Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Рак Ірини Іванівни

на здобуття ступеня вищої освіти Бакалавра

Система захисту передачі інформації між об'єктами критичної інфраструктури

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

КРБКБ.2101127.21.01.12 ПЗ

Виконала студентка 4 курсу, група КБ-21-1 _____ 28.05.25 Ірина РАК
Підпис, дата Ініціали, прізвище

Керівник канд. тех. наук, доцент _____ Віра ТІТОВА
Науковий ступінь, вчене звання Підпис, дата Ініціали, прізвище

Нормоконтролер старший викладач _____ 02.06.25 Сергій МОСТОВИЙ
Науковий ступінь, вчене звання Підпис, дата Ініціали, прізвище

До захисту допускаю:

Зав. кафедри кібербезпеки _____ Юрій КЛЬОЦ
Підпис, дата Ініціали, прізвище

2 06 2025р.

Хмельницький, 2025

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
15 лютого 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Рак Ірині Іванівні

1 Тема роботи Система захисту передачі інформації між об'єктами критичної інфраструктури

Керівник роботи к. т. н, доц. кафедри кібербезпеки Віра Юріївна Тітова

Затверджено наказом ректора університету від 07 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру _____

3 Вихідні дані до роботи Створити систему захисту передачі інформації між об'єтами критичної інфраструктури.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Обґрунтування вибору об'єкта дослідження; аналіз сучасних загроз передачі даних; огляд методів захисту інформації в критичних інфраструктурах; оцінка ефективності моделі через CORAS; проєктування захищеної мережевої архітектури; моделювання топології в Cisco Packet Tracer; реалізація міжмережевого захисту

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) CORAS-модель загроз, CORAS-модель загроз мережі , логічна топологія мережі

6 Консультанти розділів кваліфікаційної роботи

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

7 Дата видачі завдання 16 лютого 2025 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	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 політик експлуатації і безпеки	квітень	
Оформлення пояснювальної записки згідно вимог	травень	
Оформлення графічної частини	травень	
Захист КР	червень	

Студентка _____ Ірина РАК

Керівник кваліфікаційної роботи _____ Віра ТІТОВА

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система захисту передачі інформації між об'єктами критичної інфраструктури».

Авторка роботи: Рак Ірина Іванівна.

Керівник роботи: Тітова Віра Юріївна.

Пояснювальна записка: 80 с., 1 додатки, 17 рис., 40 джерел.

Графічна частина: __ презентаційних слайдів.

Кваліфікаційна робота присвячена розробці системи захисту передавання інформації між сегментами критичної інформаційної інфраструктури освітнього закладу. У роботі проаналізовано сучасні загрози інформаційній безпеці, особливості функціонування розподілених мережевих систем і методи забезпечення цілісності та конфіденційності переданих даних. Визначено актуальні ризики, пов'язані з міжмережевим трафіком, несанкціонованим доступом та внутрішніми загрозами.

У результаті розроблено та документовано комплексну систему кіберзахисту, що включає логічне сегментування, маршрутизацію з контролем доступу, прикладну фільтрацію, поведінковий аналіз кінцевих точок, політики безпеки та моделі загроз. Здійснено підготовку до впровадження розробленої архітектури захисту в реальну інфраструктуру навчального закладу.

28.05.25

ABSTRACT

Theme of the qualification work: «System of protection of information transfer between critical infrastructure facilities».

Author of the work: Rak Iryna Ivanivna.

Supervisor: Titova Vira Yuriivna.

Explanatory note: 80 p., 1 appendices, 17 figures, 40 references.

Graphic part: presentation slides.

The bachelor's qualification thesis is devoted to the development of a security system for protecting data transmission between segments of the critical information infrastructure of an educational institution. The study analyzes modern information security threats, features of distributed network systems, and methods for ensuring the confidentiality and integrity of transmitted data. Key risks related to inter-network traffic, unauthorized access, and internal threats are identified.

As a result, a comprehensive cybersecurity system was designed and documented, incorporating logical segmentation, inter-VLAN routing with access control, application-level filtering, endpoint behavioral analysis, security policies, and threat modeling. Preparation for the implementation of the developed protection architecture in the real infrastructure of the educational institution has been carried out.

29.05.25

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

3DES – Triple Data Encryption Standard

AES – Advanced Encryption Standard

DES – Data Encryption Standard

DDoS – Distributed Denial of Service

ECC – Elliptic Curve Cryptography

HSTS – Strict Transport Security

IDS – Системи виявлення вторгнень

IPS – Системи запобігання вторгнень

RBAC — Role-Based Access Control

RSA – Rivest-Shamir-Adleman

SIEM – Security Information and Event Management

КІ – Критична інфраструктураа

НАДПСУ – Національна академія Державної прикордонної служби України

ВСТУП

Сучасний світ стрімко розвивається завдяки інноваційним інформаційним технологіям, які суттєво змінюють спосіб управління економічними, соціальними та державними процесами. Особливе місце в цьому процесі займають об'єкти критичної інфраструктури – це енергетичні мережі, транспортні системи, фінансові установи, органи державного управління та системи зв’язку, без яких неможливо уявити стабільне функціонування держави. Ці системи є опорною ланкою національної безпеки, тому забезпечення їх безперебійної роботи та захисту інформації, що передається між ними, має суттєве значення.

У сучасних умовах зростає кількість і складність кібератак, спрямованих на порушення нормального функціонування інформаційних систем. Атаки на об'єкти КІ можуть спричиняти не лише фінансові збитки, але й мати критичні наслідки для національної безпеки, викликаючи аварійні ситуації, перебої в постачанні електроенергії, комунікаційних послуг, а іноді й загрозу життю людей. Такі загрози, як атаки типу «людина посередині», DDoS-атаки, злом мережевих протоколів або експлуатація вразливостей у програмному забезпеченні, постійно еволюціонують, що вимагає впровадження новітніх засобів захисту.

Актуальність теми зумовлена стрімким розвитком цифрових технологій та глобальною інтеграцією інформаційних систем, що стає ключовим чинником сучасного управління економічними, соціальними та державними процесами. В умовах підвищеної кіберзагроз, коли атаки стають все більш складними та численними, забезпечення безпеки даних, що передаються між критичними об'єктами, набуває особливого значення для збереження стабільності та надійності функціонування стратегічно важливих систем. Кожен об'єкт критичної інфраструктури, від енергетичних мереж до транспортних систем, фінансових установ і органів державного управління, є незамінною ланкою, без якої неможливе безперебійне функціонування держави. Зважаючи на це, порушення захисту інформації може мати не лише економічні наслідки, але й призвести до аварійних

ситуацій, перебоїв у постачанні ресурсів та навіть загрожувати життю людей. Тому розробка новітніх методів і технологій захисту передачі даних, які дозволять оперативно виявляти та нейтралізувати потенційні загрози, є актуальною проблемою сучасної інформаційної безпеки. Крім того, зростання складності і кількості кібератак вимагає від фахівців у сфері безпеки не лише постійно вдосконалювати існуючі системи захисту, а й впроваджувати інтегровані рішення, що поєднують сучасні криптографічні алгоритми, протоколи безпечного зв'язку, системи аутентифікації, а також технології виявлення та запобігання вторгненням. Актуальність теми визначається також необхідністю розробки моделей, які здатні ефективно адаптуватися до швидко мінливого кіберпростору, знижуючи ризики зловмисних дій та забезпечуючи безперервність роботи критичних систем.

Метою дипломної роботи є комплексний аналіз сучасних методів захисту інформації під час її передачі між об'єктами критичної інфраструктури та розробка інтегрованої моделі системи безпеки, здатної протистояти сучасним кіберзагрозам.

Основні завдання:

– аналіз загроз та ризиків;

– аналіз сучасних методів і технології захисту інформації, зокрема криптографічні алгоритми, протоколи безпечного зв'язку (VPN, SSL/TLS, IPSec), системи аутентифікації, а також методику виявлення та запобігання вторгненню;

– розробка моделі захисту;

– експериментальне тестування запропонованої моделі в симульованому середовищі, оцінити її ефективність та виявити можливість слабких місць з метою подальшої оптимізації.

В результаті здійснення вище наведеного переліку та врахуванням всіх недоліків буде розроблено ефективну систему захисту передачі інформації.

1 ТЕОРЕТИЧНІ ОСОНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Поняття критичної інфраструктури: визначення, класифікація, роль у безпеці держави

Критична інфраструктура – це комплекс об'єктів і систем, які змінюють вирішальну роль у забезпеченні стабільної роботи суспільства та економіки. Сюди належать передусім оборонні об’єкти, а також ті, що надають життєво важливі послуги та забезпечують комунікацію: електростанції, системи водопостачання, підприємства зберігання й виробництва харчових продуктів, ключові транспортні вузли, комунікаційні мережі, медичні та інші важливі об’єкти. Безпека й безперервність їхньої роботи, як у звичайних умовах, так і в надзвичайних ситуаціях (зокрема під час воєнного стану), є одним із головних завдань [1].

Національна система захисту критичної інфраструктури в Україні є основним інструментом, що відповідає за добробут країни. Це сукупність органів управління, сил і засобів центральних та місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі формування), органів місцевого самоврядування, операторів критичної інфраструктури, обов’язком яких є формування та/або реалізація державної політики у сфері захисту КІ. Крім того, важливою складовою роботи системи захисту країни є співпраця з іншими державами та міжнародними організаціями з метою обміну досвідом та координації спільної діяльності у цій сфері.

Необхідність захисту критичної інфраструктури надзвичайно важлива для нормального функціонування держави, особливо під час сучасних загроз, пов’язаних із військовими діями та постійними обстрілами мирних міст. У зв’язку з цим уряд нашої країни посилює заходи безпеки об’єктів, які вважаються критично важливими для життя суспільства. Наразі існує цілий комплекс заходів, які складаються з моніторингу та швидкого реагування на можливі загрози: теракти, кібератаки, стихійні лиха тощо.

Система захисту критичної інфраструктури в Україні будується на основі відповідного законодавства, яке визначає ключові принципи та завдання держави у цій сфері. Загрози, що можуть впливати на об'єкти критичної інфраструктури, включають техногенні та природні катастрофи, кібератаки й терористичні акти, що потребує впровадження ефективних заходів для їхнього попередження та нейтралізації. Державні органи, зокрема служба, відповідальна за захист критичної інфраструктури, здійснюють координацію між усіма суб'єктами, залученими до цієї сфери, забезпечуючи комплексний підхід до її безпеки. Попри високий рівень захищеності більшості стратегічних об'єктів, залишається проблема нестачі засобів протиповітряної оборони, що ускладнює їхню повноцінну безпеку. Президент та уряд постійно працюють над вдосконаленням політики у сфері захисту критичної інфраструктури, зокрема шляхом залучення міжнародних партнерів для розширення арсеналу засобів протиповітряної оборони. Однак через часті ракетні обстріли існує постійна загроза нових пошкоджень важливих об'єктів. Для стабільного функціонування критичної інфраструктури необхідний безперервний моніторинг, регулярне оновлення засобів захисту та підтримка відповідного програмного забезпечення. Це дозволяє мінімізувати ризики збоїв у роботі стратегічних об'єктів та гарантувати безпеку держави в умовах зростаючих викликів [2].

Критична інфраструктура охоплює широкий спектр об'єктів, які забезпечують функціонал держави, економіки та суспільства. Задля ефективного управління та захисту таких об'єктів поділяються на різні категорії, в залежності від їх призначення:

– за сферою діяльності: енергетична, транспортна, водопостачання та водовідведення, комунікаційна та інформаційна, фінансова, медична, оборонна, харчова промисловість;

– за рівнем важливості : національна, регіональна, місцева;

– за рівнем впливу на безпеку держави: об'єкти першочергового значення, критично важливі об'єкти, важливі об'єкти;

– за формою власності: державні, приватні, змішані;

– за рівнем захисту та ризику: об’єкти з високим рівнем ризику, середнього рівня ризику, низького рівня ризику.

Для встановлення рівня вимог щодо захисту об’єктів критичної інфраструктури з урахуванням їх значення для забезпечення окремих життєво важливих функцій у відповідних секторах, формувати їх категоризацію відповідно до категорій критичності, передбачених цим Законом [3].

Визначено наступні категорії критичності об'єктів критичної інфраструктури:

– I категорія критичності – об’єкти особливої важливості, які мають загальнодержавне значення, істотно впливають на інші складові критичної інфраструктури та порушення їх функціонування може спричинити кризову зупинку на державному рівні;

– II категорія критичності – життєво важливі об'єкти, відмови в роботі яких можуть призвести до виникнення кризових ситуацій регіонального значення;

– III категорія критичності – важливі об'єкти, збої в роботі яких можуть спричинити кризові наслідки на місцевому рівні;

– IV категорія критичності – необхідність об'єкта, порушення функціонування яких веде до кризових наслідків локального значення.

Процес категоризації об’єктів критичної інфраструктури створюється спеціалізованими секторальними органами у сфері захисту критичної інфраструктури з урахуванням специфіки відповідного сектору та вимог чинного законодавства.

Секторальні органи разом з операторами об'єктів критичної інфраструктури здійснюють категоризацію своїх секторів або підсекторів відповідно до Методики категоризації об'єктів критичної інфраструктури, затвердженої Кабінетом Міністрів України. У банківській та фінансовій сферах ця процедура здійснюється Національним банком України, а в інших сферах – державними органами, відповідальними за регулювання та нагляд за їхньою діяльністю.

Критична інфраструктура є однією з основних складових національної безпеки, оскільки її безперебійне функціонування забезпечує життєво важливі послуги для населення та підтримує стабільність економічної системи держави. До об'єктів критичної інфраструктури належать установи та системи, що забезпечують енергопостачання, водопостачання, транспорт, телекомунікації, охорону здоров'я, оборону та інші життєво важливі функції.

Перш за все, стабільність роботи об'єктів критичної інфраструктури гарантує безперебійне постачання основних ресурсів, необхідних для життєдіяльності як державних установ, так і приватних підприємств. Це включає електропостачання, водопостачання, інформаційно-комунікаційні послуги, які є базовими умовами для нормального функціонування суспільства. По-друге, ефективне функціонування критичної інфраструктури є запорукою економічної стабільності. Будь-які збої або аварійні ситуації в роботі ключових об'єктів можуть призвести до масштабних економічних втрат, порушення ланцюгів постачання та зниження довіри інвесторів, що негативно позначається на конкурентоспроможності країни на світовій арені. Також, критична інфраструктура виступає як основний елемент оборонної стратегії держави. Умови високої кібербезпеки та захищеності фізичних об'єктів дозволяють зменшити ризик впливу як кібернетичних, так і фізичних атак, що в умовах сучасних загроз набуває особливого значення. Забезпечення належного рівня захисту інфраструктурних об'єктів дозволяє оперативно реагувати на надзвичайні ситуації, мінімізувати можливі наслідки від атак або аварій, а також швидко відновлювати нормальне функціонування систем. Надійне функціонування критичної інфраструктури сприяє збереженню соціальної стабільності та довіри населення до державних інституцій. Безперебійна робота життєво важливих систем знижує ризик виникнення соціальних заворушень та сприяє підтриманню високого рівня громадської впевненості у здатності держави забезпечувати свою безпеку[4].

1.2 Загрози та вразливості в інформаційних системах об’єктів критичної інфраструктури

Інформаційні системи, що забезпечують функціонування об’єктів критичної інфраструктури, є основою сучасного управління державними ресурсами та послугами. Проте їх висока інтеграція з глобальними мережами та значна залежність від цифрових технологій створюють численні загрози і вразливості, які можуть мати руйнівні наслідки як для окремих організацій, так і для національної безпеки в цілому.

Критична інфраструктура є стратегічно важливим елементом сучасної держави, оскільки забезпечує безперебійність життєво важливих послуг та функцій у сферах енергетики, транспорту, фінансів, охорони здоров’я, зв’язку тощо. Зі зростанням рівня цифровізації та інтеграції інформаційних систем у всі сфери життєдіяльності з’являються нові виклики у сфері забезпечення кібербезпеки. Сучасні кіберзагрози характеризуються багатогранністю, що зумовлює необхідність розробки комплексних заходів захисту. Нижче описано основні види кіберзагроз , які є актуальними для об’єктів критичної інфраструктури.

Зловмисне програмне забезпечення охоплює широкий спектр шкідливих кодів, серед яких віруси, троянські програми, шпигунське ПЗ, а також програми-вимагачі. Ці загрози здатні інфікувати системи, шифрувати або видаляти дані, змінювати їх цілісність і тимчасово або повністю припиняти функціонування критичних інформаційних систем. Використання шкідливого ПЗ часто є першим кроком до подальших атак, спрямованих на компрометацію управлінських систем та доступ до конфіденційної інформації [5].

Фішинг та методи соціальної інженерії спрямовані на психологічне впливання на співробітників з метою отримання несанкціонованого доступу до систем. За допомогою підроблених електронних листів, повідомлень чи веб-сайтів зловмисники можуть переконати користувачів надати логіни, паролі або іншу конфіденційну інформацію. У критичних системах, де важлива своєчасна реакція

та правильне управління інформацією, успішне застосування цих методів може призвести до серйозних наслідків [6].

Атаки типу DDoS, зображено на рис.1.1, такі атаки мають на меті перевантаження мережевих ресурсів або серверів за рахунок великої кількості запитів, що призводить до тимчасової недоступності сервісів. Для об’єктів критичної інфраструктури така атака може стати причиною значних збоїв у роботі, що негативно впливає на економічну стабільність і безперервність життєвих процесів. В умовах сучасної кібербезпеки розгортання багаторівневих систем захисту від DDoS-атак є однією з пріоритетних задач [7].

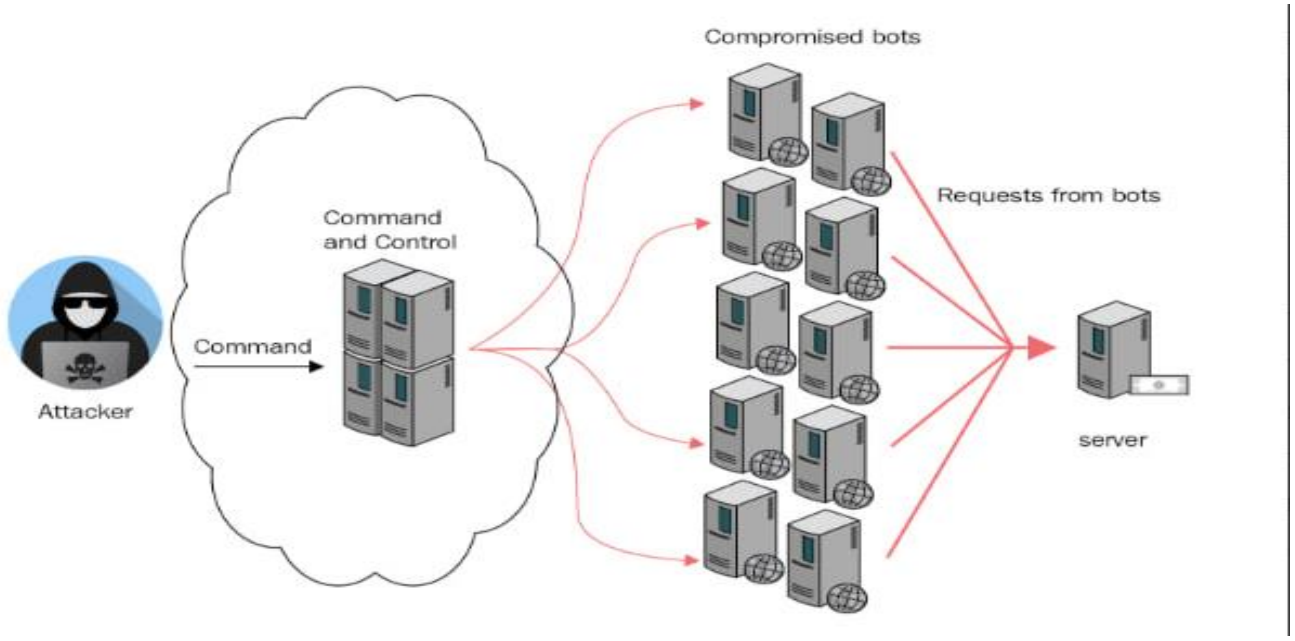


Рисунок 1.1 – Атака типу DDoS

Атаки типу «людина посередині» що зображена на рис. 1.2, під час яких, зловмисники перехоплюють та змінюють інформаційні потоки між відправником і одержувачем. Це дозволяє їм отримувати конфіденційну інформацію, модифікувати дані або вводити шкідливі команди в систему. Такий тип загроз особливо небезпечний для об’єктів критичної інфраструктури, де збереження цілісності та достовірності інформації є вирішальним для нормального функціонування [8].

Рисунок 1.2 - Атака типу «людина посередині»

Використання вразливостей у програмному забезпеченні експлуатація вразливостей, або zero-day атаки, залишається однією з найбільш актуальних загроз. Часто об'єкти критичної інфраструктури використовують застарілі або недостатньо оновлені програмні продукти, що робить їх привабливими для атак з використанням відомих або невідомих вразливостей. Успішна експлуатація таких недоліків може забезпечити зловмисникам несанкціонований доступ до систем та даних, а також можливість встановлення постійного контролю над інфраструктурою [9].

Інсайдерські загрози, які пов'язані з діяльністю власного персоналу. Інсайдерські загрози можуть бути як умисними, так і випадковими. Неправомірні дії співробітників, недбалість або порушення внутрішніх політик безпеки можуть призвести до витоку конфіденційної інформації або створення сприятливих умов для зовнішніх атак. Враховуючи високий рівень доступу, який має персонал до критичних систем, питання підвищення їх обізнаності та регулярного навчання є надзвичайно важливим [10].

Фізичні загрози для інформаційних систем об'єктів критичної інфраструктури становлять один із найважливіших чинників ризику, адже їх

реалізація може призвести до порушення доступності, цілісності та конфіденційності даних, а також до руйнування ключових компонентів системи. Ці загрози мають різноманітну природу та можуть бути класифіковані за джерелом їх виникнення: природні, техногенні, антропогенні, внутрішні, а також організаційні та технологічні вразливості.

Почнемо з природних загроз, які виникають у результаті природних процесів і явищ. Землетруси, наприклад, викликають сильні сейсмічні коливання, що здатні зруйнувати будівлі, де розташовані серверні кімнати, центри обробки даних та інше критично важливе обладнання. Такий руйнівний вплив призводить до фізичної втрати даних і може зупинити роботу ключових інформаційних систем. Повені – ще один приклад природної загрози. Затоплення приміщень з технічним обладнанням часто спричинює коротке замикання, пошкодження серверів та кабельних мереж, що веде до втрати збережених даних та порушення роботи систем. Урагани та буревії характеризуються сильними поривами вітру, які можуть спричиняти пошкодження інфраструктурних об’єктів, електромереж та систем зв’язку. Це, своєю чергою, впливає на стабільність інформаційних мереж та комунікацій. Пожежі, що можуть виникати через екстремальні температури, удари блискавки або масштабні лісові пожежі, також створюють значні ризики. Висока температура, дим і вогонь можуть завдати серйозних пошкоджень апаратному забезпеченню та комунікаційній інфраструктурі, що призводить до збоїв у роботі інформаційних систем [11].

До техногенних загроз відносяться ризики, що виникають внаслідок людської діяльності у сфері виробництва та експлуатації технологічних систем. Аварії на електромережах є типовим прикладом, оскільки перебої в електропостачанні можуть раптово вимкнути сервери, пошкодити сховища даних та призвести до виходу з ладу критичних компонентів інформаційних систем. Крім того, недостатнє охолодження серверів або мережевого обладнання, зокрема через збої у системах вентиляції та кондиціонування, може викликати критичний перегрів, що негативно впливає на працездатність апаратури і спричинює збої в

роботі систем. Хімічні витоки та вибухи, що трапляються на підприємствах, які працюють із небезпечними хімічними речовинами, є ще однією серйозною техногенною загрозою. Хімічні реакції або вибухові процеси можуть пошкодити фізичну інфраструктуру інформаційних систем, що веде до втрати або руйнування даних [12].

Антропогенні загрози спричинені безпосередніми діями людини. Вони можуть бути як навмисними, так і випадковими. Несанкціонований фізичний доступ до серверних кімнат, дата-центрів або інших критичних об’єктів дозволяє стороннім особам отримувати доступ до конфіденційної інформації, здійснювати крадіжки або навіть маніпулювати даними. Фізичне знищення обладнання через крадіжку чи вандалізм може призвести до незворотної втрати інформації та серйозних збоїв у функціонуванні систем. Терористичні атаки, включаючи диверсії, вибухи або підпали, є ще одним видом загроз, які можуть завдати масштабних руйнувань об’єктам, що містять критичні інформаційні системи. Окрім цього, помилки персоналу, зокрема неправильне експлуатаційне використання обладнання, недотримання правил пожежної безпеки або порушення інструкцій з обслуговування, можуть спричинити неочікувані збої та аварії [13].

Внутрішні загрози виникають у зв’язку з діяльністю співробітників або партнерів, які мають законний доступ до інформаційних систем. Такі загрози можуть бути як навмисними – у вигляді інсайдерських атак, коли співробітники з метою отримання фінансової вигоди або через незадоволеність своїми умовами роботи витікають конфіденційна інформація, так і випадковими, коли через недбалість або помилки співробітників відбувається ненавмисне порушення безпеки. Неправильна конфігурація систем, використання застарілого програмного забезпечення або відсутність чітких політик безпеки створюють вразливості, які можуть бути використані як зловмисниками, так і співробітниками, що не володіють необхідними знаннями з кібербезпеки [14].

Організаційні та технологічні вразливості є додатковим чинником, що значно впливає на рівень захисту інформаційних систем об’єктів критичної

інфраструктури. Незадовільна політика безпеки, яка виражається у відсутності чітких нормативних документів або несвоєчасній актуалізації процедур і стандартів кібербезпеки, може створювати умови для проникнення зловмисників у систему. Застосування застарілих технологій, що не відповідають сучасним вимогам безпеки, підвищує ризик компрометації систем через відсутність оновлень, вразливості в операційних системах та несумісність із сучасними методами захисту. Крім того, неправильне налаштування мережевих пристроїв, таких як маршрутизатори, брандмауери і системи виявлення вторгнень, створює «дірки» в захисних механізмах, що дозволяє зловмисникам обходити існуючі засоби захисту. Низький рівень підготовки персоналу, який часто є результатом недостатніх тренінгів з питань кібербезпеки, збільшує вразливість систем через використання людського фактора – співробітники можуть стати жертвами соціальної інженерії або фішингових атак [15].

1.3 Основні принципи та методи захисту інформації під час її передачі

У сучасних умовах стрімкого розвитку інформаційних технологій забезпечення безпеки інформаційних технологій забезпечення безпеки інформації набуває особливої актуальності. Передача даних, що здійснюється як у внутрішніх мережах підприємств, так і через глобальні комунікаційні мережі, супроводжується численними ризиками несанкціонованого доступу, модифікації або втрати інформації. Відповідно, надійний захист інформації під час її передачі є однією з ключових складових загальної системи кібербезпеки, що забезпечує стабільність роботи об’єктів критичної інфраструктури та державних установ.

Основні принципи захисту інформації становлять теоретичну основу для створення надійних систем безпеки, здатних протидіяти різноманітним загрозам, як зовнішнім, так і внутрішнім. Ці принципи виступають базисом для розробки технічних, організаційних та адміністративних заходів, спрямованих на

забезпечення належного рівня захищеності даних, незалежно від того, чи йдеться про конфіденційні бізнес-дані, чи про інформацію, що стосується національної безпеки. Розуміння та імплементація цих принципів є критично важливими для стабільного функціонування інформаційних систем, оскільки вони допомагають запобігти несанкціонованому доступу, зміні або втраті даних, а також забезпечують можливість відновлення нормальної роботи систем після інцидентів.

На першому місці у системі захисту інформації розташовується забезпечення конфіденційності. Цей принцип означає, що дані повинні бути доступними виключно для тих осіб або систем, які мають відповідне право доступу. Забезпечення конфіденційності вимагає впровадження ряду технологічних рішень, серед яких шифрування даних займає центральне місце. Сучасні криптографічні алгоритми дозволяють перетворювати інформацію у таку форму, що стає незрозумілою для несанкціонованих користувачів. Окрім цього, важливим елементом є розробка і впровадження систем автентифікації, які дозволяють однозначно ідентифікувати користувачів системи, а також системи контролю доступу, що гарантують, що кожен доступ до конфіденційних даних здійснюється відповідно до затверджених політик. Такий підхід мінімізує ризик витоку інформації і забезпечує високий рівень захищеності як в умовах звичайної роботи, так і під час потенційних кібератак [16].

Цілісність інформації є наступним важливим принципом, який гарантує збереження даних у первісному, незміненому стані протягом всього їх життєвого циклу. Збереження цілісності даних критично важливо для підтримання достовірності інформації, оскільки навіть незначні зміни можуть призвести до серйозних помилок у прийнятті рішень або до некоректної роботи інформаційних систем. Для забезпечення цілісності застосовуються різноманітні методи, зокрема використання криптографічних хеш-функцій, які дозволяють перевірити, що дані не були змінені, а також системи цифрового підпису, що дозволяють ідентифікувати походження інформації та виявити будь-які спроби її модифікації. У сучасних умовах, коли дані передаються по численних мережах і зберігаються на

різних пристроях, важливим аспектом є також постійний моніторинг цілісності даних та проведення аудитів систем безпеки, що дозволяє своєчасно виявити та виправити потенційні порушення [17].

Доступність інформації – це принцип, який забезпечує можливість отримання необхідних даних уповноваженими користувачами в будь-який час, незалежно від зовнішніх факторів. У сучасному інформаційному середовищі, де дані відіграють ключову роль у функціонуванні підприємств та державних установ, забезпечення високої доступності є вирішальним завданням. Різноманітні методи, такі як високодоступні серверні системи, резервне копіювання даних та плани відновлення після аварій, сприяють тому, що інформаційні системи залишаються працездатними навіть у разі виникнення технічних збоїв або кібератак. Постійний моніторинг стану систем, аналіз журналів подій і швидке реагування на інциденти допомагають забезпечити безперебійну роботу критичних компонентів, що є особливо важливим для об’єктів критичної інфраструктури.

Забезпечення доступу до інформації відповідно до принципу найменшого привілею означає, що користувачам надаються лише ті права, які необхідні для виконання їхніх службових обов’язків. Це значно зменшує ризик несанкціонованого доступу або випадкового пошкодження даних.

Багаторівневий захист - цей підхід при використанні кількох рівнів захисту – від фізичного контролю доступу до криптографічних заходів – що забезпечує до безпеки. Навіть якщо один рівень буде скомпрометовано, інші рівні залишаться активними для мінімізації загрози [18].

Основні методи захисту інформації під час її передачі між об’єктами критичної інфраструктури – це комплекс рішень, спрямованих на забезпечення безпеки даних у процесі їх переміщення, що охоплює як технологічні, так і організаційні підходи. Сучасне інформаційне середовище характеризується високою інтегрованістю мереж, коли дані переходять від одного компоненту системи до іншого через різноманітні мережеві канали, що часто є відкритими для зовнішніх впливів. Саме тому забезпечення безпеки при передачі інформації

набуває особливого значення для підтримання стабільності роботи стратегічно важливих об’єктів, де будь-яке порушення може призвести до серйозних наслідків для економіки та національної безпеки.

Шифрування даних може бути представлено за допомогою симетричних та асиметричних шифрів.

Симетричне шифрування є одним із ключових методів захисту інформації, що базується на використанні єдиного секретного ключа для процесів шифрування та дешифрування даних. Такий підхід забезпечує високу швидкість обробки інформації, що робить його зручним для захисту великих обсягів даних, зокрема в системах передавання інформації між об’єктами критичної інфраструктури. Головна перевага симетричних алгоритмів полягає у швидкості виконання криптографічних операцій, оскільки вони вимагають значно менше обчислювальних ресурсів у порівнянні з асиметричними методами. Однак основним викликом є необхідність безпечного поширення секретного ключа між сторонами, що обмінюються зашифрованою інформацією, оскільки витік ключа може призвести до повного компрометування захищених даних [19].

Одним із найсучасніших і найбільш широко використовуваних алгоритмів симетричного шифрування є AES. Цей стандарт, прийнятий Національним інститутом стандартів і технологій США, забезпечує високий рівень безпеки та ефективності завдяки застосуванню блочного шифрування. Він працює з блоками даних фіксованого розміру – 128 бітів, використовуючи ключі довжиною 128, 192 або 256 бітів. Головною особливістю AES є його стійкість до криптоаналізу завдяки використанню складної структури перестановок і підстановок у процесі шифрування. Він включає кілька раундів перетворень, кожен з яких складається з операцій заміни, змішування, перемішування та додавання ключа. Завдяки цій структурі AES залишається захищеним навіть від сучасних атак, зокрема диференційного та лінійного криптоаналізу [20].

Ще одним важливим алгоритмом симетричного шифрування є 3DES. Він розроблений на основі класичного алгоритму DES , який через обмежену довжину

ключа в 56 бітів виявився вразливим перед атаками повного перебору. 3DES використовує триразове послідовне шифрування, що значно підвищує рівень криптографічного захисту. У цьому процесі інформація спочатку шифрується одним ключем, потім дешифрується іншим, а потім знову шифрується третім ключем. Цей метод унеможливлює використання класичних атак на DES, роблячи його значно стійкішим до зламу. Однак основний недолік 3DES полягає в його меншій швидкості в порівнянні з AES, оскільки через триразове виконання операцій шифрування обчислювальні витрати значно зростають [21].

Асиметричне шифрування є одним із ключових методів криптографічного захисту даних, що базується на використанні двох пов'язаних між собою ключів – відкритого та закритого. Відкритий ключ використовується для шифрування інформації, а закритий – для її дешифрування. Це усуває проблему безпечного поширення ключів, яка є характерною для симетричних алгоритмів, оскільки відкритий ключ може передаватися вільно, тоді як закритий зберігається в таємниці та доступний лише власнику. Завдяки цій особливості асиметричне шифрування широко застосовується для забезпечення конфіденційності даних, автентифікації користувачів та цифрового підпису. Одним із найбільш відомих алгоритмів асиметричного шифрування є RSA . Він базується на складності великих чисел, що робить його стійким до зламу навіть при використанні потужних обчислювальних ресурсів. У процесі генерації ключів вибираються два великі прості числа, які перемножуються для отримання модуля, а потім обираються відкритий і закритий експоненти, що використовуються для операцій шифрування та дешифрування. Завдяки своїй стійкості RSA широко застосовується у сфері захисту електронної пошти, онлайн-транзакцій та цифрового підпису, хоча через високі обчислювальні витрати він поступається симетричним методам у швидкості. Цифрові підписи та сертифікати: використання цифрових підписів забезпечує незаперечуваність інформації, тобто підтвердження того, що повідомлення дійсно надійшло від вказаного відправника і не було змінене в процесі передачі. Сертифікати, що видаються авторитетними центрами сертифікації, підтверджують дійсність

публічних ключів. Алгоритм ECC **,** який базується на математичних операціях над еліптичними кривими. Його головна перевага полягає у високій криптографічній стійкості при значно меншій довжині ключів у порівнянні з RSA [22].

Методи контролю доступу дозволяють обмежити можливості доступу до інформації лише для тих осіб або систем, які мають на це відповідні повноваження. Серед основних підходів можна виділити:

Аутентифікація — це процес перевірки та підтвердження особи, пристрою або системи, яка намагається отримати доступ до певного ресурсу. Вона є ключовим елементом інформаційної безпеки, оскільки забезпечує, що доступ надається лише тим суб’єктам, які мають на це право. Процес аутентифікації базується на одному або кількох факторах підтвердження. Найпоширенішими є знання (паролі, PIN-коди), володіння (смарт-картки, токени, мобільні пристрої) та біометричні характеристики (відбитки пальців, розпізнавання обличчя або голосу). Сучасні системи часто використовують багатофакторну аутентифікацію, яка поєднує декілька методів перевірки, щоб підвищити рівень безпеки. Аутентифікація застосовується в різних сферах, включаючи доступ до комп’ютерних систем, фінансових сервісів, мобільних пристроїв, корпоративних мереж і навіть фізичних об'єктів. Вона є першим кроком у процесі контролю доступу, після якого може слідувати авторизація, що визначає рівень дозволів користувача на певні дії або ресурси [23]. З розвитком технологій з’являються нові підходи до аутентифікації, включаючи поведінковий аналіз, штучний інтелект і безконтактні методи перевірки особи. Це дозволяє не лише підвищити рівень безпеки, а й зробити процес ідентифікації більш зручним для користувачів.

Авторизація — це процес, який визначає права доступу користувача до ресурсів або виконання конкретних дій в інформаційній системі після підтвердження його особи через аутентифікацію. Цей етап є критично важливим для забезпечення безпеки системи, оскільки він гарантує, що після успішного входу до системи користувач отримає доступ тільки до тих ресурсів і функцій, які йому дозволено використовувати на основі його ролі та прав.

Під час авторизації система оцінює роль користувача, а також визначає його права доступу згідно з налаштованими політиками безпеки або списками доступу. Наприклад, в корпоративних або організаційних мережах доступ до інформації і ресурсів може бути обмежений залежно від того, чи є користувач адміністратором, звичайним користувачем або гостем. Адміністратори можуть мати необмежений доступ до всіх ресурсів, тоді як звичайні користувачі мають обмежений доступ тільки до тих частин системи, що відповідають їхнім функціональним обов’язкам [24].

Аудит доступу — це процес моніторингу, запису та аналізу дій користувачів або систем щодо доступу до ресурсів або інформації в рамках інформаційної системи. Метою аудиту доступу є забезпечення прозорості та контролю за використанням ресурсів, виявлення несанкціонованих дій або потенційних загроз, а також забезпечення відповідності політикам безпеки. Під час аудиту здійснюється реєстрація фактів доступу, змін або спроб доступу до інформаційних систем, що дозволяє вчасно виявляти порушення або неналежну поведінку користувачів. Процес аудиту включає збирання інформації про усі дії, що пов'язані з доступом до критичних ресурсів, таких як відкриття файлів, використання програм, а також спроби несанкціонованого доступу чи атаки на систему. Ці дані можуть бути використані для подальшого аналізу, виявлення слабких місць у системі безпеки та вжиття заходів для усунення потенційних вразливостей. Крім того, аудит доступу є важливим інструментом для відповідності стандартам безпеки та нормативним вимогам, а також для надання доказів у випадку інцидентів безпеки. Аудит доступу часто включає використання спеціалізованих інструментів, які можуть автоматично фіксувати всі дії користувачів і зберігати їх у логах. Ці логи можуть бути аналізовані для виявлення аномальних або підозрілих поведінкових патернів, які можуть вказувати на зловживання доступом або інші загрози для безпеки. Таким чином, аудит доступу є важливою складовою частиною системи безпеки, що дозволяє своєчасно реагувати на інциденти та забезпечувати захист інформації [25].

Хоча сучасні технологічні засоби є ключовими у забезпеченні інформаційної безпеки, фізичний захист також залишається невід'ємною складовою системи безпеки, до якого включаються:

Контроль доступу до приміщень є важливою складовою частиною системи фізичної безпеки, яка забезпечує захист критичних об'єктів і зон від несанкціонованого доступу. Його основною метою є регулювання того, хто має право входити в певні приміщення або території, де зберігається чутлива інформація або важливе обладнання. Це дозволяє мінімізувати ризики порушення безпеки та захистити цінні ресурси від потенційних загроз. Процес контролю доступу включає використання різноманітних технологій, таких як електронні картки або ключі, які надають доступ лише тим користувачам, хто має відповідні права. Картки можуть бути оснащені чіпами або іншими елементами для ідентифікації користувача. Крім того, зростає популярність біометричних систем, що дозволяють ідентифікувати користувачів за унікальними фізіологічними характеристиками, такими як відбитки пальців, сканування обличчя або райдужної оболонки ока. Це забезпечує більш високий рівень безпеки, оскільки біометричні дані складно підробити. Також широко використовуються пін-коди або паролі, які додають додатковий рівень захисту при відкритті дверей або доступі до приміщень. Водночас, на багатьох об'єктах застосовуються нові технології, такі як мобільні додатки, що використовують NFC або Bluetooth для безконтактного відкриття дверей за допомогою смартфонів або інших мобільних пристроїв. Це дозволяє зробити процес доступу ще більш зручним і швидким. Важливу роль відіграє також відеоспостереження з функцією розпізнавання осіб, що дозволяє не тільки фіксувати осіб, які потрапляють в охоронювані зони, але й автоматично порівнювати їх з базою даних для підвищення рівня безпеки. Крім того, системи контролю доступу можуть включати часові обмеження, які дозволяють визначати, коли саме користувачі можуть отримати доступ до приміщення, наприклад, лише в робочі години або в певні дні. Насамкінець, важливим аспектом є моніторинг і звітність. Сучасні системи можуть відстежувати та реєструвати всі дії

користувачів, що дозволяє вчасно виявляти порушення та інциденти, а також забезпечувати відповідність політикам безпеки. Це дає змогу не тільки контролювати доступ, а й аналізувати події для подальшого вдосконалення системи безпеки [26].

Захисні бар'єри та охоронні служби є ключовими компонентами фізичної безпеки, що допомагають запобігти проникненню на критичні об'єкти та створюють додатковий рівень захисту. Фізичні бар'єри, такі як огорожі, міцні стіни, замки, турнікети та інші конструкції, створюють фізичні перепони для несанкціонованого доступу. Вони можуть бути виготовлені з різноманітних матеріалів, зокрема металу та бетону, які забезпечують надійний захист від спроб проникнення або пошкодження. Такі бар'єри допомагають ефективно обмежувати доступ до чутливих територій або приміщень. Системи сигналізації також є важливими елементами фізичного захисту. Вони автоматично реагують на спроби порушити цілісність бар'єрів, наприклад, при зламі дверей або вікон, або коли виникають зміни в навколишньому середовищі, як-от дим, гази чи підвищення температури. Сучасні сигналізаційні системи включають в себе сенсори руху, відеокамери, які можуть виявляти аномальні дії, а також надсилати сповіщення у разі виявлення загрози. Охоронні служби доповнюють захисні бар'єри, забезпечуючи фізичну присутність на об'єктах. Співробітники охорони проводять патрулювання, слідкують за територією і контролюють доступ до приміщень. Вони також реагують на підозрілі ситуації і можуть взаємодіяти з правоохоронними органами для оперативного вирішення проблем. Охорона забезпечує моніторинг вхідних та вихідних потоків осіб, що дозволяє зменшити ризик проникнення сторонніх осіб та порушення безпеки. Захисні бар'єри та охоронні служби разом утворюють багаторівневу систему безпеки, яка ефективно перешкоджає незаконному доступу та реагує на загрози, що виникають. У разі надзвичайних ситуацій вони сприяють оперативному реагуванню, мінімізуючи шкоду та зберігаючи цілісність об'єкта [27].

Виявлення загроз є важливою складовою частиною забезпечення

ефективного захисту інформації. Для цього використовуються різні системи, зокрема системи виявлення вторгнень та системи запобігання вторгненням , які виконують різні функції в рамках інформаційної безпеки.

Системи виявлення вторгнень є важливим компонентом інфраструктури кібербезпеки, призначеним для моніторингу та аналізу мережевого трафіку або системних активностей з метою виявлення підозрілих дій або порушень, що можуть свідчити про спроби вторгнення або інші зловмисні дії. IDS допомагають вчасно виявити можливі загрози і зменшити ризик їхнього успішного виконання, надаючи адміністраторам системи важливу інформацію для швидкого реагування. Основною функцією систем IDS є ідентифікація аномальних або підозрілих дій, які можуть вказувати на спробу зламу або атаки. Для цього IDS використовують різні методи виявлення, зокрема, детекцію за підписами, поведінковий аналіз, а також евристичні методи. Виявлення за підписами полягає в порівнянні мережевого трафіку або дій в системах з відомими шаблонами загроз або типовими атаками, такими як віруси, трояни або спроби несанкціонованого доступу. Якщо виявляється відповідність з відомим підписом, система генерує сигнал або повідомлення для адміністратора. Більш сучасні методи виявлення включають поведінковий аналіз, при якому система навчається звичайним патернам активності в мережі або на комп'ютерах і порівнює їх з підозрілими відхиленнями. Наприклад, система може зафіксувати значне збільшення обсягу трафіку, несанкціоновану спробу доступу до важливих файлів або наявність незвичайних запитів з боку користувачів, що може вказувати на спробу кібератаки. Крім того, IDS можуть здійснювати моніторинг різних аспектів інформаційної системи, таких як мережеві підключення, журнали подій, процеси, що виконуються на комп'ютерах, і інші дані, що допомагають виявити підозрілу активність на ранніх етапах. Після виявлення загрози система зазвичай генерує попередження для адміністраторів або реагує на ситуацію, наприклад, записуючи подію в журнал або інформуючи користувачів про потенційну небезпеку. Однією з основних переваг IDS є їх здатність працювати в реальному часі, що дозволяє швидко виявляти загрози та почати процес реагування

до того, як атака або порушення безпеки завдадуть шкоди. Однак системи виявлення вторгнень не можуть самостійно заблокувати зловмисні дії або уникнути пошкоджень, тому вони часто використовуються разом із іншими заходами безпеки, такими як системи запобігання вторгненням (або фаєрволи, для створення більш комплексного рівня захисту [28]. Системи запобігання вторгненням є важливим елементом кібербезпеки, призначеним для активного захисту інформаційних систем від різноманітних загроз. Відмінною рисою IPS є не лише виявлення загроз, а й автоматичне блокування шкідливих дій, що дозволяє запобігти їхньому розвитку і мінімізувати потенційні збитки. Ці системи працюють у реальному часі, аналізуючи мережевий трафік або дії в інформаційних системах, і, в разі виявлення загрози, негайно блокують небезпечні з'єднання або обмежують доступ до підозрілих ресурсів. Вони використовують різні методи для виявлення аномалій і атак, такі як порівняння з відомими шаблонами загроз, а також більш складні техніки, що аналізують поведінку користувачів або мережевого трафіку для ідентифікації нових загроз, які не були зафіксовані раніше. Інтегровані в мережеву інфраструктуру, системи IPS здатні виявляти та реагувати на загрози в реальному часі, що є критично важливим для захисту від швидко змінюваних і складних атак. Це дозволяє системам своєчасно припиняти зловмисні дії, навіть на етапі їхнього початку, запобігаючи серйозним порушенням безпеки та зменшуючи ризики для цілісності даних. IPS також можуть коригувати доступ до ресурсів у відповідь на підозрілі активності, що робить їх важливим елементом для захисту від різних типів кібератак, таких як спроби несанкціонованого доступу, DDoS-атаки чи інші методи зловмисного вторгнення.

Завдяки своїй здатності інтегруватися з іншими елементами безпеки, такими як фаєрволи і системи виявлення вторгнень , IPS забезпечують комплексний рівень захисту, що дозволяє не лише виявляти потенційні загрози, але й миттєво на них реагувати, забезпечуючи безпеку інформаційних систем на всіх етапах їхнього функціонування. Впровадження даною системи буде корисним та ефективним рішенням [29].

1.4 Постановка задачі

Метою кваліфікаційної роботи є розробка багаторівневої системи захисту інформації при передачі даних між окремими сегментами критичної інфраструктури на прикладі інформаційно-комунікаційної мережі Національної академії Державної прикордонної служби України. Така система має забезпечувати цілісність, конфіденційність і доступність інформації у складному мережевому середовищі з підвищеними вимогами до безпеки.

Для досягнення поставленої мети необхідно:

– здійснити аналіз сучасних підходів до забезпечення кіберзахисту критичних інформаційних інфраструктур;

– провести оцінку ефективності побудованої системи на основі моделювання типових загроз і сценаріїв порушення безпеки, з урахуванням даних з CORAS-моделей ризиків;

– провести моделювання архітектури інформаційної системи об’єкта критичної інфраструктури на прикладі НАДПСУ із урахуванням структурного зонування, реалізації віртуальних підмереж (VLAN), визначення точок маршрутизації та побудови каналів передачі інформації між сегментами;

– реалізувати систему технічного захисту даних при передачі, використовуючи сучасні засоби міжмережевого екранування, засоби фільтрації прикладного трафіку (NGFW/WAF), механізми шифрування та поведінкового контролю кінцевих пристроїв EDR;

– впровадити елементи автоматизації процесів конфігурації та моніторингу за допомогою технологій Infrastructure as Code , що забезпечують централізоване управління, уніфікацію та відтворюваність параметрів безпеки.

Результатом виконання цих завдань має стати створення функціональної моделі захищеної системи передачі інформації, яка відповідає сучасним вимогам до кібербезпеки об'єктів критичної інфраструктури, забезпечує стійкість до широкого спектру загроз.

2 ПОБУДОВА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЇ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Опис об'єкта критичної інфраструктури

Національна академія Державної прикордонної служби України імені Богдана Хмельницького – вищий військовий навчальний заклад Державної прикордонної служби України, який проводить підготовку за державним замовленням військових фахівців на першому (бакалаврському) рівні вищої освіти (на основі повної загальної середньої освіти) та тактичному рівні військової освіти для Державної прикордонної служби України за 9 освітніми програмами. За 31 рік існування академією підготовлено понад 12 тисяч офіцерів- прикордонників.

Академія пропонує програми вищої освіти – від бакалаврату до магістратури та аспірантури. Навчальні плани охоплюють спеціалізацію в галузі прикордонної безпеки, міжнародних відносин, правових аспектів та інформаційних технологій, що сприяють формуванню висококваліфікованих спеціалістів. Національна академія Державної прикордонної служби України здійснює підготовку за трьома вищими освітніми програмами: бакалаврат, магістратура та доктор філософії.

Для бакалаврату приймаються громадяни України віком 17–30 років (включно ті, кому виповнюється 17 років у рік вступу) з повною загальною середньою освітою. Термін навчання – 3 роки 10 місяців за денною формою. Курсанти перебувають на повному державному забезпеченні, проживають у гуртожитках, проходять військову практику (в Україні та за кордоном) і після завершення навчання отримують ступінь бакалавра, початкове військове звання (лейтенанта) та академічне право на подальше навчання.

Програма магістратури орієнтована на офіцерів з досвідом служби, що мають здобутий ступінь бакалавра. Прийом здійснюється за державним замовленням на денної та заочної формах за спеціальностями «Безпека державного кордону» та «Правоохоронна діяльність». Вступники повинні мати досвід служби на керівних посадах не менше 5 років.

Програма доктора філософії спрямована на розвиток наукового потенціалу. Для вступу приймаються особи зі ступенем магістра (або спеціаліста), зокрема офіцери, які мають досвід роботи на оперативних посадах (для деяких спеціальностей – не менше 2 років). Навчання проводиться за денною та заочною формами, а кандидатури затверджуються відповідними державними органами [30].

Таким чином, академія забезпечує комплексну підготовку фахівців для різних рівнів військової освіти та сприяє розвитку як практичних, так і наукових компетенцій у сфері прикордонної безпеки.

В умовах сучасних загроз інформаційної безпеки та розвитку цифрових технологій питання захисту персональних даних набуває особливого значення, особливо коли йдеться про їх обробку в структурах, що забезпечують національну безпеку. Національна академія Державної прикордонної служби України є одним із ключових об’єктів критичної інфраструктури, що зберігає та обробляє великий обсяг персональних даних. Ці дані включають відомості про курсантів, співробітників, військовослужбовців, а також осіб, які проходять прикордонний контроль. Ефективне управління персональними даними в НАДПСУ базується на принципах законності, прозорості, захисту конфіденційності та мінімізації ризиків несанкціонованого доступу. Крім того, до законодавчих вимог, персональні дані обробляються з посадового забезпечення ідентифікації осіб, контролю доступу до інформаційних та фізичних ресурсів, ведення та обліку організації службової діяльності. Особливу увагу приділяю питанням інформаційної безпеки, через хід або неправомірне використання таких даних може створити загрозу для обороноздатності та правопорядку. У НАДПСУ обробка базових ідентифікаційних та контактних даних є необхідною для забезпечення належного функціонування системи управління особовим складом, організації освітнього процесу та контролю за проходженням служби.

Прізвище, ім’я, по батькові використовуються для ідентифікації особи в інформаційних системах академії, ведення особових справ, складання наказів і розпоряджень, а також для обліку в кадрових та навчальних реєстрах. Дата та місце

народження необхідні для визначення вікових обмежень щодо вступу на навчання, проходження служби та формування статистичних і аналітичних звітів про кадровий склад. Ідентифікаційний код або інший унікальний номер, наприклад, паспортні дані чи службові посвідчення, використовуються для виключення дублювання особових справ, ведення фінансового обліку, зокрема нарахування зарплати, стипендій і соціальних виплат, а також для забезпечення юридичної відповідності інформації в державних реєстрах.

Контактні дані, зокрема адреса місця проживання, необхідні для ведення обліку особового складу, визначення соціальних гарантій і пільг, організації мобілізаційних заходів та резерву, а також для забезпечення комунікації з курсантами, військовослужбовцями або їхніми родичами у разі надзвичайних ситуацій. Номери телефонів та електронна адреса використовуються для оперативного зв’язку керівництва академії та викладацького складу з особовим складом, обміну інформацією, розсилки офіційних повідомлень та управління доступом до внутрішніх інформаційних систем і онлайн-платформ НАДПСУ.

Національна академія Державної прикордонної служби України імені Богдана Хмельницького є важливим елементом критичної інфраструктури, що здійснює не тільки підготовку фахівців для Державної прикордонної служби України, а й обробляє та зберігає значну кількість персональних і конфіденційних даних. Ці дані включають відомості про курсантів, військовослужбовців, співробітників, а також осіб, які проходять прикордонний контроль. Враховуючи сучасні виклики у сфері інформаційної безпеки, Академія стає потенційною мішенню для різноманітних кіберзагроз, зокрема з боку іноземних розвідок, кіберзлочинців та інших деструктивних сил. Оскільки академія є складним навчально-адміністративним і безпековим об’єктом, що охоплює як освітні процеси, так і критичну інфраструктуру, захист даних та інформаційних систем є надзвичайно важливим. Водночас, необхідно враховувати високий рівень потенційних загроз і ризиків, що виникають через технічні, організаційні та людські фактори. Забезпечення належного захисту інформації в НАДПСУ

передбачає інтеграцію законодавчих вимог, сучасних технічних засобів і організаційних процесів для мінімізації ризику несанкціонованого доступу до конфіденційних даних, витоку інформації або її знищення. Особливо це важливо для захисту персональних даних, що використовуються для ідентифікації, управління персоналом, обліку та організації служби.

2.2 Модель захисту інформації об’єкта критичної інфраструктури

Методологія CORAS виникла як відповідь на потребу в уніфікованому та системному підході до аналізу ризиків інформаційної безпеки, який би поєднував строгі кількісні оцінки зі зрозумілою для фахівців і менеджерів візуалізацією. В її основі лежить ідея моделювання загроз у вигляді сценаріїв, що відображають як послідовність подій, так і причинно-наслідкові зв’язки між компонентами системи. Застосування CORAS передбачає не лише формалізацію термінології — таких понять, як «актив», «загроза», «вразливість», «наслідки» та «контрзаходи» — але й створення єдиної нотації для побудови діаграм, які дозволяють однозначно інтерпретувати кожен елемент моделі та його взаємодію з іншими [31].

Перший етап підготовки до аналізу ризиків за методологією CORAS полягає в чіткому визначенні того, що саме розглядається як актив. У прикладі інформаційної системи освітнього закладу активом може виступати як апаратна інфраструктура, так і дані про студентів та викладачів, не виключаючи процедурні процеси управління навчальним контентом. На наступному етапі фокус зміщується на ідентифікацію можливих загроз — кожна загроза формується у вигляді сценарію, що описує умови та дії, необхідні для досягнення шкідливої цілі. Цей підхід дозволяє системно врахувати не лише технічні, але й організаційні та людські аспекти ризиків, зокрема використання методів соціальної інженерії або помилки операторів. Подальший аналіз включає виділення вразливостей: саме вони створюють “шлях” для реалізації загрози. CORAS пропонує описувати

вразливості у вигляді відповідних елементів діаграми, які сполучаються зі сценаріями загроз та з активами стрілками, що відображають логіку атаки. Однак сам по собі лише графічний опис загрози та вразливості не дає повного уявлення про рівень ризику. Для цього необхідно надати оцінку ймовірності реалізації кожного сценарію та потенційну шкоду, яку він може спричинити. Оцінка ймовірності може базуватися як на статистичних даних про подібні інциденти, так і на експертних оцінках, а шкала наслідків часто виражається рівнями «висока–середня–низька» або конкретними величинами втрат (наприклад, вартість простою системи чи сума компенсацій). Найхарактернішою рисою CORAS є поєднання цієї кількісної інформації із зрозумілими графічними засобами. Стандартизовані символи, якими позначають активи, джерела загроз, вразливості та контрзаходи, а також різні типи стрілок, що демонструють притоки, залежності та можливі шляхи реалізації атак, створюють єдину візуальну мову моделювання. Такий формат моделі не тільки сприяє більш точному й однозначному відтворенню результатів аналізу, але й полегшує подальший перегляд і оновлення моделі у міру змін бізнес-вимог чи технічної архітектури. Після формування первинної моделі ризиків CORAS рекомендує провести процедуру валідації та коригування: залучити до обговорення зацікавлені сторони, уточнити причинно-наслідкові зв’язки, перевірити адекватність оцінок та, за необхідності, запровадити додаткові контрзаходи. До контрзаходів належать як технічні засоби (шифрування, сегментація мережі, системи виявлення вторгнень), так і організаційні (політики доступу, регулярне навчання персоналу, процедури резервного копіювання). У результаті отримують оновлену діаграму, яка демонструє, як кожен контрзахід змінює початкові оцінки ймовірності та наслідків. Застосування CORAS доречно на всіх етапах життєвого циклу інформаційної системи. На стадії проектування методологія допомагає закласти необхідні механізми безпеки до архітектури системи: під час розгортання виявляє прогалини в налаштуваннях та процесах, у процесі експлуатації забезпечує регулярний моніторинг актуальності ризик-моделі та реагування на нові загрози. Гнучкість підходу та стандартизована візуальна

нотація полегшують інтеграцію CORAS з існуючими методами управління ризиками та інструментальними платформами для моделювання та автоматизації аналізу. У результаті створюється єдина база знань про безпекові ризики організації, що підвищує прозорість прийняття рішень та оптимізує розподіл ресурсів. Методологія CORAS представлена як потужний інструмент, здатний забезпечити грунтовний аналіз ризиків інформаційної безпеки завдяки поєднанню кількісного підходу і чіткої візуалізації. Її застосування сприяє не лише виявленню й нейтралізації потенційних загроз, але й формуванню ефективних стратегій управління безпекою, що є критично важливим для підтримки безперервності операцій в умовах постійно зростаючих кіберзагроз [32].

Аналіз загроз інформаційній безпеці об’єктів критичної інфраструктури вказує на необхідність врахування як зовнішніх, так і внутрішніх чинників, що можуть становити небезпеку для конфіденційних даних та стабільності функціонування інформаційних систем. Національна академія Державної прикордонної служби України, як стратегічний військовий та освітній заклад, зберігає й обробляє значні обсяги чутливої інформації, зокрема дані про персонал, курсантів та службову діяльність. Саме тому побудова надійної моделі захисту інформації є критично важливою для забезпечення безпеки на всіх рівнях. Для ефективного структурування та візуалізації взаємозв’язків між активами, загрозами, вразливостями та наслідками використовується методологія CORAS, яка дозволяє наочно продемонструвати можливі сценарії реалізації загроз та заходи з їх нейтралізації. На рисунку 2.1 відображено Coras – модель баз даних , що ставить під удар конфіденційність.

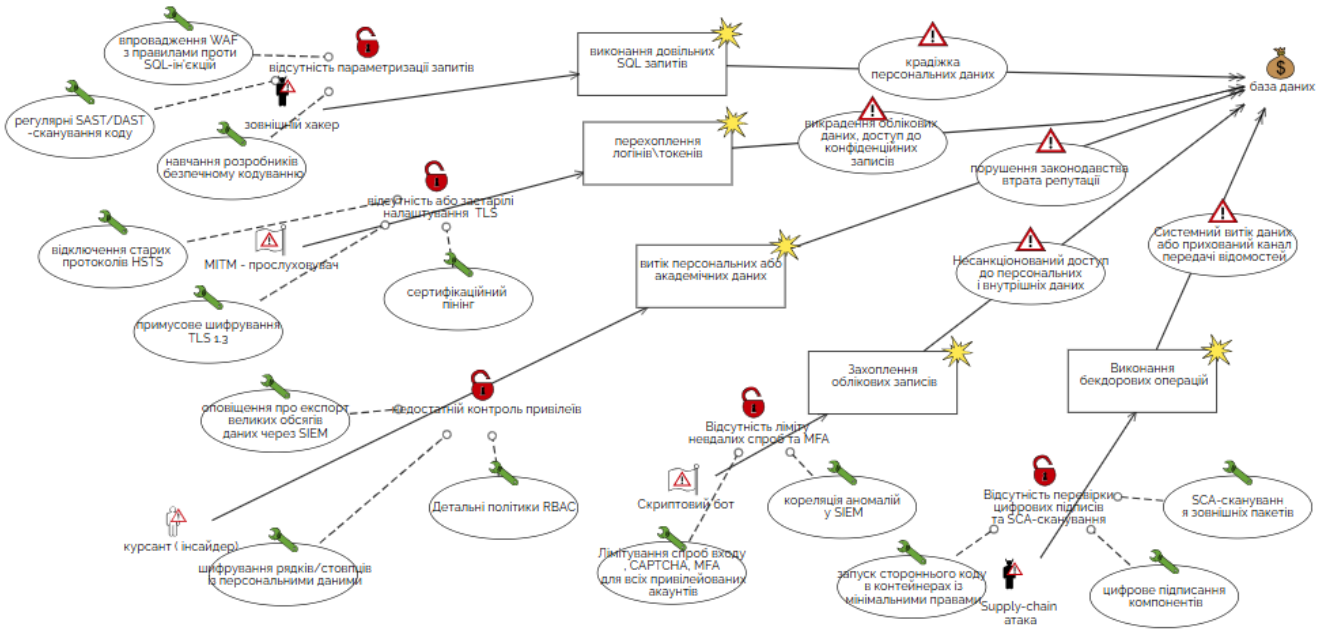


Рисунок 2.1 Coras – модель баз даних , що ставить під удар конфіденційність

У межах моделювання потенційних інформаційних загроз для освітньої установи як об'єкта критичної інфраструктури, окрему увагу було приділено загрозам, що походять від внутрішніх суб'єктів системи, зокрема — від інсайдерів. Як приклад змодельовано ситуацію, за якої курсант освітнього закладу, маючи базовий доступ до навчального порталу або бази даних із оцінками, реалізовує несанкціоноване читання або експорт конфіденційної академічної інформації. Джерелом такої вразливості є недостатній контроль рівнів доступу на читання (READ-only), що дозволяє особам з мінімальними привілеями отримати доступ до даних, які не передбачені для перегляду з їхнього боку. Результатом реалізації подібної загрози може стати витік персональних та академічних даних — зокрема, оцінок, результатів атестацій, відомостей про академічні борги тощо. Подібні витоки порушують норми чинного законодавства у сфері захисту персональних даних, зокрема Закону України «Про захист персональних даних», а також несуть загрозу репутаційним позиціям навчального закладу. З метою нейтралізації загрози з боку внутрішнього інсайдера було розроблено і впроваджено комплексну систему контрзаходів. Реалізовано детальну модель управління доступом на основі ролей , яка забезпечує суворе розмежування прав доступу до інформаційних об'єктів

відповідно до функціональних обов’язків суб’єктів системи [33]. Зокрема, кожному курсанту надається лише той мінімальний обсяг прав, який необхідний для виконання їх навчальних завдань, без можливості перегляду або експорту оцінок інших користувачів. Крім того, для підвищення рівня конфіденційності персональних записів, у базі даних впроваджено шифрування окремих рядків або стовпців, які містять чутливу інформацію — наприклад, ПІБ, академічні результати, номери документів. Шифрування виконується із застосуванням симетричних алгоритмів з керуванням ключами через окремі сервіси захисту, що дозволяє забезпечити як збереження конфіденційності, так і можливість контролю доступу до зашифрованих полів на рівні запитів. Окрім цього, у систему інтегровано механізми моніторингу активності користувачів з використанням рішень класу SIEM. Налаштовано оповіщення про спроби масового експорту даних або багаторазове читання великої кількості записів у межах нетипової активності користувача. Такі події автоматично фіксуються, корелюються з іншими подіями безпеки та передаються на аналіз адміністраторам системи безпеки. Це дозволяє не лише мінімізувати ризики витоку даних, а й вчасно реагувати на потенційні інциденти, зберігаючи довіру до інформаційної системи та дотримуючись вимог нормативно-правового регулювання у сфері інформаційної безпеки.

Атаки типу «людина посередині» .Існування цієї вразливості є відсутність або некоректна конфігурація захищених протоколів передачі даних, зокрема використання застарілих версій TLS, які не забезпечують належного рівня криптографічного захисту. У результаті, дані, що передаються між клієнтом та сервером, можуть бути перехоплені у відкритому вигляді або розшифровані за допомогою відомих методів компрометації шифрування. Інцидент, що стався на основі такої вразливості, призвів до успішного перехоплення сесій користувачів, що дало змогу хакеру отримати облікові дані та здійснити несанкціонований доступ до конфіденційної інформації, зокрема до записів у базі даних. Це, у свою чергу, створило передумови для потенційного витоку персональних даних і

порушення політик конфіденційності, що може мати серйозні юридичні та репутаційні наслідки для установи. Для усунення зазначеної вразливості було здійснено примусове застосування сучасної версії протоколу TLS 1.3, реалізовано механізм сертифікатного пінінгу для запобігання підміні сертифікатів у процесі встановлення з'єднання, відключено підтримку застарілих криптографічних протоколів, а також активовано політику HTTP Strict Transport Security , що забезпечує примусове використання HTTPS у всіх взаємодіях між клієнтом і сервером [34].

Захоплення облікових записів через автоматизовані атаки ботів. Ці атаки ґрунтувалися на масовому підборі паролів (brute-force) або використанні облікових даних, викрадених із інших сервісів, що мають спільну з цільовою системою автентифікаційну модель. Основними чинниками, які зумовили реалізацію даної загрози, були відсутність механізмів обмеження кількості спроб входу в обліковий запис, використання спрощених механізмів автентифікації, а також брак засобів активного поведінкового моніторингу у процесі автентифікації користувачів. Внаслідок цього сталася часткова компрометація користувацьких акаунтів, що призвело до несанкціонованого доступу до персональних даних у системі, зокрема до журналів успішності, контактної інформації та навчальних профілів. З метою мінімізації ймовірності повторення подібних інцидентів, було впроваджено низку превентивних заходів. Зокрема, реалізовано captcha для перевірки автентичності користувача при вході, запроваджено обов’язкову багатофакторну автентифікацію (MFA) для користувачів з розширеними правами, а також інтегровано систему виявлення аномалій у поведінці через платформу SIEM. Окрім того, удосконалено політику розмежування прав доступу, що дозволило істотно зменшити потенційну шкоду навіть у разі часткової компрометації облікових записів. Загроза, пов’язана із так званими атаками ланцюга постачання (supply chain attacks). Ці загрози реалізуються через впровадження шкідливих змін у стороннє програмне забезпечення, яке інтегрується в інформаційну систему освітньої установи [35]. Аналіз показав, що через відсутність обов’язкової перевірки цифрових підписів

програмних компонентів, а також брак політик перевірки походження бібліотек, що використовуються у серверному середовищі, став можливим запуск стороннього коду в контейнері з привілеями адміністратора. Внаслідок цього була створена загроза виконання прихованих бекдорних операцій, які не фіксуються звичайними журналами аудиту, що унеможливлює вчасне виявлення та реагування на інцидент. Для протидії цим викликам було впроваджено системний підхід до управління безпекою програмного забезпечення: зокрема, реалізовано автоматизований аналіз складу програмних залежностей , налагоджено цифрове підписання внутрішніх компонентів, а також уведено обов'язкову перевірку цілісності та автентичності всіх бібліотек, які проходять інтеграцію в основну систему. Таким чином, було значно знижено ризик прихованого впровадження шкідливого ПЗ та підвищено стійкість освітньої IT-інфраструктури до цільових атак На рисунку 2.2 наведено розгорнуту CORAS-модель загроз, що ставлять під удар цілісність бази даних академічної інформаційної системи. Цей сценарій ілюструє ланцюжок від виявлених вразливостей до небажаних подій та наслідків, а також демонструє впроваджені контрзаходи, які забезпечують відновлення точності й повноти даних після інцидентів.

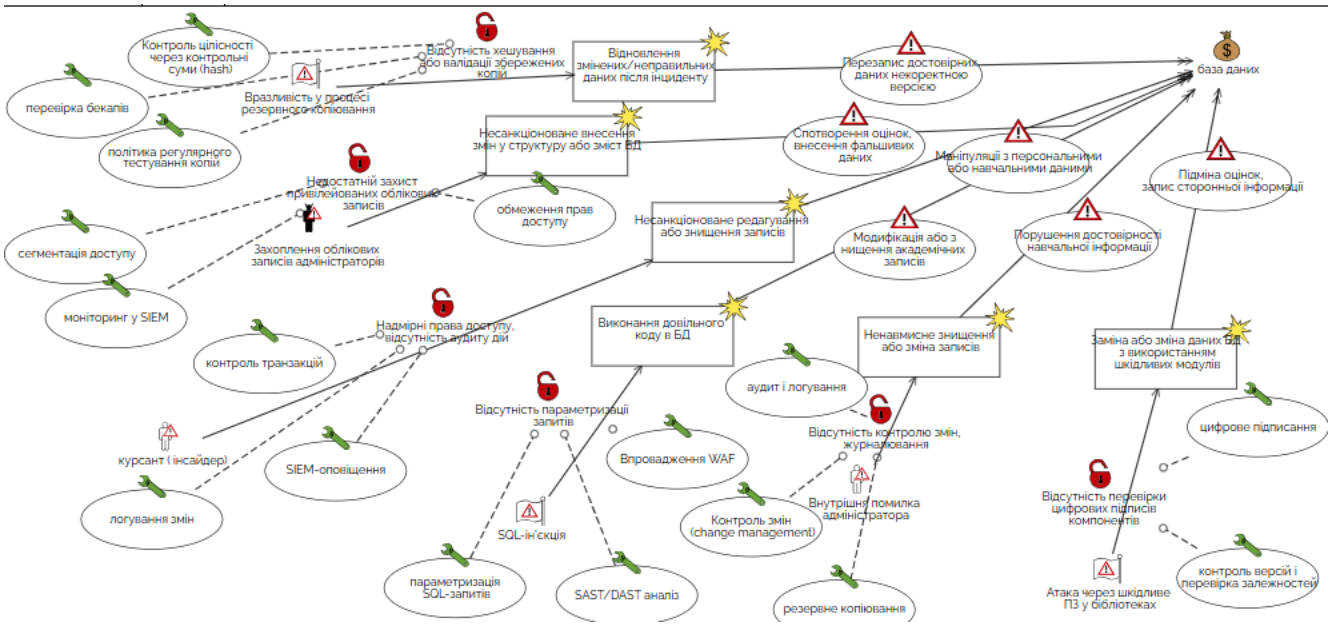


Рисунок 2.2 Coras – модель баз даних , що ставить під удар цілісність

У ході аналізу CORAS-моделі для бази даних академії було виявлено суттєву вразливість у процесі організації резервного копіювання, що безпосередньо загрожує цілісності інформаційних активів. Зокрема, відсутність механізмів криптографічного хешування та валідації збережених бекапів створювала умови для непомітних змін або пошкоджень архівів під час їхнього зберігання й передавання. Після інциденту могла відбутися автоматична відновлювальна операція з архівів, які вже містили некоректні дані — таким чином достовірні таблиці системи замінювалися спотвореними версіями, що підривало довіру до інформації та унеможливлювало коректне відновлення навчальних і адміністративних записів. На виявлену вразливість було реалізовано багаторівневу систему контролю цілісності резервних копій. Елементом цієї системи стало обчислення криптографічної хеш-суми (наприклад, за алгоритмом SHA-256) для кожного створеного архіву, причому значення контрольної суми зберігаються окремо від самих файлів, що унеможливлює їхню зміну без відповідного сліду в системі валідації. Під час відновлення бекапу автоматизована процедура порівняння поточної хеш-суми з оригінальною дозволяє виявити найменші невідповідності та відхилити потенційно зіпсовані чи змінені копії. Крім того, для гарантованого виявлення прихованих дефектів та своєчасного коригування можливих розбіжностей, запроваджено політику регулярного тестування процесу відновлення.

Захоплення облікових записів адміністраторів. Джерелом цієї загрози виступають зовнішні та внутрішні зловмисники, які, використовуючи вразливості в процесі автентифікації, здобувають контроль над привілейованими обліковими записами. Виявлено, що відсутність багатофакторної автентифікації сприяє успішному проведенню атак із застосуванням технік фішингу, brute-force або повторного використання викрадених паролів. У сукупності з нечіткою сегментацією прав і надмірним рівнем доступу ця вразливість дозволяє зловмисникам вільно вносити як структурні, так і контентні зміни до бази даних. Під час одного з тестових сценаріїв атак було продемонстровано, що отримавши

привілейований доступ, атакувальник може змінити ключові параметри таблиць, додати або вилучити записи з бази даних оцінок. Така модифікація суті навчальної інформації фактично призводить до втрати цілісності. Для нейтралізації було запроваджено багатофакторну автентифікацію зробило необхідним подвійне підтвердження особи адміністратора під час кожного входу, що суттєво ускладнило використання викрадених облікових даних. Відбулося суворе сегментування мережевої та прикладної інфраструктури з реалізацією принципу найменших привілеїв, згідно з яким кожен обліковий запис отримав лише ті права, які безпосередньо необхідні для виконання службових задач. Водночас було впроваджено централізовану систему моніторингу подій безпеки (SIEM), що дозволяє в режимі реального часу корелювати події входу, виявляти нетипові дії адміністраторів та автоматично генерувати сповіщення для служби реагування на інциденти.

Діяльність інсайдерів — курсантів , які мають надмірні привілеї доступу. Нечітко визначені ролі в межах системи контролю доступу сприяли тому, що користувачі з базовим READ-only або розширеним рівнем могли виконувати DML-операції без належного спостереження, а відсутність комплексного механізму аудит-трейлу не дозволяла своєчасно виявляти підозрілі транзакції. Унаслідок цього зловмисник мав змогу видалити окремі записи, змінити оцінки та службові відомості, а також підмінити персональні дані курсантів, що істотно підірвало довіру до інформаційної системи й створило ризики юридичної відповідальності за недотримання вимог законодавства про захист персональних даних. Як наслідок, було прийнято рішення впровадити гнучку модель розмежування доступу на основі ролей (RBAC), яка передбачає суворе віднесення кожного користувача до певної групи з жорстко обмеженими привілеями та забороною будь-яких операцій, не передбачених посадовими обов’язками. Одночасно на рівні СУБД було налаштовано детальне логування всіх SQL-запитів змін (INSERT, UPDATE, DELETE), при цьому аудиторські журнали зберігаються у незмінному форматі WORM та регулярно аналізуються за допомогою SIEM-системи. У разі спроб

масового видалення записів або появи невластивих ролі транзакцій адміністратори отримують негайні сповіщення, що дозволяє оперативно втрутитися, відкотити зміни та відновити достовірність даних із інтегрованих резервних копій.

Сценарій SQL-ін’єкції, який є одним із найпоширеніших і водночас найнебезпечніших векторів атак на реляційні СУБД. Загрозу атак SQL-ін’єкції становить зовнішній зловмисник, що через вразливості в механізмі обробки користувацького вводу отримує можливість впроваджувати у запити до бази даних довільні фрагменти коду. Основною причиною успішної реалізації такого інциденту виявилася відсутність у програмному коді параметризації SQL-запитів, через що дані користувача, інтерпретовані як частина команди, дали зловмиснику привід для виконання несанкціонованих операцій на сервері бази. В результаті атаки відбувалася модифікація або навіть повне видалення академічних записів — оцінок курсантів, історії змін і іншої критично важливої інформації, що призводило до порушення цілісності даних та значних репутаційних і операційних втрат для навчального закладу. Щоби запобігти подібним загрозам у подальшому, було реалізовано багаторівневий підхід до захисту: по-перше, інтегровано веб-аплікаційний фаєрвол (WAF) з набором пр авил, що виявляють і блокують спроби SQL-ін’єкцій у режимі реального часу, по-друге, організовано регулярне автоматизоване сканування коду за допомогою інструментів статичного та динамічного аналізу безпеки (SAST/DAST), яке дозволяє виявляти вразливі місця ще на етапі розробки, і по-третє, удосконалено механізм доступу до даних шляхом повного переходу на параметризовані SQL-запити, що гарантує розділення структури команди та даних користувача.

Також було розглянуто сценарій, в основу якого покладено внутрішню помилку адміністратора при управлінні записами. Ця загроза виникає внаслідок відсутності належного контролю змін у структурі та вмісті таблиць, а також недостатнього журналювання адміністративних операцій на рівні транзакційної системи. У результаті некоректних дій може відбутися ненавмисне видалення або модифікація навчальних записів, що призводить до порушення достовірності

академічної інформації — від спотворення оцінок окремих курсантів до розриву історії змін у всіх підсистемах обліку. Для запобігання таким інцидентам у подальшому було запроваджено формалізований процес управління змінами (change management), який передбачає погодження будь-яких коригувань на рівні керуючої ради з ІТ-безпеки, а також обов’язкову процедуру резервного копіювання перед застосуванням будь-яких оновлень [36]. Окрім того, на рівні СУБД організовано детальне логування всіх DML-операцій з використанням незмінних журналів подій, що дозволяє не лише відстежувати послідовність адміністраторських дій, а й своєчасно відновлювати вихідний стан даних у разі виявлення помилкових змін.

Сценарій, пов’язаний із впровадженням шкідливого програмного забезпечення через сторонні бібліотеки. Цей вектор атаки можливий у випадках, коли при інтеграції компонентів до складу системи не перевіряються цифрові підписи пакетів, а також відсутні механізми контролю залежностей і версій. У результаті зловмисний модуль може незалежно виконувати операції з базою даних, зокрема замінювати або неправдиво модифікувати записи, що стає причиною підміни академічних оцінок або додавання сторонньої інформації у навчальні журнали. Для попередження подібних інцидентів було впроваджено процедуру обов’язкового цифрового підписання всіх компонентів перед інтеграцією, встановлено централізований контроль версій із процедурою перевірки сумісності залежностей (SCA), а також реалізовано регулярні аудити складових системи та автоматизовані перевірки цілісності пакунків.

На рисунку 2.3 продемонстровано основні ризики, що загрожують доступності бази даних, а також демонструє сукупність технічних та організаційних заходів, спрямованих на оперативне відновлення функціональності із мінімальними перебоями та забезпечення безперервної роботи освітньої системи

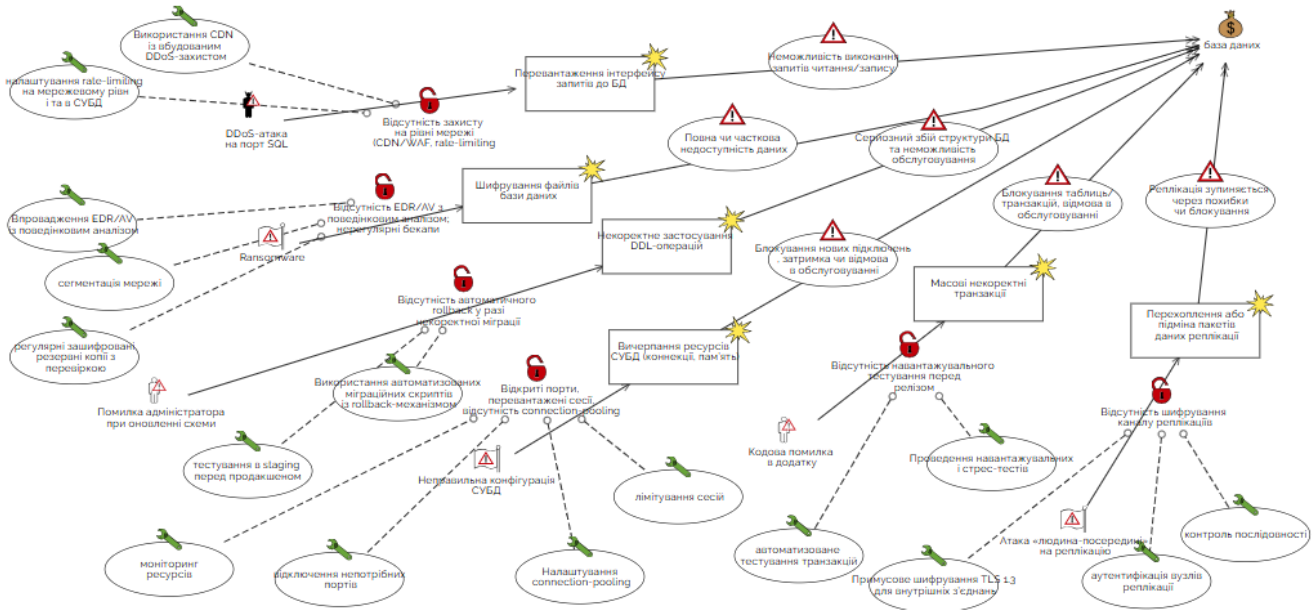


Рисунок 2.3 – Coras – модель баз даних , що ставить під удар доступність

DoS-атаки на порт SQL як одне із найбільш критичних випробувань доступності системи. Такий тип атаки стає можливим у разі відсутності відповідних мережевих бар'єрів: зокрема, коли не застосовано CDN або WAF із механізмами виявлення аномальної активності та не налаштовано обмеження швидкості запитів (rate-limiting). Зловмисник, генеруючи масивні одночасні виклики до інтерфейсу SQL, штучно створює навантаження, що призводить до виснаження ресурсів сервера бази даних та нездатності обробляти легітимні операції читання чи запису. Підтверджуючи цей сценарій у тестовому середовищі, було продемонстровано різке зростання часу відгуку й падіння пропускної здатності запитів, що у разі реальної експлуатації могло б заблокувати доступ факультетів, викладачів і студентів до освітніх сервісів. Для підвищення стійкості системи було прийнято рішення про інтеграцію CDN-провайдера з вбудованою DDoS-захистом, який виконує розподіл вхідного трафіку на географічно розподілені вузли та відсіює підозрілі запити на кордоні мережі [37]. Одночасно на рівні серверного обладнання та СУБД налаштовано політики rate-limiting, що встановлюють ліміти на максимальну кількість паралельних з'єднань і швидкість запитів із однієї IP-адреси. У разі перевищення порогових значень система

автоматично обмежує або відхиляє подальші запити, не допускаючи вичерпання ресурсів. Такий комплексний підхід поєднує розподілену фільтрацію мережевого трафіку з внутрішніми механізмами контролю навантаження, що забезпечує безперервну доступність бази даних навіть у умовах інтенсивних зовнішніх атак.

Виявлено загрозу з боку програм-шифрувальників (ransomware), яка здатна повністю блокувати доступ до критичних даних у разі успішного проникнення шкідливого коду. Причиною реалізації цієї вразливості стала відсутність у середовищі EDR/AV-рішень із поведінковим аналізом. Усуненням цієї загрози стало зашифрування файлів бази даних, у результаті якого користувачі втратили можливість виконувати операції читання та запису, що призвело до часткової чи повної недоступності інформаційної системи й значного простою освітніх сервісів. Розгорнута платформа EDR/AV із механізмами поведінкового аналізу, яка дозволяє виявляти підозрілі процеси шифрування в реальному часі та автоматично ініціювати ізоляцію уражених вузлів , мережна інфраструктура була сегментована таким чином, щоб обмежити горизонтальне поширення шкідливого ПЗ: критичні сервери баз даних опинилися в окремій зоні з жорсткими правилами доступу, тоді як менш важливі системи розташовано в сегментах із мінімальними правами. Для забезпечення стійкості до можливих атак було запроваджено політику регулярного створення зашифрованих резервних копій із подальшою перевіркою цілісності архівів за допомогою контрольних сум.

Вразливість, автоматичного механізму відкату змін у разі некоректного виконання DDL-операцій. Під час планового оновлення схеми, що виявився неповним і вивів базу в некоректний стан: відбулося порушення зовнішніх ключів, а частина таблиць втратила зв’язки з основними сутностями. Цей випадок підкреслив важливість повсюдного використання автоматизованих міграційних скриптів, які не лише підтримують належну версіонність схеми, але й містять вбудовані механізми транзакційного відкату (rollback) у разі виявлення помилок на будь-якому етапі виконання. Такі скрипти дозволяють гарантувати атомарність змін: у разі збоїв у процесі оновлення система автоматично повертає стан бази до

останньої відомої стабільної версії. Незалежно від цього, для додаткової перевірки було впроваджено обов'язкове виконання всіх міграційних операцій у середовищі staging, відокремленому від продуктивної інфраструктури. У staging-середовищі нова схема піддавалася комплексному тестуванню на коректність відносин між таблицями, продуктивність запитів та узгодженість даних, що дозволило виявити і виправити логічні помилки у міграційних скриптах до остаточного розгортання в продакшені. Крім технічного удосконалення процесу міграцій, адміністративна та інженерна групи були залучені до розробки формалізованої політики change management, яка передбачає поетапний прогін оновлень з попередньою перевіркою ризиків, затвердженням відповідальних осіб та документуванням кожної зміни. За кожним релізом закріплено власний трекер із фіксацією версії скриптів, результатів автоматичних тестів та підсумкового рішення про розгортання в продуктивній системі.

Некоректні налаштування СУБД становлять серйозну загрозу доступності системи. Зокрема, експлуатація невикористаних мережевих портів у поєднанні з відсутністю connection-pooling та незадіянням лімітування сесій спричинила виснаження ресурсів сервера бази даних — він вичерпав усі доступні з'єднання й оперативну пам'ять. Наслідком цього стала неможливість встановити нові підключення, різке зростання часу відповіді на запити й фактична відмова в обслуговуванні користувачів, що паралізувало ключові освітні сервіси та призвело до зриву навчального процесу. Для запобігання подібних інцидентів у майбутньому було впроваджено connection-pooling із чітко визначеними навантажувальними лімітами на одночасні сесії, що дозволило ефективніше розподіляти ресурси та уникнути їхнього передчасного вичерпання , для своєчасного виявлення потенційних «вузьких місць» у роботі сервера організовано безперервний моніторинг ключових метрик — кількості відкритих з'єднань, використання пам'яті та завантаження CPU. У разі перевищення критичних порогів система автоматично генерує сповіщення для адміністраторів бази даних, що дозволяє оперативно реагувати ще до настання повної відмови обслуговування.

Інцидент, спричинений логічною помилкою в програмному коді клієнтського додатку, що взаємодіє з базою даних. Основною причиною проблеми стала відсутність навантажувального та стрес-тестування перед впровадженням нової версії системи, що унеможливило виявлення критичних помилок у логіці транзакцій. Внаслідок цього, під час пікових навантажень система генерувала масові некоректні транзакції, які блокували доступ до ключових таблиць у базі даних. на виявлені недоліки були реалізовані кілька стратегічних заходів: регулярне проведення навантажувальних та стрес-тестів у середовищі, максимально наближеному до продуктивного; впровадження автоматизованого тестування транзакційних сценаріїв як невід'ємного етапу CI/CD-процесу; а також обов'язкове проведення колективного перегляду коду (code review) із залученням технічних фахівців з безпеки та архітектури. Завдяки цьому вдається не лише запобігати повторенню подібних інцидентів, а й підвищити загальну якість програмного забезпечення, що обслуговує критично важливі освітні ресурси.

Атаки типу «людина-посередині» на канали реплікації. Такі атаки стають можливими внаслідок відсутності шифрування або недостатнього контролю за автентичністю вузлів реплікації, що дозволяє зловмиснику перехоплювати, модифікувати або підмінювати передавані пакети даних. Найбільш поширеним наслідком такого інциденту є порушення доступності: зіпсовані або неконсистентні дані викликають зупинку реплікаційних процесів, помилки синхронізації, а іноді й повне блокування обслуговування з боку вторинних вузлів. Це може спричинити неузгодженість інформації між копіями бази даних, затримку в обробці запитів та неможливість забезпечити безперервність обслуговування у випадку відмови основного сервера. Впроваджено обов'язкове шифрування трафіку реплікації з використанням протоколу TLS 1.3, що гарантує конфіденційність і цілісність передаваних даних. , реалізовано механізми взаємної аутентифікації вузлів, що дозволяє ідентифікувати лише довірені компоненти системи , для підвищення стійкості реплікації було запроваджено контроль послідовності транзакцій і автоматичне виявлення аномалій у синхронізації.

На рисунку 2.4 зображено Coras – модель , що порушують конфіденційність мережевого каналу передачі даних, відображає типові сценарії атак, потенційні вразливості освітньої інфраструктури та комплекс засобів захисту.

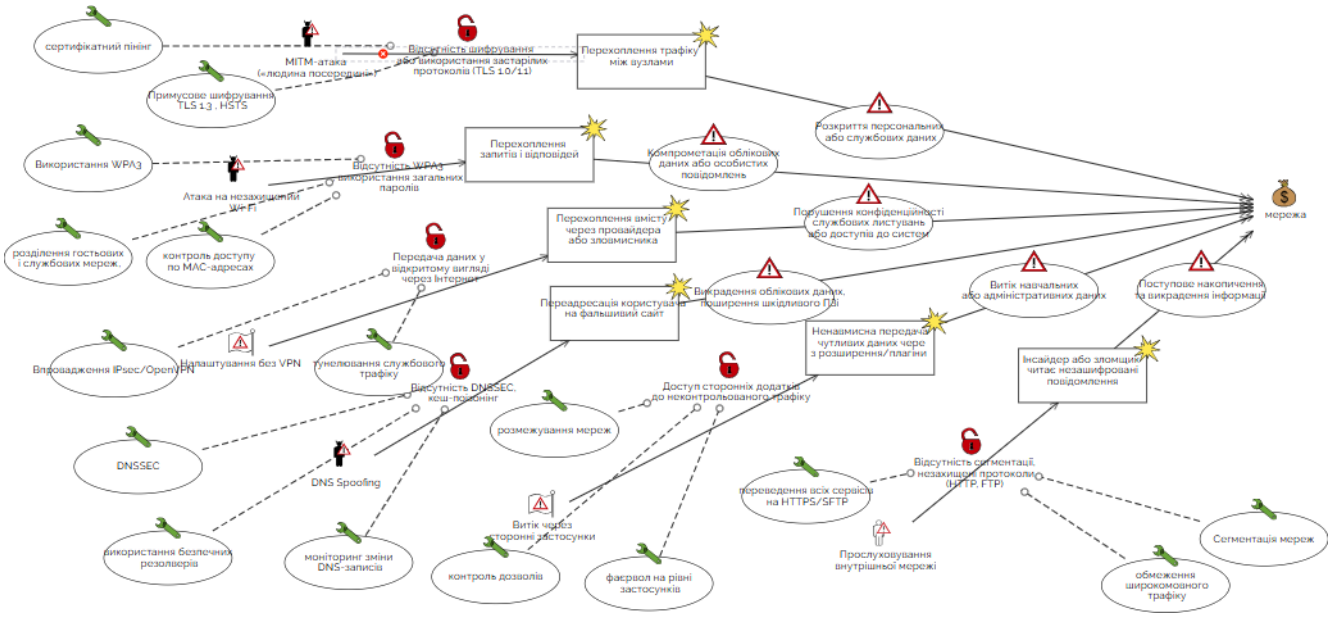


Рисунок 2.4 Coras – модель для мережі , з порушенням конфіденційності

Атака типу «людина посередині» , яка полягає у несанкціонованому перехопленні трафіку між клієнтом і сервером з метою прослуховування, модифікації або підміни переданої інформації. Основною передумовою успішної атаки є технічна вразливість на стороні клієнта або сервера — зокрема, відсутність належного шифрування каналу зв’язку або використання застарілих криптографічних протоколів, таких як TLS 1.0/1.1, які мають відомі уразливості й більше не відповідають сучасним вимогам захисту конфіденційності. Внаслідок MITM-атаки зловмисник отримує змогу повністю контролювати потік переданих даних: перехоплювати логіни й токени автентифікації, переглядати внутрішні листування, модифікувати запити, або ж імітувати інші вузли мережі. Контрзаходом в даному випадку стало: примусове використання сучасного протоколу TLS 1.3, який забезпечує покращену криптографію, зменшення

латентності й захист від широкого спектру атак, також варто впроваджувати політику HSTS , яка забороняє використання незахищеного HTTP-з'єднання навіть у разі втручання посередника. Застосування сертифікатного пінінгу (certificate pinning), що унеможливлює підміну сертифікатів навіть при наявності компрометованих центрів сертифікації. У сукупності ці заходи значно підвищують стійкість мережі до атак MITM і гарантують безпечну взаємодію між компонентами системи в умовах відкритого або частково контрольованого середовища.

Проаналізовано загрозу, пов'язану з використанням незахищених бездротових мереж Wi-Fi. Однією з ключових вразливостей виявилася відсутність сучасного протоколу шифрування WPA3 або використання єдиного (загального) пароля для доступу, що властиво багатьом навчальним закладам із публічним або напіввідкритим доступом до мережі. Таке недбале налаштування сприяє перехопленню трафіку зловмисником, який перебуває в радіусі дії точки доступу. Можлива атака реалізується через прослуховування запитів і відповідей між користувачем та мережевими сервісами, що дозволяє ідентифікувати облікові дані, куки, токени авторизації, а також вміст приватної комунікації, наприклад повідомлення чи навчальні документи. Компрометація цих даних порушує конфіденційність, а у випадку доступу до внутрішніх систем — несе ризик подальшого поширення атаки. Для усунення вказаних ризиків було впроваджено кілька технічних заходів. Реалізовано підтримку WPA3 як сучасного стандарту захисту Wi-Fi-з'єднань , розділено гостьовий та службовий трафік шляхом налаштування ізольованих віртуальних мереж (VLAN), що унеможливлює перехресний доступ між сегментами. Впроваджено механізм фільтрації пристроїв за MAC-адресами, що дозволяє жорсткіше контролювати доступ лише для авторизованих користувачів.

Виявлено відсутність використання VPN-технологій при передачі службової інформації через публічні або неізольовані мережі Інтернет. Така конфігурація означає, що дані можуть передаватися у відкритому вигляді або з недостатнім

рівнем шифрування, що створює умови для перехоплення переданої інформації на будь-якому проміжному вузлі маршруту — зокрема, на рівні інтернет-провайдера або за наявності активного зловмисника, який здійснює атаки типу «man-in-the-middle». Загроза полягає в тому, що через відсутність VPN-тунелювання можуть бути скомпрометовані службові повідомлення, облікові дані, а також запити до внутрішніх інформаційних систем, що у свою чергу порушує принцип конфіденційності та може надати зловмиснику можливість подальшого вторгнення до інфраструктури або здійснення фішингових атак із використанням викраденої інформації. З метою усунення цієї вразливості впроваджено механізми шифрування мережевого трафіку через IPsec або OpenVPN, що забезпечують безпечне тунелювання між кінцевими точками обміну даними , весь службовий трафік було ізольовано через окремі захищені канали, що гарантує автентичність, цілісність і конфіденційність переданої інформації навіть у разі використання відкритих або ненадійних мережевих середовищ.

Одним із поширених векторів атаки є DNS spoofing, при якому користувача навмисно перенаправляють на фальшивий вебсайт замість очікуваного ресурсу. Основною причиною цього є відсутність механізмів перевірки автентичності DNS-відповідей, зокрема DNSSEC, що дозволяє зловмиснику здійснити кеш-поізонінг (cache poisoning). У результаті користувач вводить свої облікові дані або взаємодіє з сайтом, який може завантажити шкідливе програмне забезпечення. Для протидії таким загрозам рекомендовано використовувати DNSSEC, який забезпечує криптографічну верифікацію записів, застосовувати безпечні DNS-резолвери та впровадити моніторинг змін у DNS-записах. Ще одним каналом витоку є сторонні застосунки, зокрема браузерні розширення, плагіни чи мобільні додатки, які мають доступ до трафіку або інформації користувача. За відсутності ефективного контролю дозволів ці застосунки можуть неусвідомлено передавати конфіденційні освітні або адміністративні дані третім сторонам. Це є особливо критичним у випадку роботи в одній мережі з освітніми сервісами або доступу до облікових записів. Запобігти подібним витокам допомагає розмежування мережевих зон

(наприклад, між студентським Wi-Fi і адміністративною мережею), фаєрволи на рівні застосунків та ретельний контроль дозволів для стороннього програмного забезпечення.

Ризик прослуховування внутрішньої мережі — ситуації, коли інсайдер або зломщик має змогу зчитувати незашифровану інформацію, що циркулює в межах інфраструктури. Основними передумовами для цього є відсутність сегментації мережі, використання небезпечних протоколів на кшталт HTTP або FTP, а також необмежений широкомовний трафік, який дозволяє захоплювати пакети з інших хостів. Такі дії можуть залишатися непоміченими протягом тривалого часу, призводячи до накопичення і подальшого викрадення чутливої інформації. Щоб протидіяти таким ризикам, доцільно впровадити мережеву сегментацію з виділенням окремих VLAN для критичних систем, обмежити широкомовлення, а також забезпечити обов'язкове використання захищених протоколів (HTTPS, SFTP) для всіх служб, що передають дані.

На рисунку 2.5 зображено ключові ризики, що загрожують цілісності даних у процесі їх передавання мережею, а також окреслює доцільні технічні й організаційні заходи для їх нейтралізації.

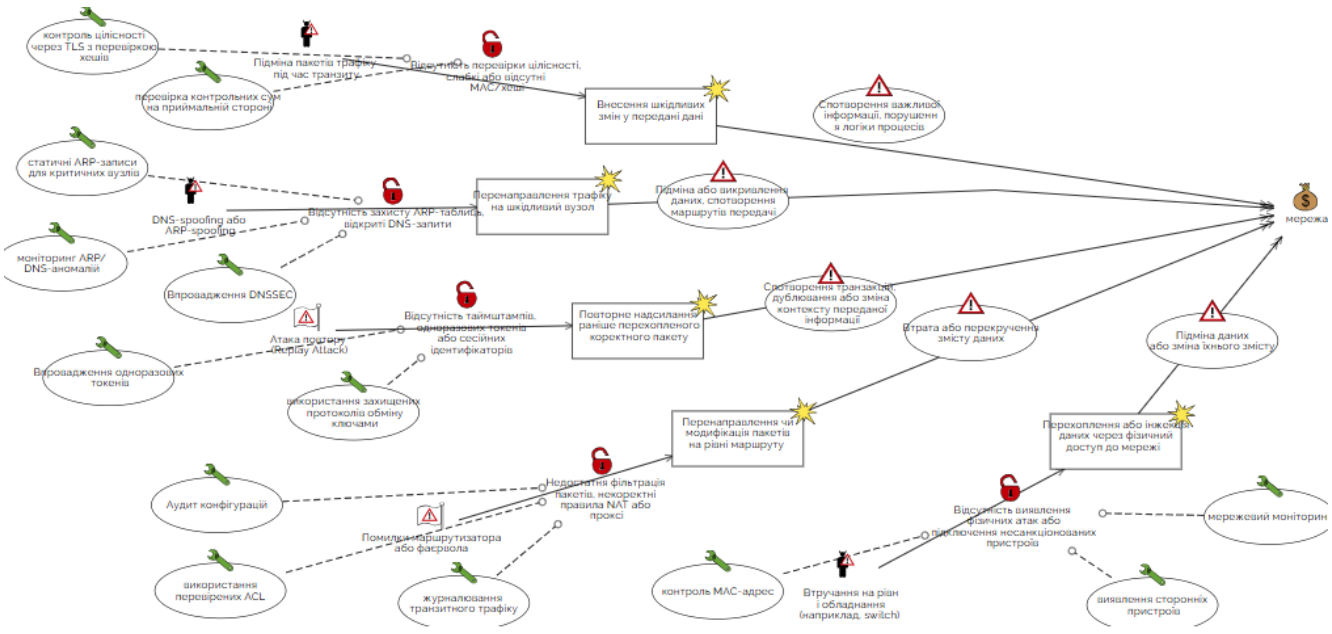


Рисунок 2.5 – Coras – модель для мережі із порушенням цілісності

Підміна пакетів трафіку під час транзиту стала можливою через недбале налаштування мережевих каналів і відсутність надійних механізмів перевірки цілісності даних на рівні протоколів передачі. Зокрема, у початкових конфігураціях не було передбачено використання MAC-кодів або криптографічних хеш-функцій для кожного пакету, що відкривало зловмисникам вікно для модифікації вмісту переданих повідомлень без спрацьовування жодних засобів контролю. Як наслідок, у ході реальної експлуатації мережі було зафіксовано випадки, коли змінені зловмисником пакети призводили до спотворення ключових даних, що в свою чергу порушувало логіку обробки освітніх сервісів та могло стати причиною некоректних рішень на рівні академії. Щоби виключити можливість подібних атак у майбутньому, у систему було інтегровано обов'язкове шифрування транспортного каналу з використанням протоколу TLS (версії 1.3), у якому на кожному етапі передавання даних відбувається обчислення та верифікація криптографічного хеш-коду. Одночасно на приймальній стороні реалізовано додатковий контроль контрольних сум, що дозволяє виявляти будь-які несанкціоновані зміни навіть у разі компрометації окремих сегментів мережі.

Модель загроз пов'язана з підміною ARP- або DNS-запитів, що реалізується через вразливість механізму адресної прив'язки в мережі й відсутність криптографічної верифікації отриманих відповідей. Зокрема, у разі незахищених ARP-запитів зловмисник може підмінити MAC-адресу шлюзу у кеші жертви, що дозволяє йому перехоплювати весь трафік між клієнтом та реальним маршрутизатором, а далі або ретрансмісувати його з незначними затримками, або модифікувати на ходу. Аналогічно зловмисник, який використовує DNS-spoofing, відповідає на DNS-запити клієнта підробленими A-записами, спрямовуючи користувача на шкідливі сервери. В результаті можуть бути викрадені облікові дані, виконана фішингова атака під виглядом авторизації на легітимному ресурсі або ін'єкція шкідливого коду в HTTP-відповіді. Для зменшення ймовірності успішної підміни DNSSEC із ланцюговою верифікацією підписів, а також застосовують статичне призначення ARP-записів на критичних хостах; додатково

встановлюють системи виявлення аномалій у ARP- і DNS-трафіку, які аналізують нетипові шаблони запит–відповідь і миттєво повідомляють про спроби «ARP flooding» або множинних DNS-запитів до непов’язаних доменів.

Модель, відома як Replay Attack, ґрунтується на слабкому управлінні сесійними ідентифікаторами та відсутності механізмів одноразової автентифікації. У цьому випадку зловмисник перехоплює раніше законно переданий пакет, що містить, наприклад, фінансову транзакцію або команду до сервера, і повторює його через деякий інтервал часу. Оскільки система не перевіряє тимчасову мітку чи унікальність токена, вона може обробити транзакцію двічі або дозволити доступ до ресурсів за вже відміченими сесіями. Така атака особливо небезпечна в середовищах із критичними фінансовими операціями або дистанційним управлінням устаткуванням. Як контрзаходи інтегрують криптографічні механізми одноразових токенів (OTP), обмін timestamp-метаданими в рамках протоколу TLS 1.3 та впровадження HMAC-підписів із зворотною міткою часу, що створює невід’ємний зв’язок між даними та моментом їх створення.

Помилка у конфігурації мережевих пристроїв, зокрема маршрутизаторів і корпоративних файрволів. Недотримання принципів мінімальних привілеїв у налаштуваннях ACL, надто відкриті правила NAT або неправильно сконфігуровані проксі-сервери відкривають канал для несанкціонованого перенаправлення або модифікації пакетів. Відсутність сегментації мережі дозволяє шкідливому трафіку вільно рухатися від периферії до внутрішніх серверів, що знижує рівень ізоляції критичних зон. Наслідком може стати витік чутливих даних, порушення цілісності систем управління або розгортання нерегламентованих мережевих служб. Усунути такі вразливості допомагає регулярний аудит конфігурацій із використанням автоматизованих сканерів, впровадження централізованих політик безпеки на основі інфраструктури SDN та постійний аналіз журналів подій у рамках SIEM для виявлення невідповідностей і нелінійних маршрутів трафіку.

Остання модель розкриває загрози на фізичному рівні мережі, коли зловмисник отримує фізичний доступ до апаратного комутатора або

неконтрольованого порту. За відсутності механізмів автентифікації та фільтрації MAC-адрес неавторизовані пристрої підключаються до мережі, що спричиняє можливість інжекції або перехоплення сегментованого трафіку. Окрім порушення цілісності , це може призвести до атак «Man-in-the-Middle», впровадження бекдорів на рівні мережевих карт та створення мостів між ізольованими сегментами. В якості превентивних заходів використовують Port Security із обмеженням числа різних MAC-адрес на порту, системи контролю доступу до мережі (NAC) з централізованим управлінням політиками та безперервний фізичний моніторинг обладнання з допомогою детекторів несанкціонованих підключень і систем віддаленої інвентаризації.

На рисунку 2.6 Coras – модель ілюструє ключові загрози доступності мережевої інфраструктури академії — від DDoS-атак та помилок конфігурації до фізичних збоїв і маніпуляцій маршрутизацією.

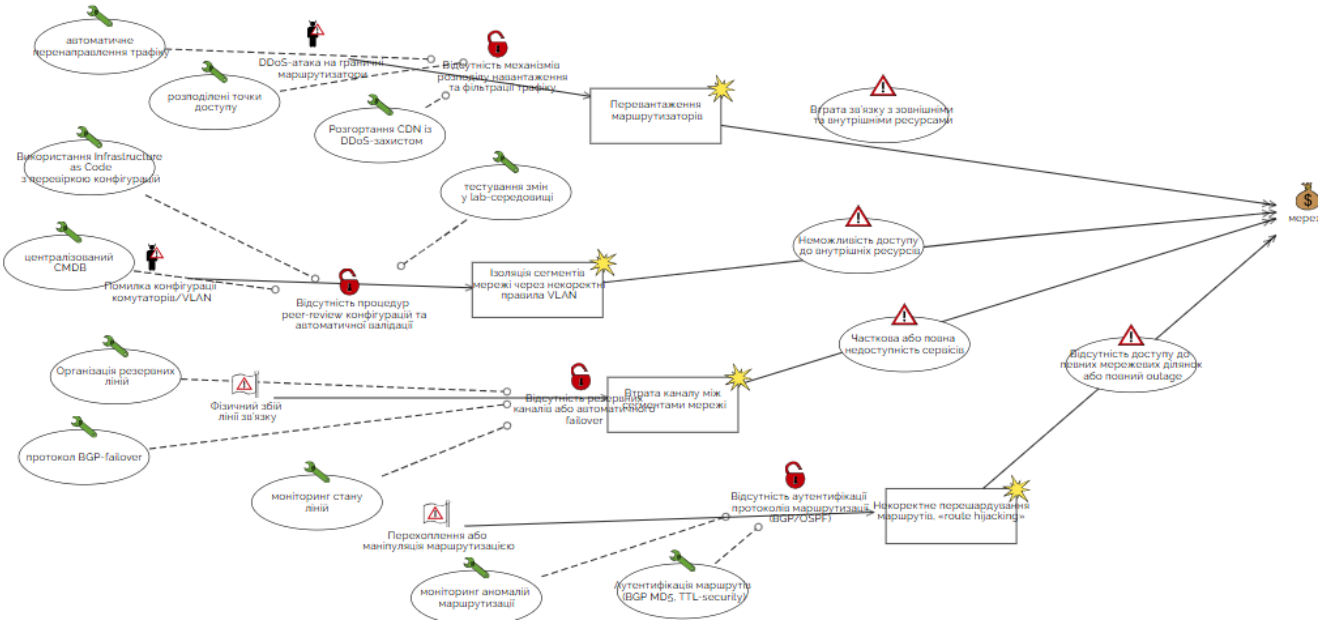


Рисунок 2.6 Coras – модель для мережі із порушенням доступності

Загроза масованої DDoS-атаки, спрямованої на граничні маршрутизатори закладу. Відсутність систем балансування навантаження та фільтрації шкідливого

трафіку дозволяла зловмисникам формувати високий обсяг одночасних запитів, що вичерпували доступні ресурси пристроїв обробки пакетів та призводили до колапсу мережевих маршрутів. Унаслідок такого перевантаження відбувалася втрата зв'язку з ключовими зовнішніми сервісами (онлайн-ресурсами, репозитаріями наукого контенту) та внутрішніми системами (авторизація, дистанційне навчання, електронні журнал і бібліотека), що могло спричинити значний зрив академічного процесу. Для мінімізації цих ризиків було реалізовано комплексний набір протидій: на першому рівні організовано розгортання контент-дистрибуційної мережі (CDN) із вбудованими DDoS-модулями, які автоматично виявляють аномальні обсяги запитів і виконують їх дроселювання ще на етапі вхідного трафіку. Додатково побудовано географічно розподілені точки доступу, які забезпечують рівномірне розподілення навантаження та надлишковість каналів. Впроваджено політику автоматичного rerouting-у, що перенаправляє легітимні запити до резервних вузлів у разі відмови основних маршрутизаторів.

Неналежне управління конфігураціями комутаторів та VLAN-сегментів створює значні ризики для доступності та цілісності внутрішніх ресурсів. Відсутність формалізованих процедур peer-review перед внесенням змін у мережеві правила призвела до того, що одна з останніх конфігурацій сепгментації помилково ізолювала критичні серверні вузли від решти корпоративної мережі. Цей інцидент, спровокований некоректно визначеними правилами VLAN, спричинив неможливість доступу до систем автентифікації, навчальних платформ і внутрішніх баз даних, що фактично паралізувало адміністративні та освітні сервіси на декілька годин. З метою усунення виявленої вразливості та попередження її повторення у майбутньому було реалізовано підхід «Infrastructure as Code», який передбачає опис мережевих налаштувань у вигляді скриптів та конфігураційних файлів із подальшим застосуванням автоматизованих засобів перевірки синтаксису та логіки сегментації до розгортання змін у продуктивному середовищі. Створення централізованої системи управління конфігурацією (CMDB) дозволило підтримувати єдиний авторитетний джерело правдивих даних про топологію

мережі, поточні політики доступу та зв’язки між пристроями. Крім того, всі оновлення обов’язково тестуються в ідентичному lab-середовищі, що моделює продуктивну топологію, з метою виявлення потенційних конфліктів та непрогнозованих наслідків перед фактичним застосуванням. Результатом впровадження цих заходів стало суттєве зниження ризику людської помилки при конфігурації мережі та підвищення операційної стійкості всієї IT-інфраструктури. Тепер будь-яка зміна VLAN-політик проходить через автоматизовані перевірки та процедури затвердження, що дозволяє оперативно виявляти й виправляти невідповідності в налаштуваннях, не перериваючи роботи освітніх та адміністративних систем.

Проаналізований інцидент із фізичним збоєм лінії зв’язку виявив, що у разі механічного пошкодження оптоволоконного кабелю чи відмови обладнання на магістральному каналі мережа не мала альтернативного маршруту для передачі даних. Відтак користувачі зіткнулися із непрацездатністю систем реєстрації, втратою доступу до хмарних сховищ та зупинкою онлайн-занять. Цей випадок підкреслив необхідність не лише наявності резервних каналів, але й відпрацювання процесу автоматичного переключення в реальному часі. У відповідь на ідентифіковані ризики було реалізовано кілька додаткових кроків. По-перше, створено фізично незалежні магістральні маршрути, що пролягають різними трасами, для мінімізації ймовірності одночасної відмови. Нлаштовано протокол BGP-failover налаштовано з урахуванням критеріїв якості ліній — затримок та втрат пакетів — що дозволяє обирати найнадійніший маршрут динамічно. Для перевірки готовності системи було організовано регулярні тренувальні переключення (failover drills), під час яких відпрацьовуються алгоритми аварійного відновлення та взаємодія між мережевою та технічною службами. Крім того, система моніторингу стану ліній була доповнена шкалами критичності сигналів та автоматичним оповіщенням відповідальних інженерів із детальною інформацією про характер відмови.

Підміна маршрутів (route hijacking), що можлива через відсутність надійної

аутентифікації протоколів маршрутизації BGP та OSPF. У такій конфігурації зловмисник здатен підміняти маршрутні оголошення, спрямовуючи трафік через неавторизовані вузли або цілком блокуючи доступ до окремих сегментів мережі, що в результаті призводить до простоїв критичних освітніх сервісів. Щоби нейтралізувати цю загрозу, у мережу було інтегровано механізми криптографічної аутентифікації маршрутів — MD5-підписи для BGP і TTL-security для OSPF — які гарантують цілісність та легітимність маршрутних оновлень. Паралельно запроваджено Resource Public Key Infrastructure (RPKI) для автоматизованої верифікації IP-префіксів за допомогою цифрових сертифікатів, а також організовано безперервний моніторинг і кореляцію подій маршрутизації з фіксацією всіх змін в аудит-трейлах. Формалізація політики змін маршрутів та регулярні тренінги для мережевих інженерів доповнили технічні заходи, забезпечивши не лише високий рівень протидії «route hijacking», а й здатність оперативно реагувати на інциденти та підтримувати безперервність освітніх сервісів.

На рисунку 2.7 продемонстровано CORAS-модель загроз конфіденційності для робочих місць, з яких здійснюється доступ до бази даних

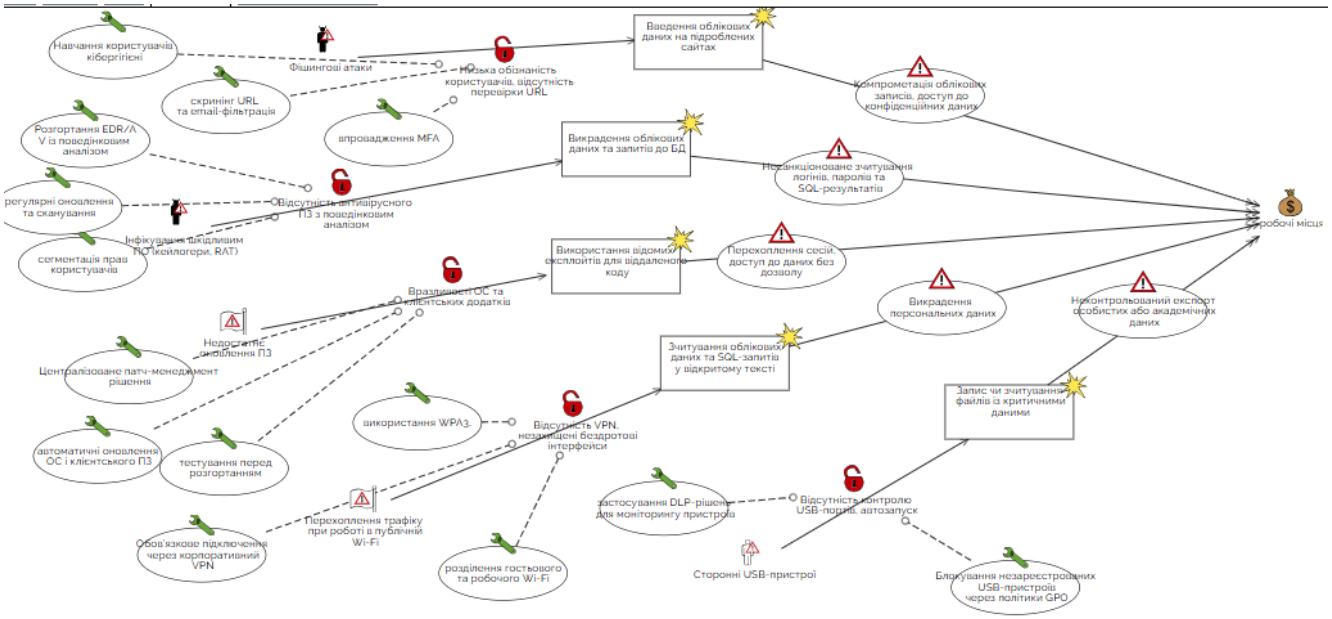


Рисунок 2.7 – Coras – модель робочих місць із порушенням конфіденційності

Фішингові атаки продовжують залишатися одним із найефективніших інструментів соціальної інженерії, спрямованих на викрадення облікових даних співробітників навчального закладу. Недостатній рівень обізнаності користувачів у питаннях кібергігієни та відсутність чітких процедур перевірки URL-посилань створюють сприятливі умови для розповсюдження підроблених електронних листів і лінків на ресурси, які імітують офіційні портали академії. У результаті введення облікових даних на таких фальшивих сторінках відбувається їхня компрометація, що відкриває зловмиснику негайний доступ до конфіденційної інформації — від навчальних даних курсантів до персональних профілів викладачів. У низці зареєстрованих інцидентів було встановлено, що фішингові листи маскувалися під сповіщення адміністрації про оновлення програмного забезпечення або перевірку безпеки, містили шкідливі вкладення та редиректи на підроблені сторінки автентифікації. Унаслідок цього не лише відбувався несанкціонований вхід у систему, але й запускалися скрипти, які відправляли скомпрометовані облікові дані на сервери зловмисників, що призводило до подальшого поширення атаки на інші акаунти. Щоби мінімізувати ймовірність успішної реалізації таких атак, було впроваджено комплекс превентивних заходів. Передусім, організовано регулярні навчальні сесії для всього персоналу, під час яких відпрацьовуються навички розпізнавання фішингових повідомлень, перевірки справжності відправника та оцінки безпечності посилань. Другою лінією захисту стала багатофакторна автентифікація (MFA), яка робить неможливим доступ до облікового запису навіть у разі компрометації пароля. На рівні корпоративної пошти й мережевого шлюзу запроваджено скринінг URL-адрес та фільтрацію електронних листів за допомогою системи DLP (Data Loss Prevention) та спеціалізованого антифішингового рішення, що автоматично блокує відомі шкідливі ресурси та попереджає користувача про потенційні ризики. У сукупності ці заходи формують багатошарову систему захисту кінцевих робочих місць і значно підвищують стійкість інформаційної системи до соціально-інженерних атак.

Інфікування робочих місць шкідливим програмним забезпеченням, таким як кейлогери або віддалені інструменти адміністрування (RAT), є однією з найнебезпечніших загроз для конфіденційності інформації в інформаційній інфраструктурі навчального закладу. Основною передумовою для успішної реалізації такої атаки часто стає відсутність сучасного антивірусного програмного забезпечення з підтримкою поведінкового аналізу, що дозволяє виявляти нові, ще не класифіковані загрози. Внаслідок цього шкідливе ПЗ може залишатися активним протягом тривалого часу, непомітно реєструючи натискання клавіш, вміст буфера обміну, дані аутентифікації та SQL-запити, які користувачі вводять у застосунках або в терміналі. Результатом такого зараження є систематичне викрадення облікових даних, конфіденційної службової інформації, а також результатів взаємодії з базою даних, включно з персональними або навчальними даними курсантів і викладачів. Це створює ризик несанкціонованого доступу до внутрішніх ресурсів, зокрема — до академічних систем управління, що потенційно загрожує цілісності та достовірності освітнього процесу. Для протидії цій загрозі було впроваджено рішення класу EDR (Endpoint Detection and Response) з можливістю поведінкового аналізу активності процесів, що забезпечує виявлення нетипових дій у реальному часі. Проведена жорстка сегментація прав користувачів на рівні операційної системи, що унеможливлює запуск потенційно шкідливих процесів із базових облікових записів. Доповненням стали регулярні оновлення антивірусних сигнатур, періодичне сканування систем на наявність шкідливих компонентів і впровадження політик мінімального доступу. Сукупність цих заходів дозволяє істотно знизити ризик компрометації конфіденційних даних через інфікування робочих станцій.

Доступ до академічних ресурсів через публічні або незахищені Wi-Fi мережі становить суттєву загрозу конфіденційності, оскільки в умовах відсутності захищеного каналу VPN та належного шифрування зловмисник може не лише пасивно перехоплювати трафік, але й здійснювати «людину-посередині» для активної модифікації або підміни даних. У такому випадку будь-які передані

облікові дані, токени аутентифікації та структури SQL-запитів опиняються у відкритому вигляді, що спричиняє ризик компрометації облікових записів і втрата контролю над базою даних. З огляду на це, для захисту від несанкціонованого доступу та витоку інформації було запроваджено обов’язкове тунелювання всього службового трафіку через корпоративний VPN із суворим застосуванням сучасних криптографічних алгоритмів. Паралельно для бездротових сегментів впроваджено стандарт WPA3, що забезпечує надійний протокол аутентифікації та шифрування, а також мережу розділено на окремі гостьову й робочу частини, до якої мають доступ лише авторизовані пристрої за фільтрацією MAC-адрес. Такий комплексний підхід створює багаторівневий захист, який істотно ускладнює проведення MITM-атак і гарантує збереження конфіденційності даних навіть за використання сторонніх бездротових мереж..

Робота з інформаційними ресурсами освітньої установи через публічні або незахищені Wi-Fi-мережі створює серйозну загрозу для конфіденційності переданих даних. У разі відсутності VPN-з’єднання або належного захисту бездротових інтерфейсів, зловмисник може легко здійснити пасивне прослуховування трафіку (sniffing), а також активно втрутитися в передані дані шляхом атак типу "людина посередині" (MITM). У подібних умовах SQL-запити, облікові дані, токени автентифікації або персональні дані можуть бути перехоплені у відкритому вигляді, що призводить до порушення конфіденційності. Особливо небезпечно це для працівників і користувачів, які працюють з академічною базою даних поза межами захищеної внутрішньої мережі — наприклад, під час дистанційного доступу до систем управління навчанням або адміністративних інтерфейсів. Такі витоки можуть спричинити як компрометацію внутрішніх акаунтів, так і втрату довіри до інформаційної інфраструктури навчального закладу. З метою нейтралізації цієї загрози було впроваджено політику обов’язкового підключення до внутрішніх ресурсів винятково через корпоративний VPN із шифруванням каналу. Також реалізовано вимогу використання стандарту WPA3 для захисту бездротових мереж, що забезпечує

стійкий до атак протокол аутентифікації та шифрування. Крім того, усі бездротові мережі було сегментовано на гостьову й робочу, де остання доступна лише авторизованим пристроям за MAC-фільтрами, що дозволяє ізолювати службовий трафік від потенційно небезпечного середовища.

Використання сторонніх USB-пристроїв на робочих місцях користувачів становить серйозну загрозу для конфіденційності даних, особливо у випадках, коли порти не захищені належними політиками контролю. У разі відсутності обмежень або моніторингу USB-інтерфейсів можлива як несанкціонована передача конфіденційної інформації на зовнішні носії, так і зчитування критичних даних з внутрішніх систем. Автозапуск програмного забезпечення з підключених пристроїв також створює ризик інфікування системи шкідливим ПЗ, що може призвести до витоку або підміни навчальних і персональних даних. Для запобігання подібним інцидентам впроваджено низку технічних заходів. По-перше, реалізовано політику блокування незареєстрованих USB-пристроїв через групові політики (GPO), що дозволяє авторизувати лише дозволене периферійне обладнання. По-друге, розгорнуто системи Data Loss Prevention (DLP), які забезпечують моніторинг і контроль усіх спроб зчитування або копіювання файлів з критичних директорій. Це дозволяє оперативно виявляти потенційні спроби ексфільтрації даних та реагувати відповідно до внутрішніх політик безпеки.

На рисунку 2.8 продемонстровано CORAS-модель загроз цілісності для робочих місць, з яких здійснюється доступ до бази даних

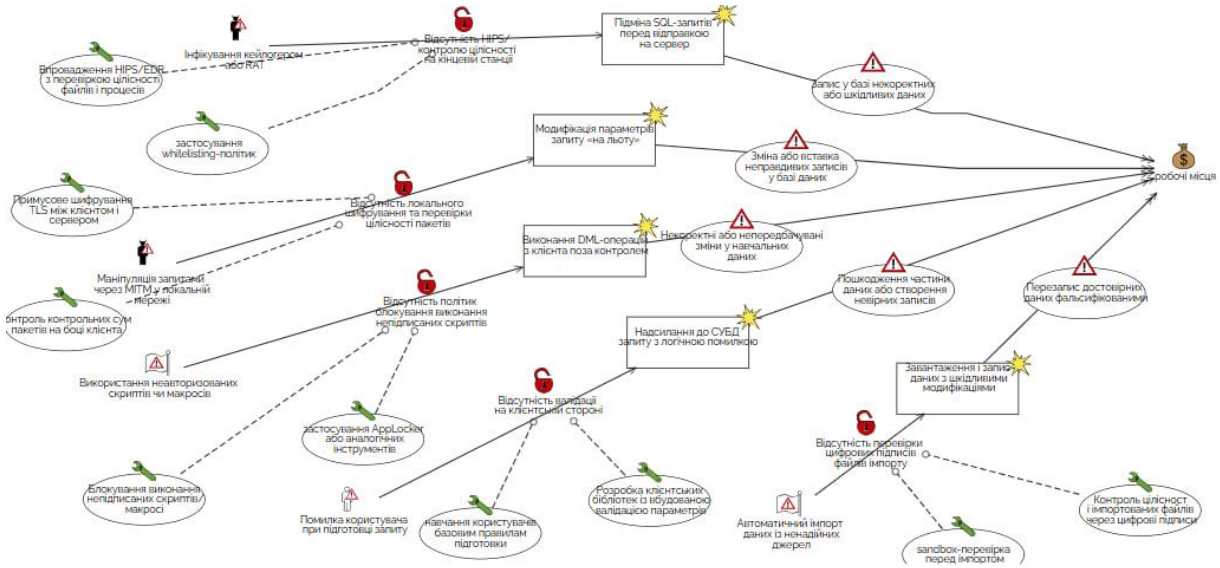


Рисунок 2.8 – Coras – модель робочих місць із порушенням цілісності

Однією з найнебезпечніших загроз для цілісності даних на робочих місцях користувачів є прихована інсталяція кейлогерів або інструментів віддаленого адміністрування . Відсутність на кінцевих станціях систем контролю цілісності і розгорнутих EDR-рішень створює сприятливі умови для непомітного розгортання таких компонентів, які здатні перехоплювати натискання клавіш та змінювати вхідні SQL-запити без відома користувача. Як наслідок, до сервера надходять модифіковані команди, що призводить до запису некоректних або навіть шкідливих даних у базі. Для подолання цього ризику було інтегровано рішення класу EDR із поведінковим аналізом процесів і контролем цілісності файлів на робочих станціях. Крім того, впроваджено політики whitelisting-додатків, які дозволяють виконувати лише заздалегідь затверджений набір процесів, та сувору сегментацію прав користувачів, що унеможливлює роботу підозрілих служб із привілеями введення даних до БД.

У локальних мережах навчального закладу відсутність локального шифрування каналу між клієнтом і СУБД відкриває шлях для атак “людина-посередині”. Зловмисник, перебуваючи в тому ж мережевому сегменті, може перехопити пакети, модифікувати параметри SQL-запитів або вставити додаткові команди, що призводить до спотворення даних на рівні СУБД. Небажані зміни

можуть залишитися непоміченими до моменту виконання запиту, порушуючи цілісність навчальних записів. Щоби запобігти цим сценаріям, було запроваджено примусове шифрування трафіку між клієнтом та сервером баз даних із використанням протоколу TLS 1.3, що містить вбудовані механізми перевірки хеш-суми кожного блоку даних. Додатково на клієнтській стороні реалізовано контроль контрольних сум пакетів, який унеможливлює проходження модифікованих повідомлень до прикладного рівня

Користувачі часто створюють або завантажують скрипти й макроси для автоматизації рутинних завдань у клієнтських застосунках. У разі відсутності політик блокування виконання непідписаних або невідомих скриптів це відкриває можливість запуску DML-операцій із несанкціонованих джерел. Розміщені в макросі SQL-запити можуть вносити зміни до цінних навчальних даних без проходження стандартних каналів перевірки. Для нейтралізації цієї уразливості застосовано механізми AppLocker (або їх аналоги), які блокують виконання всіх непідписаних скриптів і макросів. Крім того, уведено вимогу цифрового підписання будь-яких клієнтських сценаріїв і забезпечено централізоване розповсюдження лише перевірених бібліотек, що значно знижує ризик несанкціонованих DML-ін’єкцій.

Навіть легітимні користувачі можуть випадково скласти SQL-запит із логічними помилками, наприклад неправильне обчислення умов WHERE або некоректне поєднання JOIN. Відсутність валідації на клієнтській стороні дозволяє таким запитам потрапляти до СУБД, що призводить до неочікуваного пошкодження частини даних або створення невірних записів. Незабаром ці спотворення можуть розповсюдитися в аналітичних звітах і призвести до хибних висновків. Для запобігання подібних інцидентів розроблено клієнтські бібліотеки з вбудованою валідацією параметрів запитів, які перевіряють семантичну коректність і попереджають користувача про потенційні помилки ще до відправлення команди на сервер. Поряд із цим проводяться тренінги для кінцевих користувачів із базових принципів побудови запитів та перевірки їхньої логіки.

У багатьох організаційних процесах освітньої установи передбачено регулярне масове завантаження даних у базу через формати CSV або XML, що суттєво підвищує ефективність обробки великих обсягів інформації. Проте відсутність жорстких процедур перевірки цілісності таких файлів створює реальну загрозу, оскільки зловмисник або помилковий скрипт можуть внести приховані модифікації, які будуть непомітно інтегровані до таблиць БД. У результаті кілька тисяч записів можуть бути замінені некоректними або навіть шкідливими даними, призводячи до руйнування цілісності історичних академічних записів і похибок у подальших звітностях та аналітиці. Щоби запобігти подібним інцидентам, файл імпорту піддається багаторівневій перевірці цілісності. На етапі підготовки кожний файл підписується цифровим сертифікатом відповідної служби безпеки та відразу ж генерується криптографічний хеш, який зберігається в окремому захищеному сховищі разом із записом про автора та час створення. Під час безпосереднього імпорту контрольна сума та цифровий підпис перевіряються автоматизованим модулем, що виключає можливість обробки будь-яких файлів із невідповідним чи підробленим підписом. Крім цього, усі імпортні операції виконуються у відокремленому sandbox-середовищі, яке повністю імітує структуру продуктивної бази, але ізольоване від неї.

На рисунку 2.9 продемонстровано CORAS-модель загроз доступності для робочих місць, з яких здійснюється доступ до бази даних

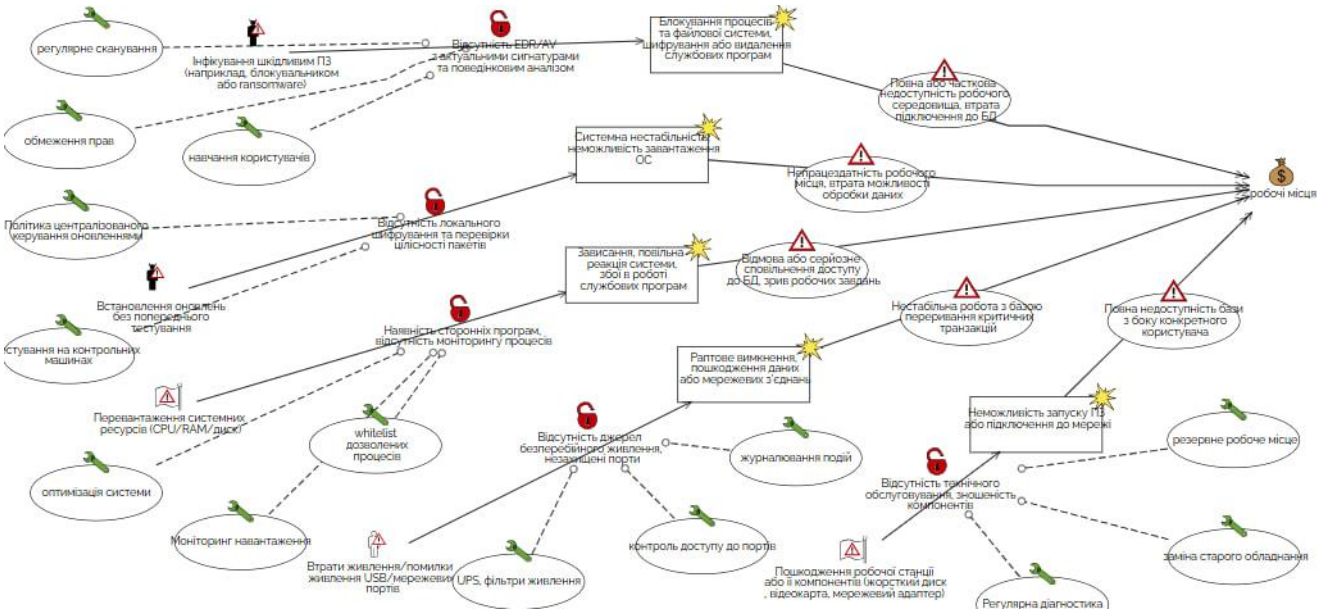


Рисунок 2.9 – Coras – модель робочих місць із порушенням доступності

Сценарій, спричинений інфікуванням робочої станції шкідливим програмним забезпеченням, користувацький комп'ютер виявився вразливим через відсутність сучасних EDR/AV-рішень із поведінковим аналізом. Внаслідок цього на ньому непомітно запустився ransomware-модуль, який заблокував системні сервіси та зашифрував критичні файли, включно з локальними кешами підключення до бази даних. Користувач втратив можливість не лише виконувати робочі задачі, але й підтримувати жодне з'єднання з сервером, що призвело до повного простою на його ділянці освітнього процесу. Для запобігання повторним інцидентам було розгорнуто рішення класу EDR із постійним моніторингом поведінки процесів, а права користувачів скореговано за принципом «найменших привілеїв», що унеможливлює запуск неавторизованих програм.

Другий випадок пов'язаний із невдалим оновленням операційної системи та драйверів: через автоматичне розгортання без попереднього тестування на контрольних машинах новий пакет патчів містив помилку, яка призвела до неможливості завантаження ОС. Результатом стала відсутність робочого середовища на цій станції — користувач не міг ані увійти в систему, ані звернутися до бази, що спричинило затримку в обробці даних та звернень. Щоб уникнути

подібних проблем у майбутньому, було впроваджено централізовану політику патч-менеджменту з обов’язковим тестуванням оновлень у стендовому середовищі перед їхнім розгортанням у продакшені.

Наступний інцидент виник унаслідок непомірного навантаження на ресурси робочої станції — одночасного запуску важких аналітичних процесів, сторонніх застосунків і фонового оновлення, через що центральний процесор і оперативна пам’ять вичерпалися. Це спричинило «зависання» інтерфейсу користувача та неможливість виконати жодної операції з базою даних вчасно, що перервало освітній процес. Для зменшення ймовірності таких збоїв впроваджено систему моніторингу навантаження із механізмами попередження та обмеження кількості одночасно запущених ресурсомістких завдань.

Четвертий випадок демонструє наслідки раптового відключення живлення на робочому місці без наявності джерела безперебійного живлення або апаратної захисту портів. У результаті непередбаченої відсутності електропостачання користувач втратив відкриті сесії та незбережені зміни, а під час екстреного вимкнення могли бути пошкоджені файли, необхідні для коректного підключення до бази даних. Щоби гарантувати безперервність роботи, на кожному робочому столі встановлено UPS із фільтрацією напруги, а доступ до портів та блоків живлення захищено апаратними засобами та програмними політиками.

Фізичне пошкодження ключових компонентів станції — жорсткого диска або мережевого адаптера, що виникло через їхню зношеність і відсутність регламентного обслуговування. Пошкоджений накопичувач унеможливив завантаження ОС, а відмова мережевого контролера повністю відключила користувача від корпоративної мережі та бази даних. Щоби підвищити надійність обладнання, введено графіки планових діагностичних перевірок та заміни критичних елементів апаратної частини, а також запущено програму гарячого резервування робочих місць для оперативного переключення на запасні комп’ютери.

2.3 Оптимальні засоби захисту

У результаті аналізу CORAS-моделей, що охоплюють усі рівні інформаційної інфраструктури НАДПСУ — від серверів баз даних і магістральних каналів мережі до індивідуальних робочих місць користувачів — було визначено, що подолання окремих точкових уразливостей без побудови єдиної архітектури призводить до надмірної складності та підвищує ризик помилок в експлуатації. Зокрема, фрагментарне застосування рішень, кожне з яких захищає лише один або два вектори атак, створює «острови» безпеки, що не здатні ефективно протистояти злагодженим складним загрозам. Саме тому в якості центральних опор обрано три взаємодоповнювані технології, які одночасно охоплюють більшість виявлених ризиків і які, інтегрувавшись один з одним, формують єдину багаторівневу платформу захисту.

Міжмережевий екран нового покоління з інтегрованим модулем веб-аплікаційного фаєрвола [38]. Завдяки глибинній інспекції трафіку на рівні пакетів і прикладних протоколів він здатний одночасно блокувати масштабні DDoS-атаки, перехоплення чи підміну маршрутів, SQL-ін’єкції, а також аномальні HTTP-запити, що можуть сигналізувати про спроби автоматизованих сканувань чи цілеспрямованих атак на веб-інтерфейси. Примусова політика TLS 1.3, реалізована на рівні цього пристрою, забезпечує наскрізне шифрування каналів реплікації баз даних, клієнт-серверної взаємодії та VPN-тунелів з перевіркою цілісності кожного блоку даних. При цьому адміністрування єдиного NGFW/WAF здійснюється через централізовану консоль, що суттєво спрощує впровадження узгоджених політик безпеки й гарантує відсутність «білих плям» у захисті.

Рішення кінцевої точки з поведінковим аналізом (EDR/AV) [39]. На відміну від традиційних антивірусів, які орієнтовані переважно на сигнатури відомих шкідливих програм, сучасні EDR-платформи аналізують у режимі реального часу поведінку процесів та зміни в системних файлах. Це дозволяє виявляти приховані кейлогери, RAT-модулі, програми-шифрувальники та інші загрози, що раніше

могли залишатися непоміченими. У контексті навчального закладу, де інсайдери й зовнішні зловмисники можуть використовувати різноманітні техніки соціальної інженерії, поведінковий аналіз кінцевих точок гарантує оперативну локалізацію інцидентів, їх ізоляцію й кореляцію з подіями автентифікації в LDAP/AD та сигналами SIEM. Таким чином, compromise одного пристрою не дає зловмиснику безконтрольно просуватися далі мережею.

Централізоване управління життєвим циклом програмного забезпечення та конфігурацій на основі принципів Infrastructure as Code. Автоматизовані конвеєри патч-менеджменту дозволяють тестувати нові версії операційних систем, клієнтських додатків, драйверів і мережевих пристроїв у стендових середовищах, що імітують виробничу інфраструктуру, а потім розгортати їх у продакшен з гарантією відтворюваності. Опис конфігурацій у вигляді артефактів коду усуває людський фактор при налаштуванні комутаторів, VLAN, фаєрволів і VPN-шлюзів та запобігає виникненню «островів» застарілих прошивок чи неконсистентних параметрів [40].

Цей підхід не лише закриває відомі вразливості, але й виключає ризики, пов’язані з некоректними оновленнями та конфігураційними помилками, що здатні паралізувати мережеві й прикладні сервіси. Усі три компоненти додатково інтегруються через SOAR-платформу, яка забезпечує автоматизацію реакції на інциденти. Виявлення аномалії — наприклад, надзвичайного навантаження на мережевий інтерфейс, сповіщення SIEM або тривожний сигнал від EDR — запускає уніфікований плейбук, що передбачає ізоляцію вузла, переналаштування маршрутизаторів або негайне розгортання відповідного патча. Поєднання з підходом Zero Trust, у якому кожен запит і кожне з’єднання перевіряються за контекстом, не дозволяє жодному компоненту вважатися довіреним за замовчуванням. Надалі політики доступу враховують роль користувача, стан кінцевого пристрою й поточні умови мережі, що гарантує сувору сегментацію та мінімізацію прав.

2.4 Висновки

У розділі було здійснено прикладну оцінку ризиків для інформаційної інфраструктури Національної академії Державної прикордонної служби України (НАДПСУ) як освітньої установи, що виконує функції критичного значення. Детальний аналіз функціональної структури академії дозволив виявити ключові активи, що обробляють та передають конфіденційну, персональну, службову й навчально-академічну інформацію, зокрема дані про контингенти здобувачів, оцінювання, внутрішні накази, бази даних користувачів, матеріали дистанційного навчання, а також інформацію, що пов’язана з доступом до відомчих мереж. Було підкреслено, що критичність таких активів полягає не лише у високій вартості даних, а й у можливих наслідках їх компрометації, що може вплинути як на освітню, так і на оборонну функцію академії. На основі отриманих характеристик середовища було побудовано низку CORAS-моделей, які дозволили системно представити сценарії порушення конфіденційності, цілісності та доступності інформаційних ресурсів. Моделі охоплювали як класичні технічні загрози (перехоплення трафіку, шкідливе ПЗ, помилки конфігурацій, DDoS-атаки), так і соціотехнічні вектори атак (фішинг, маніпуляція з USB-пристроями, людський фактор), що є особливо актуальними в контексті масового використання клієнтських робочих місць, Wi-Fi-з’єднань та веб-інтерфейсів для роботи з БД. Результати моделювання показали, що більшість ризиків є взаємопов’язаними та можуть мати каскадний вплив на інші компоненти інфраструктури. Зокрема, порушення конфіденційності може бути наслідком проблем із цілісністю файлів, або ж уразливостей, що виникають через втрату доступності до критичних сервісів. Також було проведено аналіз засобів захисту з метою виявлення найбільш ефективних та універсальних механізмів, які можуть бути застосовані в умовах НАДПСУ для нейтралізації або мінімізації виявлених загроз. Було обґрунтовано доцільність переходу від вузько орієнтованих рішень до інтегрованих систем безпеки, таких як міжмережеві екрани нового покоління (Next-Generation Firewall),

централізовані системи управління конфігураціями (CMDB), сегментація мереж із підтримкою VLAN і контроль доступу на рівні користувача (NAC). Окрему увагу приділено засобам, що здатні одночасно протидіяти кільком типам загроз, як-от розгортання EDR/AV із поведінковим аналізом, застосування корпоративного VPN, впровадження DLP-рішень, а також побудова резервної інфраструктури з підтримкою failover.

3 РОЗРОБКА СИСТЕМИ ЗАХИСТУ

3.1 Проектування логічної топології мережі

У процесі виконання була розроблена модель фрагмента інформаційно-комунікаційної інфраструктури Національної академії Державної прикордонної служби України із застосуванням віртуального середовища Cisco Packet Tracer. З огляду на складність, розгалуженість та масштабність реальної мережі академії, у дослідженні зосереджено увагу на одному логічному сегменті, що дає змогу наочно продемонструвати принципи побудови захищеної мережевої архітектури на прикладі окремої ділянки. Інформаційна мережа академії побудована за принципами функціонального сегментування, коли кожна підсистема або категорія користувачів обслуговується в межах власного адресного простору. Зокрема, один із сегментів використовує IP-адресацію в діапазоні 172.16.0.0/16 та обслуговує внутрішню адміністративно-освітню інфраструктуру, тоді як інший сегмент із префіксом 172.20.0.0/16 призначений для спеціалізованих або віддалених об’єктів, що мають обмежене з’єднання з основним центром. У рамках симульованої мережі акцент зроблено саме на моделюванні підмережі 172.16.0.0/16, яка включає базові структурні компоненти системи — центральний маршрутизатор з підключенням до міжмережевого екрана, керований комутатор рівня доступу, низку віртуальних локальних мереж (VLAN 10 – адміністративний персонал, VLAN 20 – навчальні класи, VLAN 30 – обслуговування), серверну інфраструктуру з IP-адресацією в

окремому діапазоні (192.168.100.0/24), а також зовнішнє з'єднання через пристрій Cisco ASA 5505. Саме в цій частині мережі реалізовано логічну топологію, здійснено базову маршрутизацію між VLAN, налаштовано розширені списки контролю доступу (ACL), виконано базові правила NAT, а також впроваджено базову міжмережеву фільтрацію із можливістю подальшого масштабування політик безпеки.

Логічна топологія мережі НАДПСУ задає структуру взаємодії підмереж і пристроїв на рівні IP–маршрутизації та VLAN, що дозволяє чітко розділити мережеві потоки відповідно до функцій академії. У контексті НАДПСУ це означає відокремлення освітніх лабораторій, адміністративних підрозділів та дослідницьких центрів, що забезпечує відповідність держстандартам інформаційної безпеки та захищає внутрішні ресурси. Виділення окремих VLAN для навчальних ПК, серверів інформаційно-бібліотечної системи та гостьового доступу мінімізує ризик несанкціонованого доступу й поширення шкідливого ПЗ між групами користувачів. Для НАДПСУ це критично: внутрішні навчальні матеріали, персональні дані курсантів та службова документація лишаються ізольованими навіть у разі компрометації одного з сегментів. Маршрутизатори в логічній топології реалізують між-VLAN маршрутизацію та політики доступу, необхідні для обміну даними між навчальними корпусами, лабораторіями та центральним сервером. У середовищі НАДПСУ це гарантує швидку й надійну передачу критичної інформації — від результатів тренувань до даних симуляційних систем прикордонного контролю — відповідно до внутрішніх регламентів безпеки.

На рисунку 3.1 подано схему логічної топології мережі НАДПСУ, яка ілюструє структуру взаємоз'єднань між підмережами та пристроями

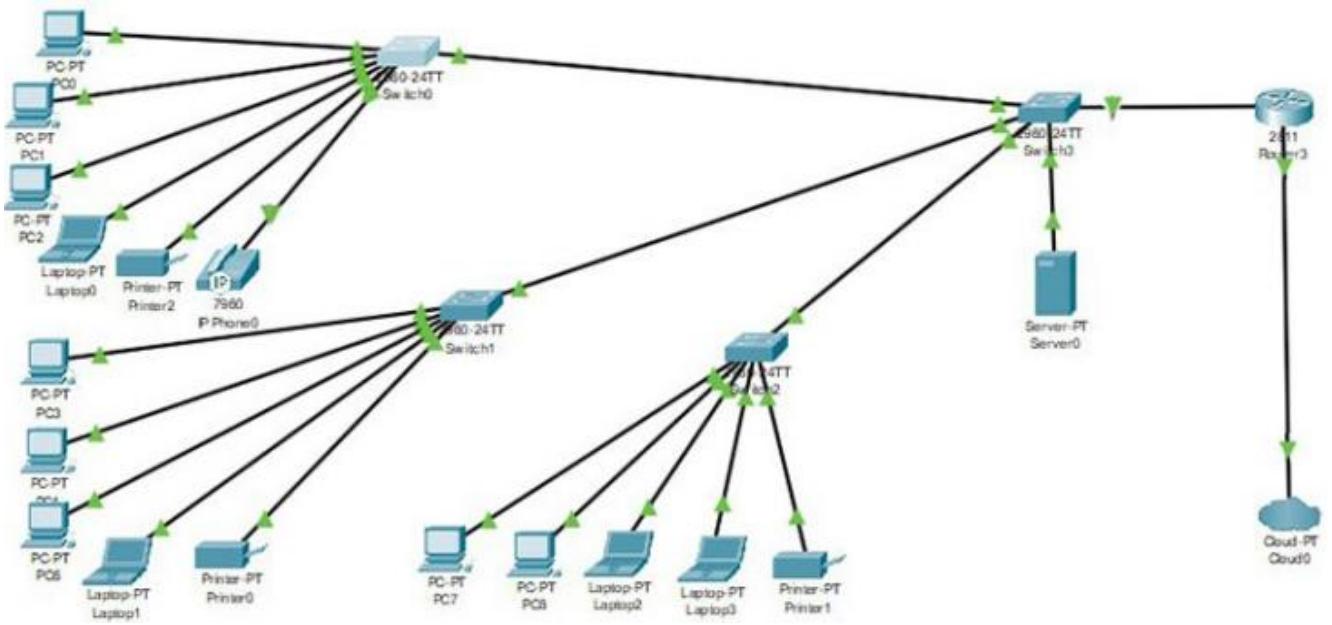


Рисунок 3.1 – Логічна топологія мережі до впровадження засобів захисту

У логічній топології мережі НАДПСУ внутрішня інфраструктура розбивається на три окремі віртуальні локальні мережі (VLAN) із чітким призначенням кожної зони: адміністративна, навчальна та гостьова. До складу топології входять кілька комутаторів доступу (Switch0, Switch1, Switch2), до яких під’єднано типові кінцеві пристрої — персональні комп’ютери, ноутбуки, принтери, а також IP-телефон. Мережа поділена на віртуальні локальні мережі (VLAN), що забезпечують логічне зонування за функціональним призначенням: адміністративні, навчальні та допоміжні підрозділи. Комутатор агрегації (Switch3) забезпечує маршрутизацію між VLAN та передає трафік до маршрутизатора (Router0), через який здійснюється вихід у глобальну мережу (Cloud0).

Серверний вузол (Server0) розміщено в окремому сегменті та підключено безпосередньо до комутатора розподілу, що гарантує централізований доступ до критичних сервісів за умови дотримання визначених політик доступу. Маршрутизація між сегментами здійснюється на рівні 3-го рівня моделі OSI, із застосуванням механізмів фільтрації трафіку та міжмережевих обмежень. Конфігурація моделює безпечне, структуроване та масштабоване інформаційне

середовище, придатне для функціонування у складі критичної інфраструктури освітнього закладу.

3.2 Налаштування систем захисту на пристроях

З метою забезпечення цілісної моделі захисту інформаційного обміну між логічними сегментами мережі, з урахуванням принципів зонування, мінімізації прав доступу та контролю маршрутизації трафіку здійснюється конфігурація мережевих пристроїв з урахуванням вимог до побудови захищеної інформаційної інфраструктури об’єкта критичної інфраструктури. Впровадження базових механізмів безпеки — таких як віртуальні локальні мережі (VLAN), розширені списки контролю доступу (ACL), маршрутизація між сегментами, фільтрація вихідного трафіку на міжмережевому екрані та організація NAT — спрямоване на забезпечення стійкості мережі до несанкціонованих дій, обмеження міжсегментної взаємодії, ізоляцію критичних сервісів та створення контрольованих каналів взаємодії з зовнішнім середовищем

На рисунку 3.2 зображено конфігурацію розширеного списку контролю доступу (ACL), який застосовується до VLAN 10 (адміністрація) з метою надання повного доступу до всіх мережевих ресурсів, забезпечує контрольований і захищений доступ адміністративного сегмента до інших частин мережі.

```
Router(config)#ip access-list extended ADMIN_ACCESS
Router(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#interface gig0/0.10
Router(config-if)#ip access-group ADMIN_ACCESS in
```

Рисунок 3.2 – Список доступу для першої групи

Даний фрагмент конфігурації демонструє реалізацію політики безпеки на рівні маршрутизатора шляхом використання розширеного списку контролю доступу (ACL). Створений ACL з назвою ADMIN_ACCESS гарантує, що всі пристрої адміністративної VLAN (192.168.10.0/24) можуть безперешкодно взаємодіяти з будь-якими іншими сегментами мережі, що необхідно для виконання управлінських, моніторингових та діагностичних функцій без відлагоджень. Прикріплення цього ACL до під інтерфейсу у вхідному напрямку забезпечує, що перевірка прав користувачів виконується безпосередньо при надходженні трафіку від адміністративного сегмента, що мінімізує навантаження на внутрішні ресурси та підвищує ефективність обробки пакетів. Така конфігурація відповідає принципу “найменших привілеїв” для інших VLAN, дозволяючи адміністраторам мережі мати максимальні права, водночас чітко відокремлюючи їхні права від користувацьких або гостьових сегментів.

На рисунку 3.3 наведено фрагмент CLI-конфігурації розширеного списку контролю доступу LAB_ACCESS, призначеного для сегмента VLAN 20. Цей ACL гарантує, що навчальні робочі станції можуть звертатися лише до сервера 192.168.100.10, водночас блокуючи доступ до адміністративної підмережі та зберігаючи можливість виходу в зовнішні мережі.

```
Router(config)#ip access-list extended LAB_ACCESS
Router(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 host 192.168.100.10
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)#permit ip 192.168.20.0 0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#interface gig0/0.20
Router(config-if)#ip access-group LAB_ACCESS in
```

Рисунок 3.3 – Список контролю доступу для другої групи

Розширений список контролю доступу LAB_ACCESS, призначений для ізоляції трафіку сегмента VLAN 20 (навчальні класи). Першою директивою permit ip 192.168.20.0 0.0.0.255 host 192.168.100.10 гарантується, що всі запити навчальних робочих станцій спрямовуються виключно до критичного серверного ресурсу з IP

192.168.100.10, який містить необхідні для освітнього процесу навчальні матеріали та програми. Другою командою deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255 блокується будь-яка спроба доступу до адміністративної VLAN 10, що виключає можливість несанкціонованих внутрішніх переміщень зловмисників і захищає конфіденційні адміністративні ресурси. Нарешті, директива permit ip 192.168.20.0 0.0.0.255 any забезпечує можливість виходу навчальних станцій до інших внутрішніх та зовнішніх сервісів (наприклад, Інтернету), необхідних для навчального процесу, що поєднує суворе дотримання політик безпеки з необхідною функціональною гнучкістю. Після визначення правил ACL прив'язка списку до під інтерфейсу за допомогою команди ip access-group LAB_ACCESS in гарантує, що фільтрація відбувається безпосередньо при вході трафіку в маршрутизатор, мінімізуючи ризики обходу політик та забезпечуючи централізований контроль доступу.

На рисунку 3.4 продемонстровано приклад застосування розширеного списку контролю доступу для сегмента обслуговування (VLAN 30). Цей фрагмент CLI-коду ілюструє, як на рівні маршрутизатора обмежується доступ технічного персоналу до критичних підмереж Академії, одночасно відкриваючи вихід у зовнішні ресурси через міжмережевий екран.

```
Router(config)#ip access-list extended MAINTENANCE_ACCESS
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 host 192.168.100.10
Router(config-ext-nacl)#permit ip 192.168.30.0 0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#interface gig0/0.30
Router(config-if)#ip access-group MAINTENANCE_ACCESS in
```

Рисунок 3.4 – Список контролю доступу для третьої групи

Наведену конфігурацію можна розглядати як ключовий етап імплементації багаторівневої системи захисту інформаційної інфраструктури НАДПСУ. Застосування списку контролю доступу MAINTENANCE_ACCESS до під

інтерфейсу гарантує, що технічний персонал та зовнішні служби отримують лише обмежений набір прав: доступ до внутрішніх адміністративних і навчальних підмереж, а також до серверної зони, суворо заборонений. Це істотно зменшує поверхню атаки й виключає можливість “горизонтальних” переміщень потенційного зловмисника між критичними сегментами мережі. При цьому директива permit ip 192.168.30.0 0.0.0.255 any у поєднанні з політиками NAT на міжмережевому екрані ASA забезпечує технічному персоналу необхідний вихід у зовнішні сервіси (оновлення програмного забезпечення, доступ до віддалених репозиторіїв), зберігаючи при цьому конфіденційність внутрішніх ресурсів. Така побудова відповідає принципу «розділяй і володарюй»: кожен сегмент мережі отримує мінімальний набір прав, достатній для виконання своїх функцій, що підвищує стійкість системи до внутрішніх і зовнішніх загроз. Крім того, реалізація ACL на рівні маршрутизатора гарантує централізовану точку контролю, де відбувається інспекція та фільтрація пакетів ще до передачі їх до інших вузлів мережі. Це знижує навантаження на комутатори й сервісні вузли, а також спрощує адміністрування й аудит безпекових політик.

На рисунку 3.4 показано конфігурацію інтерфейсів VLAN1 (outside) та VLAN2 (inside) на Cisco ASA 5505 із налаштуванням динамічного NAT. Ця схема ілюструє, як внутрішні адреси мережі 192.168.0.0/16 маскуються під IP зовнішнього інтерфейсу ASA для виходу в інтернет.

```
ASA(config)#interface vlan 1
ASA(config-if)#nameif outside
ASA(config-if)#security-level 0
ASA(config-if)#ip address dhcp setroute
ASA(config-if)#no shutdown

ASA(config)#interface vlan 2
ASA(config-if)#nameif inside
ASA(config-if)#security-level 100
ASA(config-if)#ip address 192.168.100.1 255.255.255.0
ASA(config-if)#no shutdown

ASA(config)#object network INSIDE-NET
ASA(config-network-object)#subnet 192.168.0.0 255.255.0.0
ASA(config-network-object)#exit

ASA(config)#nat (inside,outside) dynamic interface
```

Рисунок 3.4 – Налаштування ASA

Налаштування інтерфейсів VLAN1 (outside) і VLAN2 (inside) із різними рівнями довіри створює чітку демаркаційну лінію між публічною та приватною зонами мережі. Завдяки динамічному NAT (PAT), всі внутрішні пристрої користуються єдиною публічною IP-адресою ASA при виході в Інтернет, що значно зменшує поверхню атаки: зовнішні зловмисники бачать лише адресу ASA, а не окремі хости. При цьому використання DHCP для отримання IP-з’єднання з провайдером та опції setroute автоматизує налаштування маршрутів за замовчуванням, забезпечуючи безперебійну доступність зовнішніх ресурсів навіть при зміні параметрів мережі провайдера. Крім того, така конфігурація полегшує адміністрування та масштабування інфраструктури, оскільки додавання нових внутрішніх підмереж або пристроїв не вимагає внесення змін до публічних налаштувань — всі вони успішно потрапляють у NAT-пул ASA. В результаті мережа НАДПСУ отримує високий рівень захищеності зовнішніх з’єднань, підтримуючи при цьому гнучкість і простоту керування.

Впровадження міжмережевого екрана нового покоління (NGFW), інтегрованого з модулем веб-аплікаційного фаєрвола (WAF). Вибір цього компонента був зумовлений необхідністю забезпечення контролю не лише на

мережевому рівні, а й на рівні прикладних протоколів, зокрема HTTP, HTTPS та SQL. В умовах сучасних загроз саме прикладний рівень стає найбільш уразливим, що вимагає застосування розширеної моделі інспекції та фільтрації. На підготовчому етапі було проведено аудит мережевої архітектури з метою визначення оптимальної точки розміщення NGFW. Зважаючи на існуючу конфігурацію, згідно з якою гранична фільтрація здійснюється пристроєм Cisco ASA 5505, було прийнято рішення інтегрувати NGFW між ASA та внутрішньою інфраструктурою академії. Така схема дозволила зберегти логіку існуючих міжмережевих політик, водночас забезпечуючи поглиблену перевірку внутрішнього трафіку перед його доставкою до критичних сервісів. На практичному етапі пристрій NGFW (в рамках моделювання — на базі FortiGate або Cisco Firepower) було переведено у режим transparent firewall, що дозволило обійти потребу в додатковій маршрутизації та забезпечити безперервність сервісів. У цьому режимі міжмережевий екран функціонує як мережевий міст, зберігаючи MAC-адреси й IP-структуру незмінними. Було налаштовано інтерфейси з відповідними зонами безпеки, прив’язаними до логічних сегментів мережі. У подальшому в інтерфейсі керування було створено політики фільтрації HTTPS-трафіку, при цьому NGFW здійснював SSL-термінацію з примусовим використанням протоколу TLS версії 1.3. Паралельно було активовано модуль WAF, який відповідає за захист веб-додатків, зокрема тих, що розміщені у внутрішній серверній зоні за адресами підмережі 192.168.100.0/24. Було застосовано профіль безпеки, побудований на основі правил OWASP Top 10, що включає виявлення SQL-ін’єкцій, XSS-атак, directory traversal та спроб сканування структурних елементів веб-інтерфейсів. В рамках політики фільтрації було також увімкнено моніторинг заголовків HTTP, методів GET/POST та вмісту URI. Трафік, що відповідав визначеним шаблонам ризикованої поведінки, блокувався негайно з паралельною фіксацією подій у журналі аудиту. Для забезпечення надійної ідентифікації потенційних загроз було налаштовано інтеграцію NGFW із внутрішнім сервером автентифікації на базі LDAP, що дозволило асоціювати

трафік із конкретними обліковими записами користувачів. Додатково NGFW було підключено до SIEM-системи для централізованого збору, аналізу та кореляції подій безпеки. Це забезпечило створення єдиного аналітичного простору, де дані з міжмережевого екрана поєднувалися з логами автентифікації, повідомленнями з кінцевих пристроїв та журналами операційної системи серверів. На завершальному етапі відбулася перевірка працездатності конфігурації. Було здійснено серію тестів, які охоплювали моделювання SQL-ін'єкцій, відправлення аномальних HTTPS-запитів, емулювання автоматизованих сканерів, а також перевірку стійкості до зміни TLS-параметрів на клієнтській стороні. Всі подібні спроби були успішно виявлені і заблоковані, про що свідчили відповідні журнали подій NGFW, а також повідомлення в SIEM. Адміністративне керування новим модулем захисту здійснювалося через окрему консоль із багаторівневою системою доступу, що включала як локальні облікові записи, так і механізми зовнішньої авторизації через RADIUS та TACACS+. У результаті впровадження міжмережевого екрана нового покоління з інтегрованим WAF вдалось досягти якісного посилення безпеки прикладного рівня мережі НАДПСУ, забезпечити контроль цілісності HTTPS-комунікацій, уніфікувати механізми захисту веб-додатків та сформувати передумови для централізованого управління безпековими подіями в реальному часі. Такий підхід створив основу для подальшого впровадження адаптивних стратегій кіберзахисту, які можуть масштабуватись відповідно до еволюції загроз і зростання інфраструктури академії.

Впровадження рішення класу EDR, орієнтованого на забезпечення безперервного контролю за активністю кінцевих пристроїв у режимі реального часу. Даний крок був зумовлений тим, що в більшості відомих кіберінцидентів точкою проникнення до внутрішньої мережі є саме робочі станції користувачів, які найчастіше стають жертвами фішингових атак, соціальної інженерії, або несанкціонованого запуску шкідливого коду. Саме тому захист адміністративних, навчальних і сервісних терміналів потребував комплексного рішення, здатного не лише виявляти загрози, а й запобігати їх подальшому розповсюдженню в

інфраструктурі. На початковому етапі було визначено критичні вузли, що підлягають обов'язковому моніторингу: до них увійшли робочі місця керівного складу, викладачів, системних адміністраторів, а також сервери внутрішніх ресурсів. Для кожного з пристроїв було встановлено EDR-агент, який функціонує у фоновому режимі та не впливає на продуктивність системи. Після реєстрації агентів у централізованій EDR-консолі, було активовано основні профілі моніторингу, включаючи контроль процесів, файлової активності, змін у системному реєстрі, мережевих з'єднань та API-викликів. Уся зібрана телеметрія передавалась до системи аналізу поведінкових аномалій, яка базується на вбудованих правилах і машинному навчанні. Особливу увагу було приділено виявленню загроз без використання сигнатур, що дозволило знаходити нові або модифіковані форми шкідливого програмного забезпечення, які традиційні антивіруси не ідентифікують. У випадках виявлення підозрілої активності система автоматично генерувала інцидент, який передавався в консоль адміністратора безпеки. У межах обробки подій здійснювалася кореляція з логами автентифікації (LDAP/AD), інформацією з SIEM-системи, а також з історією запуску додатків на відповідному хості. Це дозволило отримувати повний контекст дій користувача, виявляти зв'язки між скомпрометованими обліковими записами, мережевими сесіями та шкідливими об'єктами. У рамках реагування на інциденти застосовувались наперед визначені сценарії, що включали ізоляцію кінцевого пристрою від мережі, примусове завершення процесу, видалення шкідливого коду, або блокування доступу до зовнішніх сервісів. У складніших випадках адміністратору пропонувалась можливість ініціювати forensic-аналіз пристрою, що дозволяло виявити повний ланцюг компрометації — від моменту початкового впливу до кінцевого виконання шкідливих дій. За допомогою журналювання змін і модулів сценарного аналізу всі події фіксувалися з точністю до секунди, з подальшим формуванням звітів для подальшого аудиту. Інтеграція EDR у загальну архітектуру захисту НАДПСУ забезпечила високий рівень видимості дій на кінцевих точках, скоротила час реагування на загрози, знизила ризик lateral

movement зловмисників по внутрішній мережі, а також підвищила ефективність координації дій адміністративного персоналу. Це дозволило сформувати єдиний оперативний простір між засобами моніторингу, автентифікації та аналітики, забезпечивши стійкість до загроз навіть у разі складної багатовекторної атаки.

Розвитку системи кіберзахисту стало впровадження принципів централізованого управління інфраструктурними конфігураціями на основі підходу Infrastructure as Code (IaC). Такий підхід є актуальним у сучасних інформаційних системах, зокрема в умовах зростання масштабів і складності мережі, коли ручне налаштування пристроїв призводить до підвищеного ризику помилок, втрати консистентності та складнощів при відтворенні конфігурацій у разі аварійного відновлення. Передумовою впровадження стала потреба в уніфікації конфігурацій для однотипних пристроїв, таких як маршрутизатори, комутатори, точки доступу та міжмережеві екрани. Було прийнято рішення застосовувати інструменти автоматизації, що дозволяють описувати інфраструктуру як код, із можливістю її керованого розгортання, тестування та оновлення. У межах моделювання розглянуто використання платформи Ansible як оптимального рішення з відкритим кодом, яке підтримує SSH-з'єднання з мережею Cisco, має бібліотеки модулів для конфігурації мережевого обладнання та легко інтегрується з системами контролю версій . На початковому етапі було створено окремий репозиторій, у якому зберігалися шаблони конфігурацій ключових мережевих компонентів. Опис інфраструктури було здійснено у форматі YAML у вигляді playbook'ів, кожен з яких відповідав певному сценарію, наприклад: налаштування VLAN, конфігурація портів комутатора, генерація списків доступу, розгортання політик NAT або VPN. Було визначено змінні, які адаптують шаблони під конкретні підмережі, діапазони IP-адрес, рівні доступу та профілі трафіку. Ці змінні зберігалися окремо у змінних середовища (inventory), що дозволило використовувати один і той самий шаблон для десятків пристроїв без ризику помилок при повторенні дій. Після створення базових конфігурацій була проведена автоматизована перевірка їхньої коректності за допомогою симуляційного

середовища. У випадку мережевого обладнання, що підтримує API або SSH, було здійснено пряме застосування конфігурацій на пристрої через команди Ansible ansible-playbook. Усі події виконання зберігались у логах системи, що дозволяло виявити помилки або невідповідності ще на етапі розгортання. Додатково було реалізовано функцію бекапу — перед кожним застосуванням змін зчитувалась поточна конфігурація з пристрою та зберігалася у захищеному каталозі. Таким чином, у разі збоїв зміни можна було скасувати шляхом відновлення з резервної копії. Усі підключення до пристроїв здійснювались по SSH з використанням сертифікатів або ключів, що зберігалися в захищених сховищах. Контроль прав доступу адміністраторів реалізовувався через систему ролей Git та розмежування прав у самій платформі автоматизації. Усі зміни в шаблонах проходили етап погодження (pull request), що дозволяло здійснювати рецензію змін до їх впровадження. Впровадження принципу Infrastructure as Code у межах мережі НАДПСУ дозволило досягти високого рівня узгодженості між окремими сегментами інфраструктури, мінімізувати людський фактор при масштабуванні або супроводі мережевих пристроїв, а також забезпечити цілісність та повторюваність конфігурацій. Інтеграція системи управління з системою контролю версій, автоматизованим тестуванням і політиками безпеки створила фундамент для подальшого розгортання CI/CD-підходу в контексті обслуговування інфраструктури критичних інформаційних об’єктів. У перспективі це дозволяє зменшити час впровадження змін, покращити контроль за змінами в налаштуваннях і значно підвищити рівень операційної надійності системи

На рисунку 3.1 представлено фрагмент логічної топології мережі, схема відображає сегментовану структуру локальної мережі, що включає адміністративні, навчальні та сервісні вузли з відповідною маршрутизацією, контролем доступу та виходом до зовнішнього середовища через міжмережевий екран.

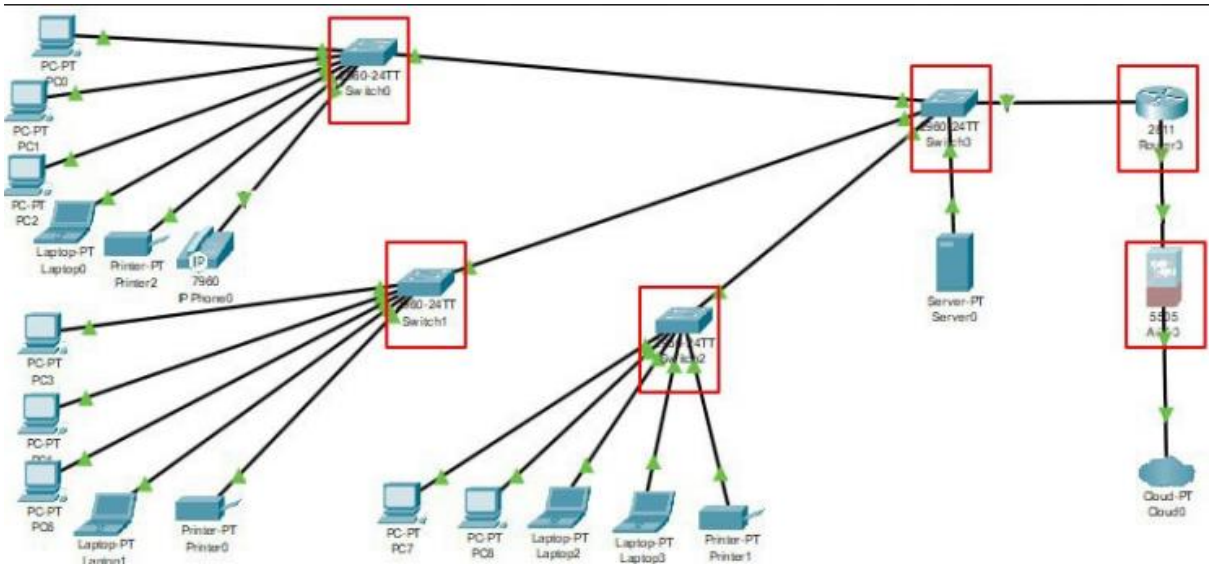


Рисунок 3.5 – Логічна топологія мережі після впровадження засобів захисту

Побудована модель мережі, демонструє результат впровадження комплексної системи захисту, що поєднує логічне сегментування, контроль доступу, маршрутизацію та захищений вихід до зовнішнього середовища. У структурі реалізовано ізольовані підмережі з чітко визначеними ролями, що уможливлює безпечну взаємодію між користувачами, сервісами та адміністративними ресурсами. Завдяки впровадженим заходам створено стабільне, захищене та функціонально розмежоване інформаційне середовище, яке відповідає сучасним вимогам до безпеки критичної інфраструктури в умовах діяльності навчального закладу.

3.3 Висновки

Змодельовано фрагмент інформаційно-телекомунікаційної інфраструктури Національної академії Державної прикордонної служби України з метою реалізації технічних засобів захисту інформаційних потоків між логічно ізольованими сегментами мережі. З урахуванням масштабності реального середовища, дослідження зосереджено на сегменті з адресним простором 172.16.0.0/16, до якого

входять ключові компоненти внутрішньої мережі: маршрутизатор, міжмережевий екран, комутатори доступу, серверна інфраструктура, а також підмережі, призначені для адміністративного, навчального та технічного персоналу. Реалізована логічна топологія побудована на основі ізоляції віртуальних локальних мереж (VLAN) з подальшою маршрутизацією між ними, що дало змогу забезпечити контрольовану взаємодію між сегментами. Впровадження розширених списків контролю доступу (ACL) дозволило регламентувати доступ до ресурсів відповідно до обмежень, визначених політикою мінімальних прав. Налаштовано механізми трансляції адрес (NAT) та фільтрації трафіку, що забезпечило створення захищеного каналу виходу в зовнішнє середовище через міжмережевий екран Cisco ASA. Для підвищення ефективності захисту прикладного рівня до мережі інтегровано міжмережевий екран нового покоління з вбудованим веб-аплікаційним фаєрволом, що дало змогу здійснювати аналіз HTTP/HTTPS-трафіку, контролювати параметри TLS-з’єднань і виявляти атаки на веб-інтерфейси. Завдяки цьому досягнуто підвищення стійкості серверної зони до складних загроз прикладного характеру. Водночас було реалізовано систему виявлення та реагування на загрози з боку кінцевих пристроїв. За допомогою платформи EDR забезпечено моніторинг поведінкової активності, виявлення аномалій, фіксацію інцидентів безпеки та їх кореляцію з іншими джерелами подій. Це сприяло локалізації потенційно небезпечної активності на ранніх етапах і зменшенню ризику горизонтального розповсюдження загроз мережею. Управління конфігураціями здійснюється із застосуванням методології Infrastructure as Code, що передбачає створення шаблонів конфігураційних сценаріїв для автоматизованого налаштування пристроїв. Такий підхід забезпечив узгодженість параметрів між різними компонентами інфраструктури, мінімізував ймовірність помилок при розгортанні системи та заклав основу для подальшої автоматизації змін і оновлень. Результати, отримані в ході моделювання, засвідчили ефективність застосування багаторівневого підходу до організації захисту.

ВИСНОВКИ

Дипломна робота присвячена розробці та обґрунтуванню багаторівневої архітектури захисту передачі інформації між об’єктами критичної інфраструктури в закладі вищої освіти на прикладі Національної академії Державної прикордонної служби України. У процесі дослідження здійснено системний аналіз нормативно-правового забезпечення та міжнародних стандартів у сфері інформаційної безпеки, виконано класифікацію загроз і вразливостей, а також оцінено існуючі методи захисту інформаційних потоків. Застосування методології CORAS дозволило формалізувати ризики, змоделювати актуальні сценарії атак і виявити критичні точки уразливості, що лягло в основу адаптованої моделі інформаційної безпеки з чітко визначеними функціональними та нефункціональними вимогами.

Практична частина дослідження реалізована в середовищі Cisco Packet Tracer, де побудовано логічну мережеву топологію з сегментуванням за допомогою VLAN, політиками контролю доступу на основі ACL, фільтрацією трафіку та ізоляцією критичних серверних вузлів. Інтеграція засобів наступного покоління — NGFW і WAF — забезпечує глибоку інспекцію мережевого та прикладного трафіку, а впровадження EDR-рішень дає змогу здійснювати поведінковий моніторинг кінцевих пристроїв. Використання підходу Infrastructure as Code сприяло автоматизації керування конфігураціями, уніфікації параметрів налаштувань та зниженню впливу людського фактора на процес розгортання і супроводження системи безпеки.

Проведений експериментальний аналіз підтвердив здатність розробленої архітектури ефективно забезпечувати конфіденційність, цілісність і доступність даних навіть за умов інтенсивного навантаження та різноманітних кіберзагроз. Запропоноване рішення вирізняється високим рівнем модульності та масштабованості, що дає змогу адаптувати його до потреб інших організацій із підвищеними вимогами до захисту інформації.

ПЕРЕЛІК ДЖЕРЕЛ

1. Критична інфраструктура. Київ Пост. URL: https://www.kyivpost.com/uk/post/28283 (дата звернення: 26.02.2025).

2. Положення про утворення державної служби. від 24.09.2003 №912/2003.Дата оновлення 20.04.2025 URL: https://zakon.rada.gov.ua/laws/show/787-2022-п#Text (дата звернення: 26.02.2025).

3. Про критичну інфраструктуру.:Закон України від 16.11.2021 №1882-IX.Дата оновлення:21.09.2024 URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 26.02.2025).

4. Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури.. URL: https://zakon.rada.gov.ua/rada/show/v0023519-21#Text (дата звернення: 26.02.2025).

5. Зловмисне програмне забезпечення - Терміни та визначення кібербезпеки.
URL: https://www.vpnunlimited.com/ua/help/cybersecurity/malware?srsltid=AfmBOorzo9_35EkF7vu95j4mt8971pH5oVnPpgwAL6E3I0YEk8U_MGi1 (дата звернення: 26.02.2025).

6. Фішинг та інші техніки соціальної інженерії. Освітній проект «На Урок» для вчителів. URL: https://naurok.com.ua/post/fishing-ta-inshi-tehniki-socialno-inzheneri (дата звернення: 26.02.2025).

7. DoSS – атака. URL:https://foxminded.ua/ddos-ataka/ (дата звернення: 26.02.2025).

8. Атаки типу Man-In-The-Middle: що треба знати кожному. URL: https://www.imena.ua/blog/man-in-the-middle/ (дата звернення: 26.05.2025).

9. Атака на ланцюг постачання - втручання в кібербезпеку ланцюга постачання.URL: https://www.eset.com/ua/about/newsroom/blog/business-security/kolichestvo-atak-na-tsep-postavok-rastet-kto-pod-pritselom-i-kak-

protivostoyat/?srsltid=AfmBOoq8RP (дата звернення: 27.02.2025).

10. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 27.02.2025).

11. Guide for Conducting Risk Assessments. URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (дата звернення: 27.02.2025).

12. Класифікація техногенних небезпек та коротка характеристика їх вражаючих факторів | Журнал ECOBUSINESS. URL: https://ecolog-ua.com/news/klasyfikaciya-tehnogennyh-nebezpek-ta-korotka-harakterystyka-yih-vrazhayuchyh-faktoriv (дата звернення: 28.02.2025).

13. Лелюк О. Антропогенні зміни довкілля. *BYE*. URL: https://vue.gov.ua/Антропогенні_зміни_довкілля (дата звернення: 28.02.2025).

14. Загрози безпеки AIC, причини виникнення загроз - Бібліотека BukLib.net. URL: https://buklib.net/books/28541/ (дата звернення: 28.02.2025).

15. .Smarttender. Об'єкти критичної інфраструктури: детальний аналіз та відповіді на поширені питання. URL: https://smarttender.biz/blog/view/ob-yekti-kritichnoyi-infrastrukturi-detalniy-analiz-ta-vidpovidi-na-poshireni-pitannya (дата звернення: 28.02.2025).

16. Системи виявлення вторгнень. *ESET Online Help*. URL: https://help.eset.com/ees/9/uk-UA/idh_hips_main.html (дата звернення: 01.03.2025).

17. Проблеми забезпечення безпеки в комп’ютерних системах і мережах | Тест з інформатики – «На Урок». URL: https://naurok.com.ua/test/problemi-zabezpechennya-bezpeki-v-komp-yuternih-sistemah-i-merezhah-2493352.html (дата звернення: 02.03.2025).

18. Проблеми безпеки у відкритих інформаційних системах.

URL: https://ua.kursoviks.com.ua/metodychki/449-testi-problemi-bezpeki-u-vidkritikh-informatsiynikh-sistemakh (дата звернення: 02.03.2025).

19. Симетричне шифрування. URL: https://medium.com/@karlooo/симетричне-шифрування-1e878058d361 (дата звернення: 26.05.2025).

20. Що таке IPS/IDS і де застосовується - Блог - HostZealot. *HostZealot*. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya (дата звернення: 01.03.2025).

21. Шифрування: типи і алгоритми. URL: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/ (дата звернення: 01.03.2025).

22. Про стандарт Triple DES (3DES). URL: https://rubydevelopers.org/t/triple-des-3des/424 (дата звернення: 04.03.2025).

23. Аудит безпеки інформаційної безпеки. *ТЗІ* - інформаційна безпека та захист інформації. URL: https://tzi.com.ua/audbezib.html (дата звернення: 02.03.2025).

24. Аутентифікація і авторизація: що це і в чому відмінність.. URL: https://qagroup.com.ua/publications/autentyfikatciia-i-avtoryzatciia/ (дата звернення: 02.03.2025).

25. Аудит системи інформаційної безпеки. URL: https://referatss.com.ua/work/audit-sistemi-informacijnoi-bezpeki-2/ (дата звернення: 02.03.2025).

26. ІПС ЛІГА:ЗАКОН - система пошуку, аналізу та моніторингу нормативно-правової бази. URL: https://ips.ligazakon.net/document/KP201109 (дата звернення: 02.03.2025).

27. Сучасні методи фізичної охорони: від класичних до високотехнологічних рішень. URL: https://strazh.in.ua/methods.html (дата звернення: 05.03.2025).

28. Що таке мережеве IDS - Терміни та визначення кібербезпеки. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/network-based-

ids?srsltid=AfmBOoqSRgcPXNKjVZdMivbYiF1uSeOA729n2l9k0I35fkPJ2UT_96Qo (дата звернення: 05.03.2025).

29. Що таке IPS/IDS і де застосовується - Блог - HostZealot. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya (дата звернення: 05.03.2025).

30. НАДПСУ – НАДПСУ. URL: https://nadpsu.edu.ua/ (дата звернення: 12.03.2025).

31. Coras | A complete solution for connecting customers to tickets. URL: https://coras.io/index.php (дата звернення: 15.04.2025).

32. The CORAS Method. *The CORAS Method*. URL: https://coras.sourceforge.net/ (дата звернення: 19.04.2025).

33. Що таке керування доступом на основі ролей (RBAC)? Визначення | Солікс. URL: https://www.solix.com/uk/kb/role-based-access-control/ (дата звернення: 26.04.2025).

34. Дія.Освіта – IT-студії. URL: https://it-osvita.diia.gov.ua/task/item/21cadbcd-2818-4752-acd2-324d3af66ece (дата звернення: 26.04.2025).

35. Атака на ланцюг постачання - втручання в кібербезпеку ланцюга постачання. ESET. | ESET. URL: https://www.eset.com/ua/about/newsroom/blog/business-security/kolichestvo-atak-na-tsep-postavok-rastet-kto-pod-pritselom-i-kak-protivostoyat/?srsltid=AfmBOorJah1R (дата звернення: 26.04.2025).

36. Управління змінами (Change management). URL: https://www.maxzosim.com/change-management/ (дата звернення: 26.04.2025).

37. DDoS Protection. URL: https://retn.net/trending/free-ddos-protection-ukraine?campaignid=22182198951&adgroupid=175285084020&keyword=ddos-атака&device=c&network=g&gad_source=1&gad_campaignid=22182198951&gbraid=0AAAAABLSOx-2VT46yZmC2l-PrVV_Vuhy2&gclid=Cj0KCQjwotDBBhCQARIsAG5pinPohIKHVAY2ffG30yo2

8kE3e2PQztvwif6FdmWj327OjizheBGIWRMaAkjHEALw_wcB (дата звернення: 26.04.2025).

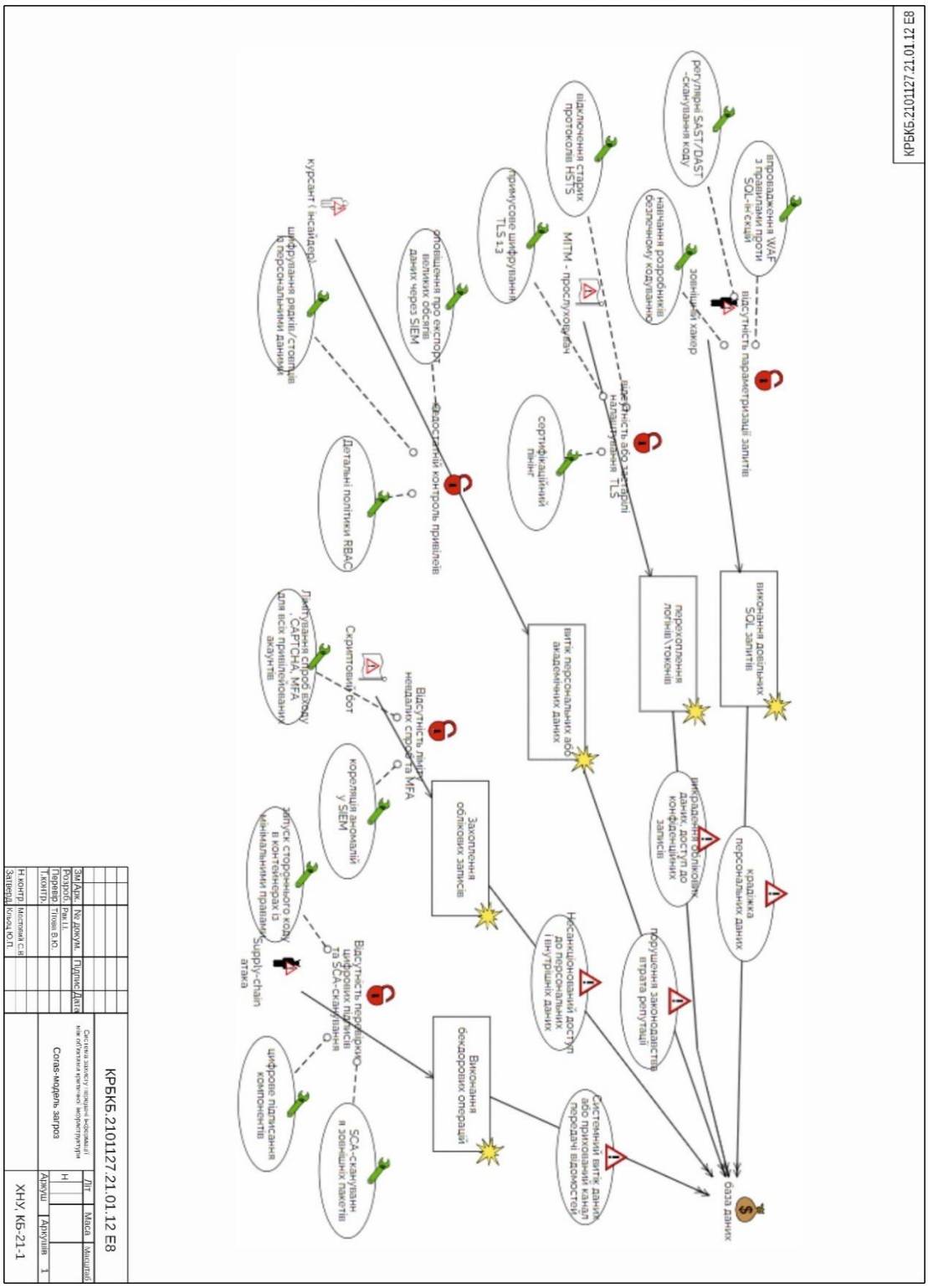
38. Що таке міжмережевий екран і навіщо він потрібен?. URL: https://stack-systems.com.ua/blogs/shtcho-take-mizmerezevyj-ekran-i-navishtcho-vin-potriben?srsltid=AfmBOoqitqB-f1sJaQm2t055ubULQTRgJxBXMwMZf8XJsvXbcptn (дата звернення: 03.05.2025).

39. Рішення / ІБ / Endpoint. URL: https://softlist.ua/servises/endpoint?gad_source=1&gad_campaignid=21002459508&gbraid=0AAAAAp6FHDoXdyW2BzRKt4MQjXGI3XAOC&gclid=EAIaIQobChMItN--zL7B (дата звернення: 03.05.2025).

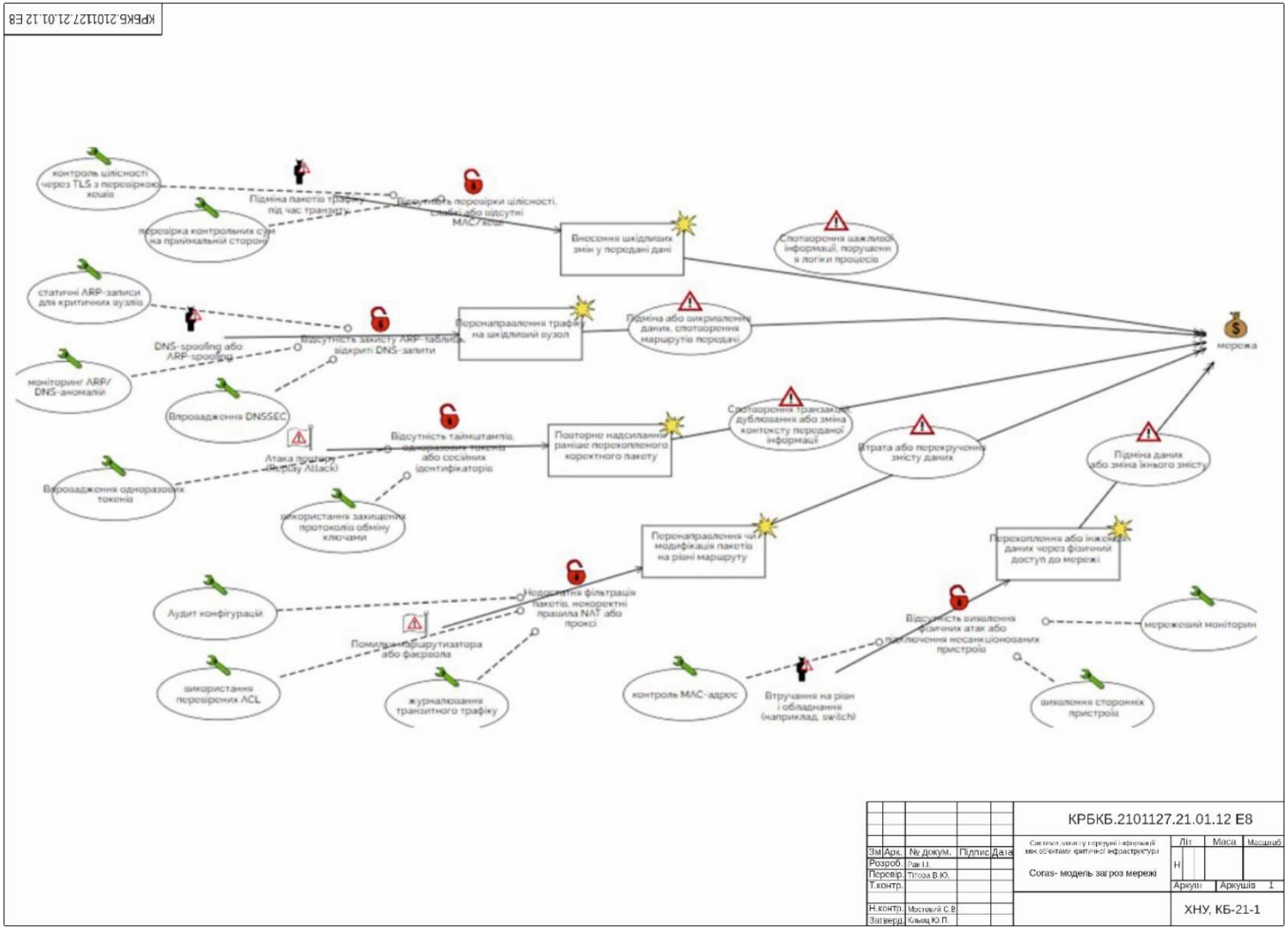
40. Що таке ALM керування життєвим циклом програми: визначення | Найкращі інструменти | Повне керівництво. URL: https://visuresolutions.com/uk/блог/alm/ (дата звернення: 03.05.2025).

ДОДАТОК А

Копії графічної частини

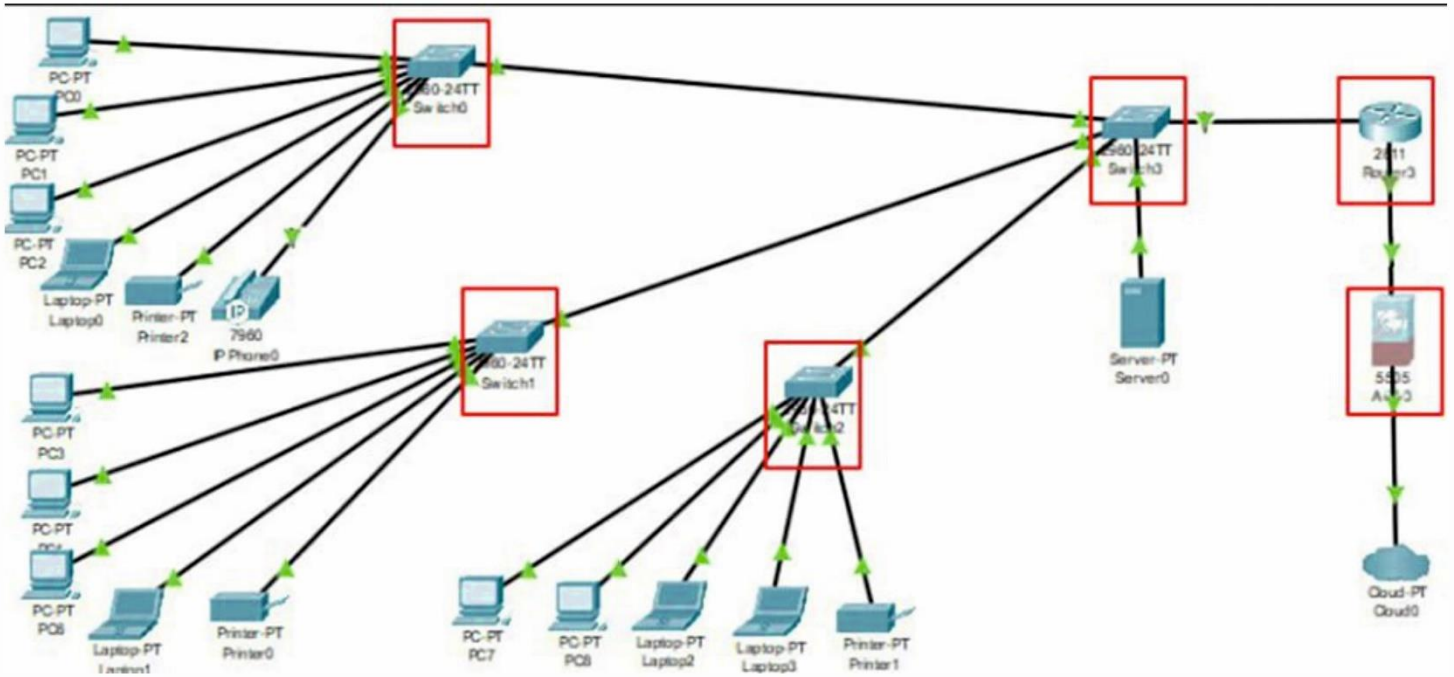


КРБКБ.2101127.21.01.12 Е8



					КРБКБ.2101127.21.01.12 Е8
Зм.	Арк.	№ докум.	Підпис	Дата	Система захисту передачі інформації між об'єктами критичної інфраструктури
Розроб.		Рак І.І.			Літ. / Маса / Масштаб
Перевір.		Тітова В.Ю.			Н
Т.контр.					Coras- модель загроз мережі
					Аркушів 1
Н.контр.		Мостовий С.В.			ХНУ, КБ-21-1
Затверд.		Кільоц Ю.П.			

КРБКБ.2101127.21.01.12 Е8



					КРБКБ.2101127.21.01.12 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Система захисту у передачі інформації між об'єктами критичної інфраструктури	Літ / Маса / Масштаб
Розроб.		Рак І.І.			Логічна топологія мережі	Н
Перевір.		Тітова В.Ю.				Аркуш / Аркушів 1
Т.контр.						
Н.контр.		Мостяний С.В.				ХНУ, КБ-21-1
Затверд.		Кльоц Ю.П.				

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Рак Ірини Іванівни
ПІБ здобувача вищої освіти

Студентки ФІТ, 4 курсу, групи КБ-21-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлена. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщена та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

24.05.25
дата

підпис

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Рак Ірина Іванівна

Співавтор:

Назва: Система захисту передачі інформації між обєктами критичної інфраструктури

Науковий керівник:

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:1.1%

Коефіцієнт подібності 2:0%

Мікропробіли: 0

Заміна букв: 2

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-05-29 23:05:05.0

Після аналізу Звіту подібності констатую наступне:

☑ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

30.05.2025р.

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 0.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 9%**

	Document		Sum coincidence on the DB	
ID: 242465 Title: Система захисту передачі інформації між обєктами критичної інфраструктури Added in a DB: 2025-05-29 Authors: Рак Ірина Іванівна Heads: Тітова В.Ю. Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	133660	1983	970 (1%)	19 (1%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система захисту передачі інформації між об'єктами критичної інфраструктури

Автор: Рак Ірина Іванівна

Спеціальність: 125 – Кібербезпека

Освітня програма:Кібербезпека

Науковий керівник: Віра ТІТОВА, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих методів та технологій, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 1,1%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Віра ТІТОВА

Завідувач кафедри Кб _____ Юрій КЛЬОЦ

Гарант ОП _____ Віктор ЧЕШУН

Дата:

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Рак Ірина Іванівна
Тема: «Система захисту передачі інформації між об'єктами критичної інфраструктури»
Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*» Освітня програма «Кібербезпека»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3; кількість сторінок записки 87;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена розробці системи захисту передавання інформації між сегментами критичної інформаційної інфраструктури освітнього закладу. У роботі проаналізовано сучасні загрози інформаційній безпеці, особливості функціонування розподілених мережевих систем і методи забезпечення цілісності та конфіденційності переданих даних. Визначено актуальні ризики, пов'язані з міжмережевим трафіком, несанкціонованим доступом та внутрішніми загрозами.

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було розглянуто існуючі технології захисту інформації в системах критичної інфраструктури, проведено їх порівняльний аналіз. У другому розділі побудовано моделі захисту інформації об'єктів критичної інфраструктури. У третьому розділі наведено реалізацію системи захисту, проведено її налаштування та оцінювання ефективності.

4. Позитивні сторони кваліфікаційної роботи полягають у тому що, у процесі реалізації системи було проведено аналіз загроз та ризиків інформаційним об'єктам критичної інфраструктури; проаналізовано сучасні методи і технології захисту інформації, зокрема криптографічні алгоритми, протоколи безпечного зв'язку (VPN, SSL/TLS, IPSec), системи аутентифікації, а також методику виявлення та запобігання вторгненню; розроблено моделі захисту інформаційних об'єктів критичної інфраструктури; проведено експериментальне тестування запропонованої моделі в симульованому середовищі.

5. Негативні сторони кваліфікаційної роботи: немає

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує відмінної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці багато наглядних пояснень. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «відмінно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Д.т.н., професор, професор кафедри телекомунікацій, медійних та інтелектуальних технологій, Бойко Юлій Миколайович

« 02 » червня 2025. (підпис)