL: https://zakon.rada.gov.ua/go/2145-19 (дата звернення: 25.04.2026).
8. Про вищу освіту : Закон України від 01.07.2014 № 1556-VII. URL: https://zakon.rada.gov.ua/go/1556-18 (дата звернення: 25.04.2026).
9. Data protection in the EU. European Commission. URL: https://tinyurl.com/5dabwysv (дата звернення: 25.04.2026).
10. European Data Protection Board. URL: https://www.edpb.europa.eu/edpb_en (дата звернення: 25.04.2026).
11. Guidelines 9/2022 on personal data breach notification under GDPR. European Data Protection Board, 2023. URL: https://tinyurl.com/yfe78u3d (дата звернення: 25.04.2026).

12. Захист персональних даних. Уповноважений Верховної Ради України з прав людини. URL: https://ombudsman.gov.ua/ (дата звернення: 25.04.2026).

13. Посібник з європейського права у сфері захисту персональних даних. Київ : К.І.С., 2020. 436 с. URL: https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-ukr.pdf (дата звернення: 25.04.2026).

14. Захист персональних даних: правове регулювання та практичні аспекти : практичний посібник / Уповноважений Верховної Ради України з прав людини. Київ, 2021. URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/Handbook_Pers_Data_Protect_2021.pdf (дата звернення: 25.04.2026).

15. Посібник щодо захисту персональних даних : навч.-метод. посіб. / ОБСЄ. Київ, 2021. URL: https://tinyurl.com/4bumwth3 (дата звернення: 25.04.2026).

16. Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. Основи інформаційної безпеки : навч. посіб. Вінниця : ВНТУ, 2018. 316 с.

17. Інформаційна безпека : підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін. ; за ред. В. В. Остроухова. Київ : Ліра-К, 2021. 412 с.

18. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі. Книга 1 : навч. посіб. Львів : Магнолія 2006, 2013. 256 с. URL: https://tinyurl.com/kpzt35jx (дата звернення: 25.04.2026).

19. Хоменко В. Г., Павленко М. П. Комп'ютерні мережі : навч. посіб. Донецьк : ЛАНДОН-ХХІ, 2011. 316 с. URL: https://tinyurl.com/yrv4uunf (дата звернення: 25.04.2026).

20. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Ч. 1 : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с. URL: https://tinyurl.com/2wjtz9dz (дата звернення: 25.04.2026).

21. Мінухін С. В., Кавун С. В., Знахур С. В. Комп'ютерні мережі. Загальні принципи функціонування комп'ютерних мереж : навч. посіб. Харків : Вид. ХНЕУ, 2008. 210 с.

22. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека. Ч. 2 : навч. посіб. Харків : Вид. ХНЕУ, 2008. 196 с.

23. Інформаційна безпека держави : навч. посіб. / В.І. Гур'єв та ін. Чернігів : НУЧК, 2018. 166 с. .

24. Янко А. С., Вигівський Р. А. Система захисту комп'ютерної мережі. Системи управління, навігації та зв'язку. 2022. № 2. С. 91-94.

25. Наумук І. М. Використання Cisco Packet Tracer як засобу моделювання комп'ютерних мереж. ВІСНИК ХНТУ. 2024. № 1. С. 253-257.

26. Лунін Д. О., Гапон А. І. Моделювання комп'ютерних мереж : метод. вказівки. Харків : НТУ "ХПІ", 2023. 39 с. URL: https://tinyurl.com/yhe6zp98.

27. Налаштування VLAN на комутаторах Cisco : лабораторна робота № 7. Житомирський державний технологічний університет. URL: https://tinyurl.com/cd8u592t (дата звернення: 25.04.2026).

28. Сегментація мережі, використання протоколу 802.1Q. LanMarket. URL: https://tinyurl.com/5em5jdw7 (дата звернення: 25.04.2026).

29. Сегментація мережі за допомогою VLAN на Cisco. ITEDU. URL: https://tinyurl.com/552ax385 (дата звернення: 25.04.2026).

30. Що таке ACL (Access Control List) та його налаштування. Highload. URL: https://highload.tech/uk/acl-access-control-list/ (дата звернення: 25.04.2026).

31. Cisco Packet Tracer. Cisco Networking Academy. URL: https://www.netacad.com/cisco-packet-tracer (дата звернення: 25.04.2026).

32. Cisco Packet Tracer Resources. Cisco Networking Academy. URL: https://tinyurl.com/2fpwp2vd (дата звернення: 25.04.2026).

33. Configuring VLANs. Cisco Catalyst 2960 Series Switches Configuration Guide. Cisco. URL: https://tinyurl.com/yc4h935v (дата звернення: 25.04.2026).

34. Configuring VLAN Trunks. Cisco Catalyst 2960 Series Switches Configuration Guide. Cisco. URL: https://tinyurl.com/3ut73h6z (дата звернення: 25.04.2026).

35. Configure IP Access Lists. Cisco. URL: https://tinyurl.com/2tnvefuc (дата

звернення: 25.04.2026).

36. What is Network Segmentation? Cisco. URL: https://tinyurl.com/dtbnys2w (дата звернення: 25.04.2026).

37. What is a Firewall? Cisco. URL: https://tinyurl.com/mvyvras3 (дата звернення: 25.04.2026).

38. CERT-UA – Урядова команда реагування на комп'ютерні надзвичайні події України. URL: https://cert.gov.ua/ (дата звернення: 25.04.2026).

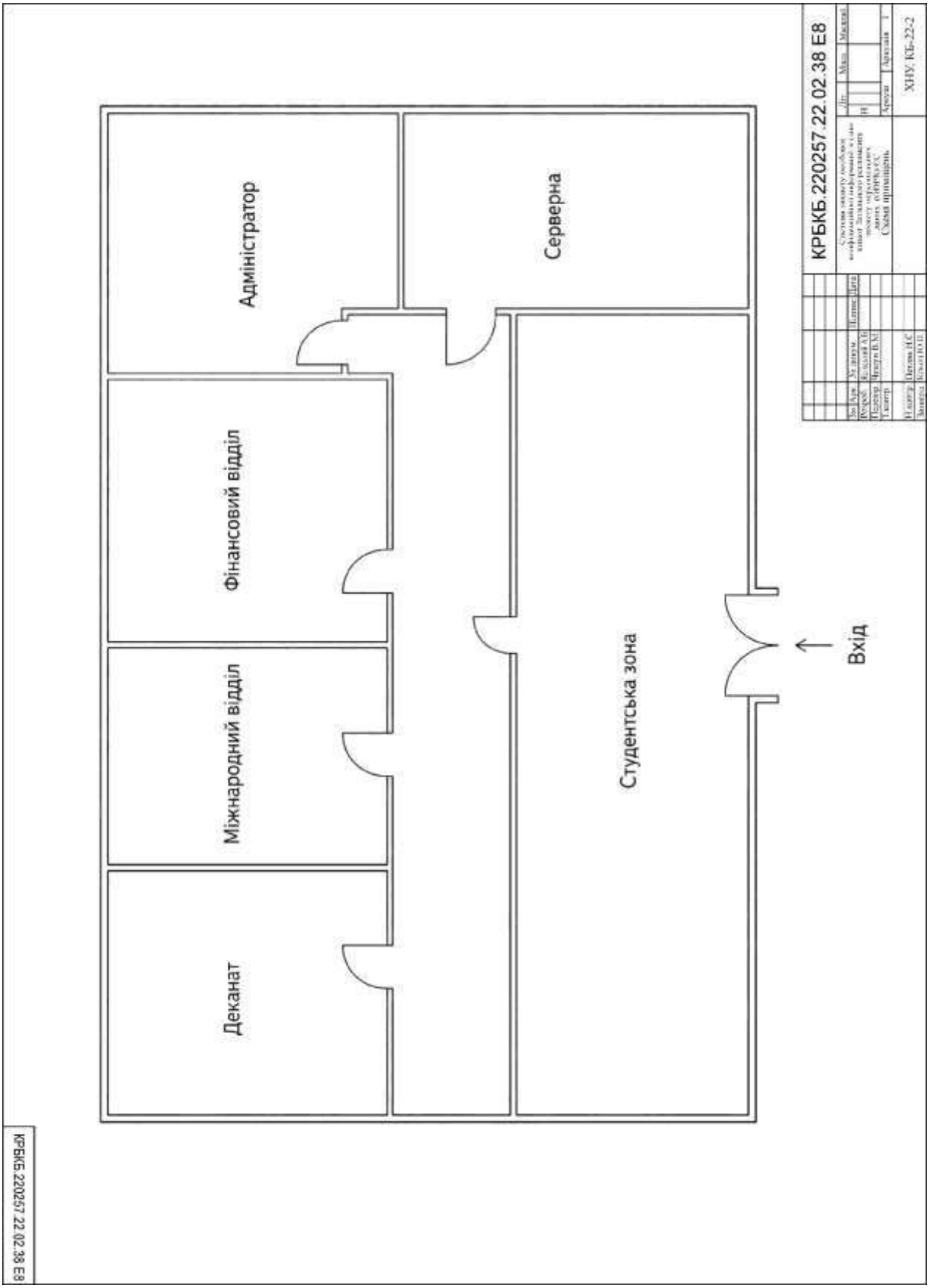
39. Рекомендації щодо захисту інформації. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/activity/security (дата звернення: 25.04.2026).

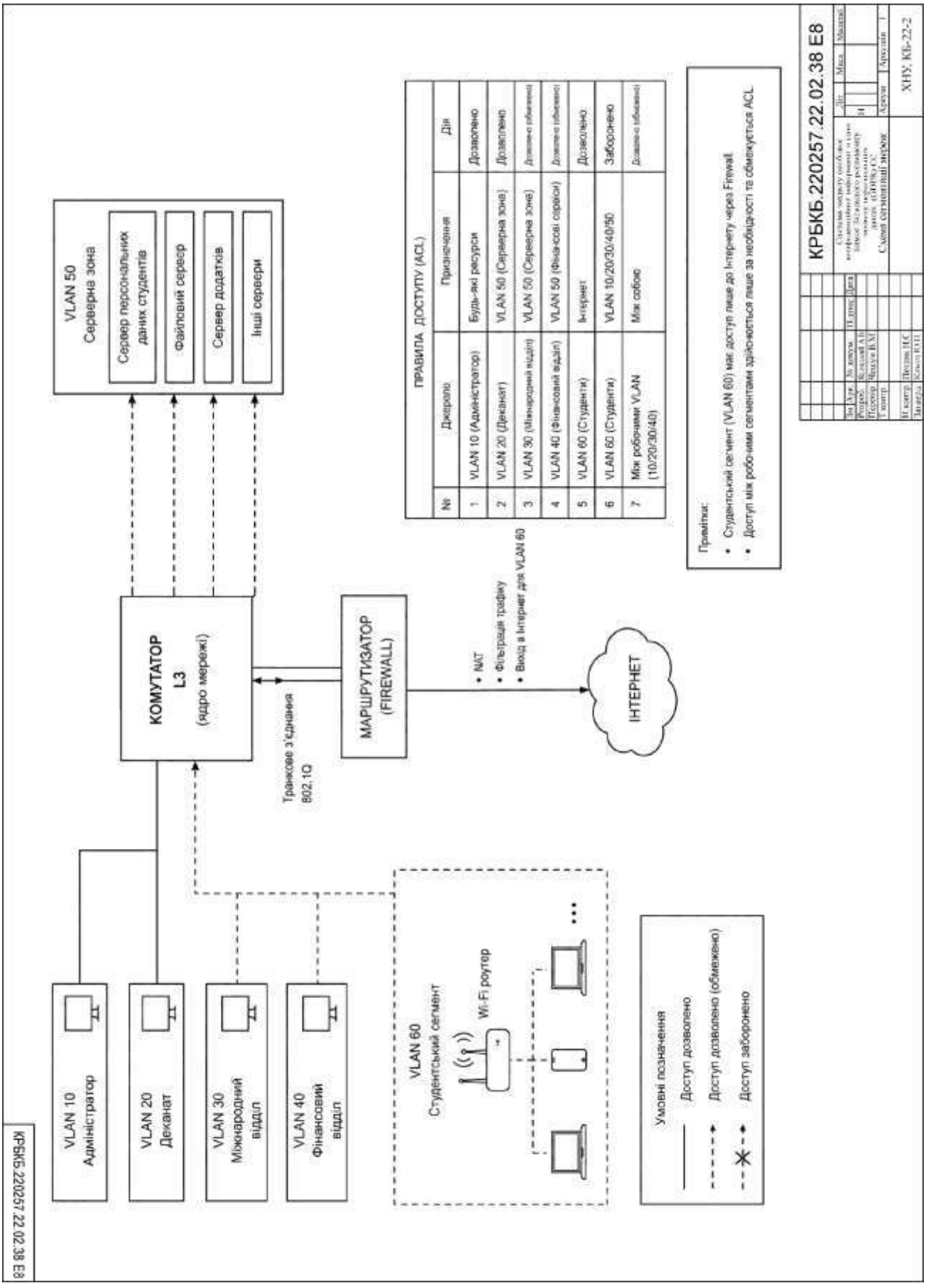
40. Основи кібергігієни та захисту даних. Prometheus. URL: https://prometheus.org.ua/ (дата звернення: 25.04.2026).

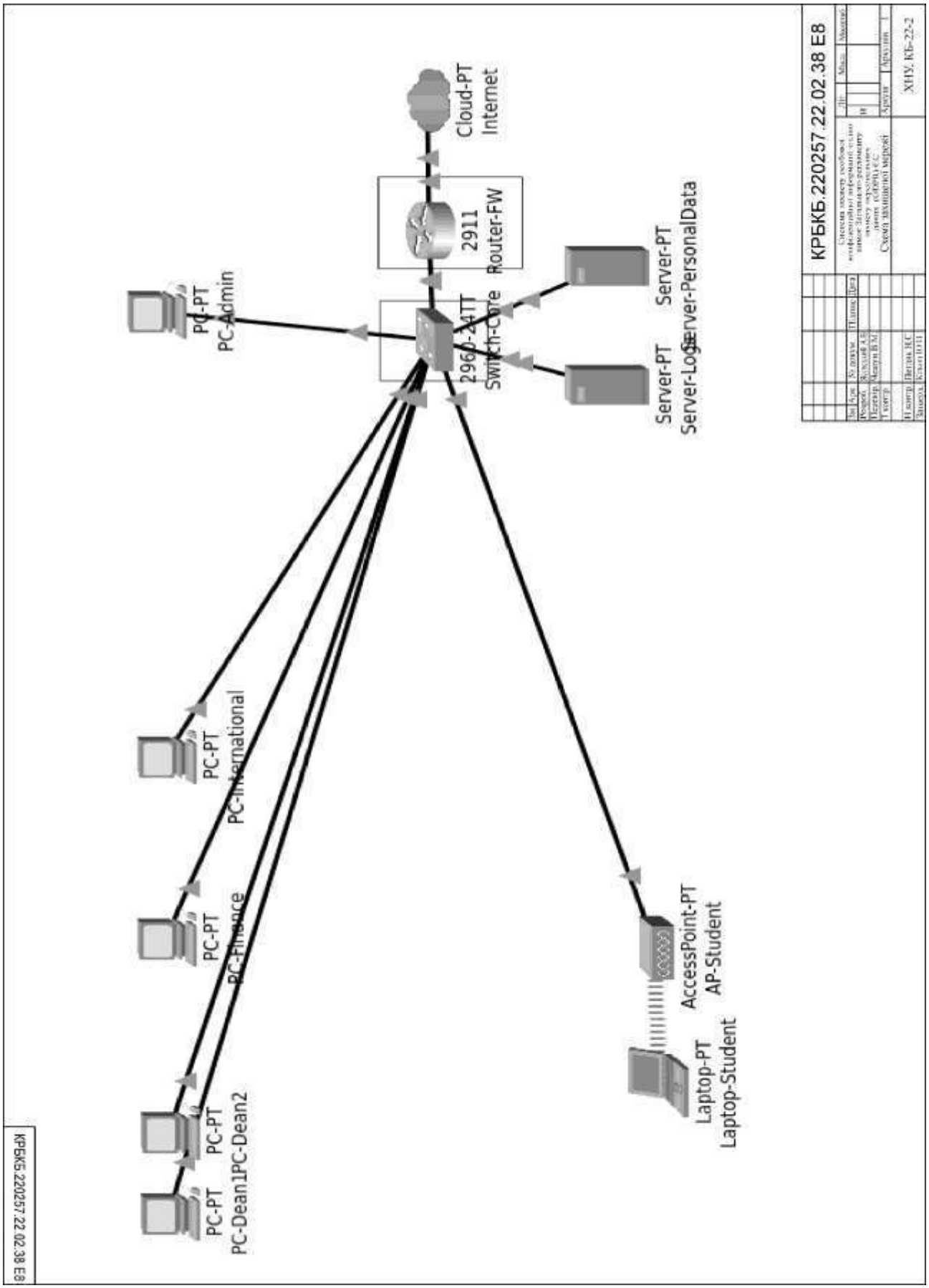
Додаток А

(обов’язковий)

Копії графічної частини




VLAN 50
Серверна зона
Сервер персональних даних студентів
Файловий сервер
Сервер додатків
Інші сервери
КОМУТАТОР
L3
(ядро мережі)
Транкове з'єднання
802.1Q
МАРШРУТИЗАТОР
(FIREWALL)
• NAT
• Фільтрація трафіку
• Вихід в Інтернет для VLAN 60
ІНТЕРНЕТ
VLAN 10
Адміністратор
VLAN 20
Деканат
VLAN 30
Міжнародний відділ
VLAN 40
Фінансовий відділ
VLAN 60
Студентський сегмент
Wi-Fi роутер
Умовні позначення
Доступ дозволено
Доступ дозволено (обмежено)
Доступ заборонено
ПРАВИЛА ДОСТУПУ (ACL)
№ | Джерело | Призначення | Дія
1 | VLAN 10 (Адміністратор) | Будь-які ресурси | Дозволено
2 | VLAN 20 (Деканат) | VLAN 50 (Серверна зона) | Дозволено
3 | VLAN 30 (Міжнародний відділ) | VLAN 50 (Серверна зона) | Дозволено обмежено
4 | VLAN 40 (Фінансовий відділ) | VLAN 50 (Фінансові сервіси) | Дозволено обмежено
5 | VLAN 60 (Студенти) | Інтернет | Дозволено
6 | VLAN 60 (Студенти) | VLAN 10/20/30/40/50 | Заборонено
7 | Між робочими VLAN (10/20/30/40) | Між собою | Дозволено обмежено
Примітки:
• Студентський сегмент (VLAN 60) має доступ лише до Інтернету через Firewall
• Доступ між робочими сегментами здійснюється лише за необхідності та обмежується ACL
КРБКБ.220257.22.02.38 Е8
Схема сегментації мережі
ХНУ, КБ-22-2
КРБКБ.220257.22.02.38 Е8


Cloud-PT
Internet
2911
Router-FW
2960-24TT
Switch-Core
PC-PT
PC-Admin
Server-PT
Server-PersonalData
Server-PT
Server-Log
PC-PT
PC-International
PC-PT
PC-Finance
PC-PT
PC-Dean1
PC-PT
PC-Dean2
AccessPoint-PT
AP-Student
Laptop-PT
Laptop-Student
КРБКБ.220257.22.02.38 Е8
ХНУ, КБ-22-2
КРБКБ.220257.22.02.38 Е8