МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВЕТЕРИНАРНОЇ МЕДИЦИНИ ТА БІОТЕХНОЛОГІЙ ІМЕНІ С.З. ҐЖИЦЬКОГО
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

першого (бакалаврського) рівня вищої освіти

на тему:

«Розробка системи захисту закладу вищої освіти від кіберзагроз»

Виконала: студентка 4 курсу
спеціальності 126 «Інформаційні системи та технології»

Цап Марта Ігорівна
(прізвище та ініціали)

Керівник: Желєзняк А.М.
(прізвище та ініціали)

ЛЬВІВ 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Рівень вищої освіти перший (бакалаврський)
Спеціальність 126 «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____
(підпис)
д.т.н., професор, Тригуба А. М.
(вч. звання, прізвище, ініціали)
“____” _____202 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Цап Марта Ігорівна
(прізвище, ім’я, по батькові)

1. Тема роботи *«Розробка системи захисту закладу вищої освіти від кіберзагроз»*

керівник роботи *к. е н., доцент., Желєзняк А.М.*
(наук.ступінь, вч. звання, прізвище, ініціали)

затверджені наказом Львівського НУП №123/к-с від 25.02.2025 р.

2. Строк подання студентом роботи 12.06.2025
3. Вихідні дані: *аналітичні дані роботи та характеристика об’єкту дослідження, опис технології, науково-технічна і довідкова література.*

4. Зміст кваліфікаційної роботи (перелік питань, які потрібно розробити)
Вступ
1. Аналіз предметної області
2. Постановка задачі
3. Проєктування моделі системи кіберзахисту
4. Охорона праці та безпека в надзвичайних ситуаціях
Висновки
Бібліографічний список
5. Перелік графічного матеріалу
Графічний матеріал подається у вигляді презентації

6. Консультанти розділів

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата		Відмітка про виконання
		завдання видав	завдання прийняв	
1, 2, 3	*Желєзняк А.М., к.е.н., доцент кафедри інформаційних технологій*			
4	*Городецький І.М., к.т.н., доцент кафедри інженерної механіки*			

7. Дата видачі завдання 01.11.2024

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Відмітка про виконання
1	*Отримання завдання. Вивчення рекомендованої літератури по темі роботи. Написання аналітичного огляду предметної області.*	*01.11.2024 – 15.12.2024*	
2	*Проектування та опис технічного завдання, функціональних вимог та технічної сторони реалізації проекту (написання проектної частини).*	*16.12.2024 – 05.02.2024*	
3	*Програмна реалізація проекту (аналітичні дані роботи та характеристика об'єкту дослідження, опис технології, розрахунок ефективності проекту)*	*06.02.2025 – 31.03.2025*	
4	*Розгляд питань з охорони праці та безпеки у надзвичайних ситуаціях*	*01.04.2025 – 30.04.2025*	
5	*Завершення оформлення основної частини, написання висновків та підготовка презентаційного матеріалу*	*01.05.2024 – 26.05.2024*	
6	*Завершення роботи в цілому. Підготовка до захисту кваліфікаційної роботи*	*27.05.2024 – 12.06.2024*	

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Желєзняк А.М.*
(підпис) (прізвище та ініціали)

УДК 004.056:378

Кваліфікаційна робота: 66 сторінок текстової частини, 8 таблиць, 25 рисунків, 23 джерел літератури, 3 додатки.

«Розробка системи захисту закладу вищої освіти від кіберзагроз» Цап М.І. - Кваліфікаційна робота. Кафедра інформаційних технологій. Дубляни, Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Ґжицького, 2025 р.

Подано характеристику інформаційної інфраструктури сучасного освітнього закладу.

Проаналізовано предметну область, вивчено існуючі моделі кіберзахисту, технології виявлення вразливостей, методи реагування на інциденти та визначено функціональні вимоги до удосконалення безпеки в цифровому середовищі.

Здійснено проєктування архітектури системи кіберзахисту відповідно до актуальних стандартів та методик. Запропоновано комплексну модель удосконалення інформаційної безпеки на основі інтеграції CVSS, SIEM, SOAR, Zero Trust і VR-навчання.

Здійснено аналіз ризиків, запропоновано сценарії резервного копіювання та практики безпечної взаємодії користувачів з інформаційними системами. Також розглянуто питання охорони праці та психофізіологічної безпеки при роботі з комп’ютерною технікою.

Ключові слова: інформаційна безпека, кіберзагрози, SIEM, SOAR, CVSS, вразливості, резервне копіювання, освітнє середовище, мережна архітектура, політика безпеки, кібергігієна, етичний хакінг.

ЗМІСТ

ВСТУП

Кібербезпека є невід’ємною складовою стабільного функціонування сучасних організацій, особливо у сфері освіти, де активно впроваджуються цифрові технології. Заклади вищої освіти дедалі активніше використовують цифрові технології для забезпечення навчального процесу, організації внутрішньої документації, обміну інформацією, зберігання персональних та академічних даних. У зв’язку з цим зростає ймовірність виникнення кіберзагроз, які можуть порушити роботу установи, спричинити витік конфіденційної інформації або навіть призвести до зупинки навчального процесу.

Варто зазначити, що вища освіта є привабливою ціллю для кіберзлочинців через наявність великих масивів персональних даних, а також часто через недостатню увагу до питань безпеки на рівні користувачів. До найбільш поширених загроз належать фішингові атаки, проникнення до систем через вразливості, шкідливе програмне забезпечення, зокрема програми-здирники, а також атаки типу «відмова в обслуговуванні» (DDoS). Усе це створює потребу в розробці ефективної системи захисту, що враховує як технічні, так і організаційні заходи.

Об'єктом дослідження є інформаційне середовище Північного кампусу, Львівського національного університету ветеринарної медицини та біотехнологій імені С. З. Ґжицького, яке включає в себе різноманітні елементи цифрової інфраструктури: внутрішні інформаційні системи, сервери, бази даних, електронні поштові сервіси, платформи для дистанційного навчання. Саме це середовище потребує системного підходу до забезпечення кібербезпеки з урахуванням потенційних ризиків, сучасних технологій і реальних потреб закладу.

Метою даної роботи є розробка комплексної системи захисту вищого навчального закладу від кіберзагроз, що базується на сучасних підходах до інформаційної безпеки. У межах дослідження передбачається проаналізувати

типові загрози, з якими стикаються освітні установи, виявити вразливі елементи в системі захисту університету, розглянути існуючі політики безпеки та розробити практичні рекомендації щодо їх удосконалення.

Предметом дослідження є методи та засоби забезпечення кібербезпеки в освітньому середовищі, зокрема засоби захисту інформації, управління доступом, політики реагування на інциденти, а також заходи з підвищення обізнаності персоналу та студентів щодо цифрової безпеки.

В ході виконання кваліфікаційної роботи були поставлені наступні завдання:

1. Дослідити теоретичні та методологічні аспекти, основні тенденції та підходи у сфері кібербезпеки освітніх установ.
2. Проаналізувати типові кіберзагрози, що виникають у вищих навчальних закладах, та визначити їхні джерела.
3. Провести аудит інформаційного середовища Північного кампусу Львівського національного університету ветеринарної медицини та біотехнологій імені С. З. Ґжицького з метою виявлення вразливих елементів.
4. Оцінити ефективність чинних політик інформаційної безпеки в університеті.
5. Розробити практичні рекомендації щодо підвищення рівня кіберзахисту: технічні, організаційні та освітні заходи.
6. Сформувати комплексну модель системи захисту освітнього середовища від кіберзагроз з урахуванням реальних потреб закладу.
7. Надати пропозиції щодо впровадження інформаційної безпеки як елементу цифрової культури в навчальному середовищі.

Таким чином, дослідження спрямоване на формування практично орієнтованої моделі захисту інформаційного простору університету, що може бути застосована як у межах зазначеного закладу, так і в інших вищих навчальних установах України.

РОЗДІЛ 1.
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Огляд видів кіберзагроз

Кіберзагрози стали фундаментальною проблемою цифрової епохи, в якій функціонують сучасні організації, установи, компанії та освітні заклади. У міру того як людство все глибше інтегрується у цифрове середовище, зростає залежність від інформаційних систем, що зумовлює потребу в посиленні заходів захисту від кібер інцидентів. Обсяг даних, що обробляються в цифровій формі, постійно зростає, охоплюючи як персональну, так і конфіденційну інформацію, яка часто є критичною для безперервності діяльності організацій.

Сучасна цифрова інфраструктура стикається з широким спектром кіберзагроз, які постійно змінюються та ускладнюються. Серед них вирізняється фішинг, який базується на соціальній інженерії. У фішингових атаках зловмисники надсилають електронні листи або повідомлення, що імітують справжні, з метою змусити користувача розкрити конфіденційні дані. Фішинг — одна з найпоширеніших форм кібератак, що часто слугує першим кроком до масштабного компрометування інформаційних систем. Зловмисники вдосконалюють методи обману: листи можуть містити посилання на фальшиві сайти, які візуально не відрізняються від оригінальних, або вкладення з шкідливим кодом. Особливо небезпечними є так звані spear-phishing атаки — цілеспрямовані атаки на конкретних осіб або організації з урахуванням їх контексту та поведінки. Фішинг може також здійснюватися через SMS (smishing) або голосові дзвінки (vishing), що розширює канали атаки.

На рисунку 1.1. Наводиться приклад, коли на електронні скриньки державних установ України надходили листи, що маскувалися під повідомлення від «Нової Пошти». У цих листах йшлося про нібито підтвердження відправлення вантажу з проханням перейти за посиланням для

перегляду деталей. За посиланням ховався архів із шкідливим програмним забезпеченням Agent Tesla.

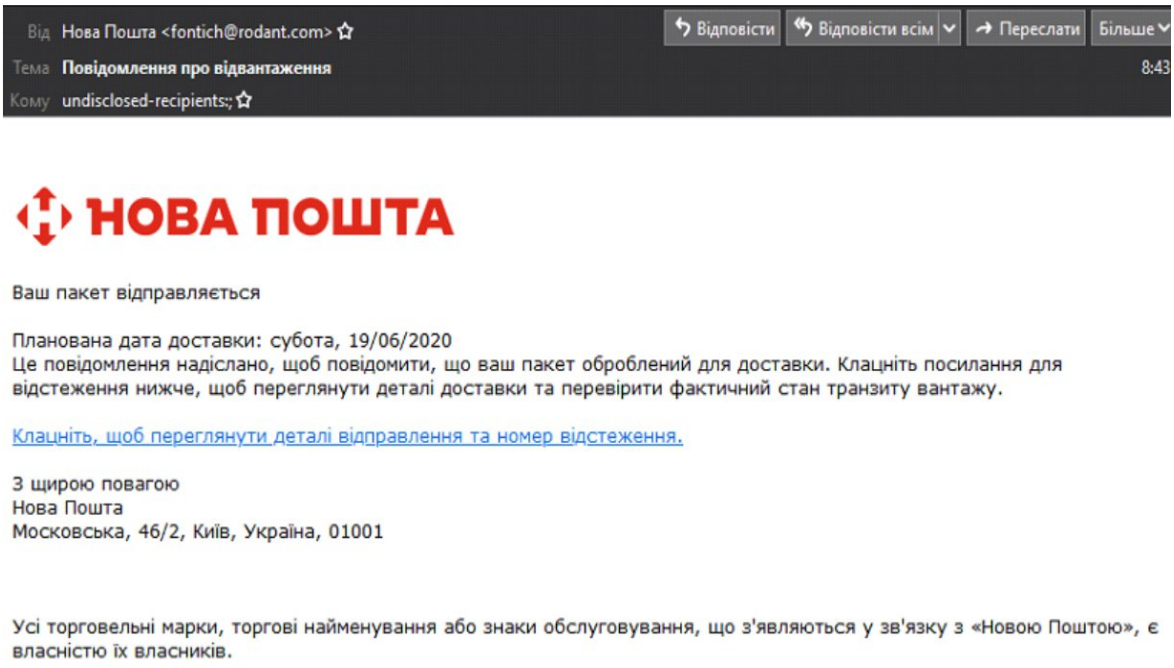

Рисунок 1.1 - Фішинговий електронний лист [1]

Іншою поширеною загрозою є шкідливе програмне забезпечення. Його різновиди включають троянські програми, кейлогери (keylogger), шпигунське ПЗ, рекламні віруси та програми-вимагачі (ransomware). Особливо небезпечними є програми, що шифрують дані та вимагають викуп, — їх використання часто спричиняє зупинку бізнес-процесів. Наприклад, у разі ураження корпоративної мережі організації може бути паралізована робота цілих підрозділів, що призводить до втрати репутації, фінансових збитків і юридичних наслідків.

DDoS-атаки (атаки на відмову в обслуговуванні) стають інструментом тиску на комерційні структури, медіа та державні ресурси. Такі атаки спрямовані на виведення з ладу онлайн-сервісів через масову кількість одночасних запитів, що перевантажують сервери. Наслідком є неможливість доступу до веб-сайту або сервісу, що негативно впливає на імідж і довіру клієнтів чи користувачів.

На рисунку 1.2. зображена типова архітектура DDoS-атаки. Зловмисник (attacker) керує мережею заражених пристроїв, так званих "зомбі" (zombie), через проміжні сервери-«керівники» (handler). Ці зомбі-комп’ютери надсилають тисячі або навіть мільйони запитів до сервера-жертви (victim), що в результаті призводить до перевантаження і відмови в обслуговуванні. Такий розподілений характер атаки ускладнює її виявлення і протидію, адже шкідливі запити надходять із легітимних, на перший погляд, пристроїв по всьому світу.

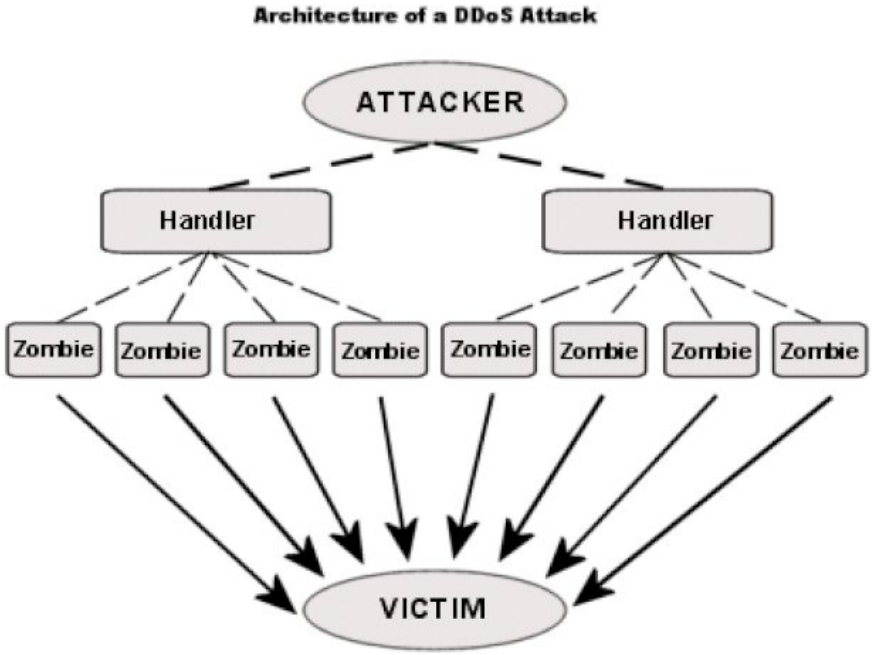

Рисунок 1.2. - Архітектура DDoS-атаки [2]

Також слід зазначити загрозу використання соціальної інженерії у більш широкому розумінні, ніж просто фішинг. Це може бути обман, маніпуляція або психологічний тиск на працівників, що дозволяє зловмиснику отримати несанкціонований доступ до інформації або ресурсів. Наприклад, видаючи себе за адміністратора або IT-спеціаліста, зловмисник може змусити працівника змінити пароль або надати віддалений доступ до системи.

Внутрішні загрози також набувають особливої актуальності. Вони можуть виходити від співробітників, які мають доступ до систем організації.

Наприклад, підключення зараженого зовнішнього накопичувача або пересилання конфіденційної інформації в ненадійний канал комунікації може мати серйозні наслідки.

Ще однією з новітніх загроз є атаки на ланцюг постачання. Зловмисники проникають у системи через скомпрометовані компоненти програмного або апаратного забезпечення постачальника. Такі атаки важко виявити, оскільки шкідливий код може бути інтегрований ще на етапі розробки або поставки продукту.

Рисунок 1.3. - Статистика та характеристики атак на ланцюг постачання за даними ENISA. [3]

Як показано на рисунку 1.3, 66% таких атак фокусуються саме на коді постачальника, що дозволяє зловмисникам впливати на кінцеву систему без прямого втручання. Крім того, 62% атак використовують шкідливе програмне забезпечення, яке часто поширюється через оновлення чи пакети програм. Ще 62% зловмисників зловживають довірою клієнтів до своїх постачальників, що ускладнює виявлення загрози, а 58% атак мають на меті отримання доступу до конфіденційних даних.

Варто зазначити, що кіберзагрози є багатовимірними й вимагають адаптивного, проактивного підходу. Сучасні методи захисту повинні охоплювати як технічну складову, так і підвищення обізнаності персоналу, постійне оновлення програмного забезпечення та стратегічне планування безпеки.

1.2 Основні проблеми забезпечення кібербезпеки

Попри розвиток технологій захисту, компанії, установи та інші організації регулярно стикаються з численними викликами у сфері кібербезпеки. Багато проблем мають системний характер і потребують комплексного підходу до вирішення. Основним джерелом ризиків часто стає недостатня координація між керівництвом, технічними підрозділами й кінцевими користувачами.

Одна з ключових проблем — використання застарілого програмного забезпечення. Через брак коштів або недооцінку ризиків компанії продовжують експлуатувати програми, які більше не оновлюються виробником. Це робить їх уразливими до атак, зокрема до експлойтів (спеціальні програмні коди або методи, які використовуються для використання вразливостей у програмному забезпеченні, операційних системах або апаратному забезпеченні.) [4]

Ще одна важлива проблема — неконтрольоване управління доступом. У багатьох організаціях облікові записи колишніх працівників залишаються активними, паролі зберігаються у відкритому доступі, або ж працівники мають надмірні повноваження. Відсутність принципу мінімальних прав веде до того, що при зламі одного облікового запису зловмисник отримує широкий доступ до ресурсів організації.

Недостатній рівень обізнаності працівників також є серйозною перешкодою на шляху до створення ефективної системи захисту. Навіть найкращі технології можуть бути безсилі, якщо працівники не вміють

розпізнавати фішингові повідомлення, не дотримуються політик безпеки або свідомо порушують встановлені правила. Проблема часто поглиблюється через відсутність навчання з кібергігієни.

Людський фактор загалом відіграє провідну роль у виникненні інцидентів. Це може бути як необережне натискання на шкідливе посилання, так і навмисне викрадення інформації. Також не можна ігнорувати помилки в конфігурації систем, які трапляються через поспіх або нестачу кваліфікації в IT-персоналу. Наприклад, неправильно налаштований сервер може стати відкритим для доступу ззовні без жодного захисту.

Брак фінансування є ще одним типовим бар'єром на шляху до забезпечення кіберстійкості. Інвестиції в кібербезпеку часто розглядаються як витрати, а не як інвестиції в довгострокову стабільність. Це призводить до ситуацій, коли системи безпеки не відповідають поточним загрозам, а політики реагування на інциденти залишаються неактуальними або відсутні зовсім.

Ще один аспект — відсутність інтеграції кібербезпеки в загальну стратегію розвитку. Кібербезпека не повинна бути лише технічним питанням IT-відділу. Вона має бути складовою корпоративної культури, стратегічного планування і процесу ухвалення рішень. Успішні організації впроваджують політики, які охоплюють усі рівні — від топменеджменту до пересічного користувача.

У зв'язку з цим компанії все частіше впроваджують формалізовані політики кібербезпеки, які визначають правила поводження з інформацією, управління доступом, реагування на інциденти, а також відповідальність за порушення. Наприклад, політика «Zero Trust» передбачає, що жоден користувач або пристрій не вважається надійним за замовчуванням — усі дії перевіряються, і доступ надається лише в межах необхідного. Інші популярні підходи включають використання багатофакторної автентифікації (MFA), обмеження доступу за принципом найменших привілеїв (Least Privilege) та регулярний аудит безпеки.[5]

В таблиці 1.1. описано основні принципи політики «Zero Trust» та подано їх характеристику.

Таблиця 1.1. – Принципи політики «Zero Trust»

Назва принципу	Опис
Мікросегментації	Полягає в розділенні мережі на невеликі ізольовані сегменти, де кожен вузол або ресурс контролюється окремо. Це дозволяє зменшити масштаб потенційного вторгнення.
Принцип "Найменших привілеїв" (Least Privilege Access)	Кожен користувач, пристрій або програма мають доступ лише до мінімально необхідного обсягу ресурсів, що знижує ризик зловживання або компрометації.
Інспекція трафіку	Уся мережна активність, включно з внутрішнім трафіком, підлягає аналізу та моніторингу. Це дає змогу виявляти підозрілу поведінку в режимі реального часу.
Постійна перевірка	Довіра не надається автоматично — кожен запит перевіряється з урахуванням контексту: пристрою, геолокації, поведінки користувача, часу доступу тощо.

Також важливим є впровадження планів реагування на кібер інциденти, які регламентують дії працівників у разі виявлення порушення безпеки. До таких планів входять алгоритми фіксації інцидентів, повідомлення відповідальних осіб, збереження доказів і запуск відновлювальних процесів. Компанії, що мають такі плани, значно швидше і з меншими втратами долають наслідки атак.

Згадуючи про освітні установи, варто зазначити, що багато з цих підходів також застосовні й у сфері освіти. Проте рівень їх впровадження часто залишається нижчим у зв’язку з обмеженими ресурсами, а отже й ризики — вищими.

Таким чином, забезпечення кібербезпеки в сучасних умовах — це не лише впровадження технічних рішень, а й створення цілісної екосистеми захисту. Вона повинна поєднувати правові, організаційні та освітні компоненти, які взаємодіють між собою і постійно адаптуються до нових викликів.

1.3. Приклади відомих кібератак та їх наслідки

Практика демонструє, що навіть великі компанії та державні структури з потужною IT-інфраструктурою можуть ставати жертвами успішних кібератак. Ці випадки є важливими для аналізу, оскільки дозволяють виявити спільні вразливості та засоби протидії.

Відомим прикладом масштабної кіберзагрози, що продемонструвала вразливість цифрової інфраструктури на рівні держави, стала атака вірусу-вимагача Petya.A, яка у 2017 році призвела до значних збоїв у роботі установ та підприємств по всьому світу. Особливої шкоди зазнала саме Україна. Як видно з рисунка 1.4, понад 75% усіх зареєстрованих випадків зараження припали саме на українські комп’ютери. Для порівняння, в Німеччині зафіксовано лише 9,06% випадків, а в Польщі — 5,81%. Такий дисбаланс свідчить про цілеспрямований характер атаки та вказує на низький рівень готовності організацій в Україні до протидії складним загрозам.

Атака Petya.A відзначалась особливою небезпекою через механізм поширення: використовуючи вразливості в системах Windows (зокрема EternalBlue), вона миттєво заражала цілу мережу після потрапляння на один комп’ютер. Шифрування системних файлів та вимога викупу робили її класичним прикладом програм-здирників (ransomware). Однак у випадку з Україною аналітики припускають, що справжньою метою атаки було не отримання прибутку, а дестабілізація роботи критичної інфраструктури.

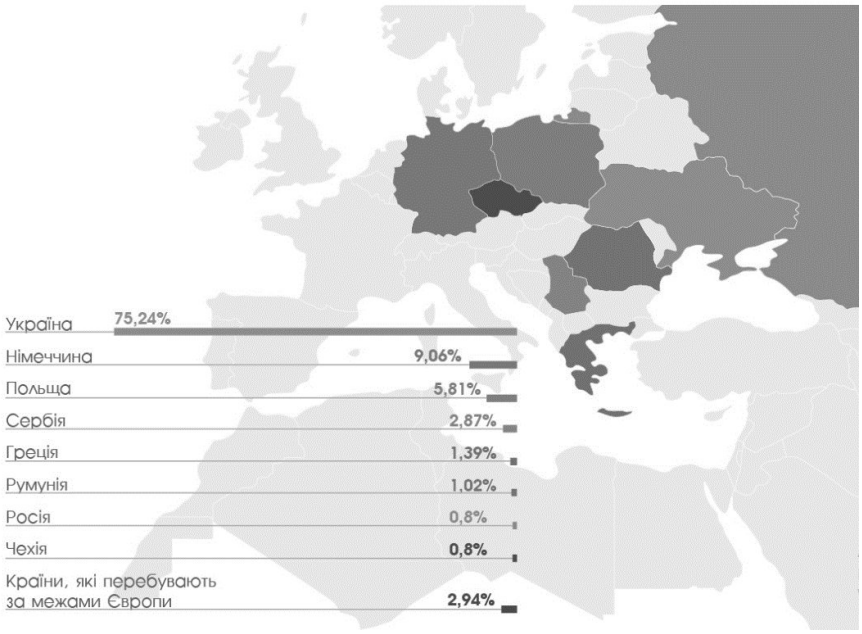

Рисунок 1.4 – Кількість випадків зараження комп'ютерів вірусом-вимагачем Petya.A, у % від загальної кількості в світі [6]

Цей інцидент підкреслив необхідність упровадження проактивних систем кіберзахисту, а також важливість навчання персоналу основам цифрової гігієни та резервного копіювання даних.

Схожим за масштабом і механізмом був вірус WannaCry. Він також використовував вразливості Windows і шифрував інформацію на жорсткому диску. (рис.1.5)

Рисунок 1.5 - Інтерфейс вікна-вимоги вірусу-здирника WannaCry[7]

Проте в цьому випадку зловмисники мали фінансову мету й отримали значні суми в біткоїнах. Атака зачепила понад 200 тисяч комп’ютерів по всьому світу, включно з лікарнями, банками та університетами.

Іншим прикладом є злам мережі університету Каліфорнії, внаслідок якого були викрадені персональні дані тисяч студентів і викладачів. У цьому випадку зловмисники отримали доступ через фішингове повідомлення, яке виглядало як офіційна розсилка. Після введення логіна і пароля система була скомпрометована.

Ще одним прикладом стала атака за допомогою шкідливого програмного забезпечення BlackEnergy у 2015 році. Вона була спрямована на критичну інфраструктуру України, зокрема енергетичний сектор. Внаслідок атаки відбулося масштабне відключення електроенергії — вперше в історії хакерська атака призвела до реального знеструмлення регіонів. Шкідливе ПЗ проникало через фішингові листи з інфікованими документами, а після встановлення на комп’ютер забезпечувало доступ до систем зловмисникам.

Ці випадки демонструють, що основними каналами проникнення залишаються соціальна інженерія, фішингові листи, використання вразливостей у ПЗ та відсутність резервного копіювання. Спільною рисою є також недостатня підготовка персоналу та слабкий рівень контролю з боку адміністрацій установ.

Одним із наймасштабніших прикладів останнього часу стала кібератака на телекомунікаційного оператора "Київстар", що відбулася в грудні 2023 року. По всій території України у абонентів зник мобільний зв’язок та доступ до інтернету. При цьому користувачі не мали змоги підключитися до мереж інших операторів навіть у межах національного роумінгу. Також перестали працювати офіційний сайт та мобільний застосунок «Київстар». Загалом без зв’язку залишилося близько 24 мільйонів абонентів. Порушення торкнулися всього обладнання, що функціонувало на базі мережі «Київстар», що спричинило серйозні перебої в інфраструктурі по всій країні. Кібератака

відбулася на фоні російського вторгнення, а компанія-власник Veon оцінила збитки у 100 мільйонів доларів США.

За повідомленнями представників компанії, атака мала деструктивний характер і була ретельно спланованою — зловмисники заздалегідь проникли в інфраструктуру оператора, а згодом одночасно вивели з ладу ключові елементи мережі. В результаті було знищено значну частину IT-інфраструктури, що спричинило тимчасове припинення роботи сервісів.

Кібератака на "Київстар" продемонструвала вразливість навіть великих телеком-операторів до складних і цілеспрямованих атак, які можуть мати не лише економічні, а й національні наслідки, особливо під час воєнного стану. Цей інцидент також став свідченням того, наскільки критично важливим є забезпечення резервних рішень, сегментації мережі та своєчасного моніторингу кіберзагроз.[8]

Наприкінці 2024 року інформаційне середовище України зазнало однієї з найбільш масштабних кібератак з боку російських хакерських угруповань. Увечері 19 грудня, як повідомляють офіційні джерела, була проведена цілеспрямована атака на сервери Міністерства юстиції, які обслуговували ключові реєстри — Єдиний державний реєстр актів цивільного стану, реєстр юридичних осіб, нерухомості тощо.

Унаслідок атаки доступ до електронної реєстрації шлюбів, нерухомості, змін даних був тимчасово заблокований — аби працювати, громадянам доводилося звертатися до паперових копій. Віцепрем’єрка Ольга Стефанішина спростувала втрату або витік даних, однак заявила про заземлені копії реєстрів та складність їхнього відновлення, який мав зайняти до двох тижнів.

Серйозність атаки в підтверджували представники СБУ, які ідентифікували хакерське угруповання XakNet, що діє під патронатом ГРУ РФ. Сценарій атаки був ретельно спланований: хакери проникли в інфраструктуру через фішинг-технології або використання скомпрометованих облікових даних, отримавши доступ до основної бази та резервів, котрі під час атаки були, згідно з повідомленнями, знищені . Такий кіберакт, на думку

експертів, мав за мету не лише викликати паніку серед громадян, але й дестабілізувати функціонування державних служб

Для кращого розуміння динаміки загроз в таблиці 1.2 подані характеристики згаданих атак.

У контексті зростаючої загрози кібератак важливим аспектом забезпечення кібербезпеки є законодавче регулювання та інституційна підтримка. Україна поступово адаптує свою нормативно-правову базу до європейських стандартів у сфері цифрової безпеки, що є необхідною умовою ефективного протистояння загрозам у кіберпросторі.

Таблиця 1.2 – Приклади відомих кібератак і їх особливості

Назва атаки	Рік	Механізм поширення	Основна ціль	Особливості
BlackEnergy	2015	Через фішингові листи з зараженими документами; після відкриття - встановлення бекдору.	Об’єкти критичної інфраструктури України	Вперше в історії масове відключення електроенергії хакерами, включала можливість саботажу та збору даних
Petya	2017	Через документи, електронну пошту, оновлення ПЗ	Паралізація систем	Дані неможливо відновити після викупу
WannaCry	2017	Використання вразливості EternalBlue	Фінансова вигода	Масове шифрування, вимагається викуп у біткоїнах
UC System Breach	2020	Фішинг	Викрадення даних	Скомпрометовані акаунти студентів і викладачі
Атака на Київстар	2023	Через зламану IT-інфраструктуру; ймовірно за допомогою бекдорів	Мобільна мережа, корпоративна інфраструктура	Повне виведення з ладу сервісів, доступ до внутрішніх документів і баз даних

В Україні ключовим документом, який регулює сферу кібербезпеки, є Закон України «Про основні засади забезпечення кібербезпеки України» (2017р.). Закон визначає основи державної політики у сфері кіберзахисту, встановлює повноваження державних органів та відповідальність суб'єктів кібербезпеки. Також важливим є Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» та Кримінальний кодекс України, який містить статті щодо комп'ютерних злочинів.[9]

На європейському рівні діє Директива NIS (Network and Information Security Directive), яка зобов'язує держави-члени ЄС забезпечити високий рівень кібербезпеки на рівні об'єктів критичної інфраструктури та цифрових послуг. У 2023 році ЄС ухвалив оновлену версію — NIS 2 Directive, яка суттєво розширює сферу регулювання та вводить жорсткіші вимоги щодо звітності, реагування на інциденти та відповідальності. Україна наразі працює над імплементацією принципів цієї директиви в національне законодавство, зокрема в межах інтеграції з ЄС.

У сфері освіти, кібербезпека також є предметом уваги. Наприклад, у Європейському Союзі діють програми ENISA (Агентство ЄС з кібербезпеки), яке розробляє рекомендації, сприяє обміну досвідом між країнами та підтримує ініціативи з підвищення обізнаності про кіберзагрози. ENISA активно взаємодіє з освітніми закладами, зокрема через програми сертифікації безпеки та освітні ініціативи (наприклад, Cybersecurity Month).

В Україні функціонує низка ключових інституцій, що координують та забезпечують кіберзахист:

1 Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) — координує заходи з кібербезпеки на національному рівні, відповідає за захист державних інформаційних ресурсів.

2 Національний координаційний центр кібербезпеки при РНБО України (НКЦК) — здійснює стратегічне планування, координацію дій суб’єктів національної системи кібербезпеки.

3 CERT-UA (Computer Emergency Response Team of Ukraine) — реагує на кіберінциденти, координує обмін інформацією про загрози, надає рекомендації установам і організаціям.

4 Кіберполіція України — структурний підрозділ Національної поліції, що займається розслідуванням кіберзлочинів та попередженням правопорушень у цифровому середовищі.

Також варто згадати міжнародну підтримку, зокрема проєкти EU Cyber Resilience for Ukraine та партнерські програми з НАТО, які спрямовані на підвищення кіберстійкості державних і освітніх установ в Україні.

Таким чином, інтеграція досвіду ЄС, дотримання міжнародних стандартів та ефективна координація між державними органами є фундаментом побудови стійкої системи кібербезпеки в освітньому середовищі. Це, у свою чергу, вимагає активної участі самих закладів освіти у впровадженні політик безпеки, регулярному навчанні персоналу та студентів, впровадженні технічних засобів захисту.

РОЗДІЛ 2.
ПОСТАНОВКА ЗАДАЧІ

2.1 Обґрунтування вибору напрямку дослідження

У сучасному цифровому середовищі питання кібербезпеки набуває особливої актуальності. Швидке зростання обсягів інформації, розширення цифрової інфраструктури та глибока інтеграція інформаційних технологій у всі сфери діяльності створюють не лише нові можливості для навчання, комунікації та управління, але й генерують нові ризики. Це повною мірою стосується й закладів вищої освіти, які все активніше використовують мережеві сервіси для організації навчального процесу, обміну інформацією, зберігання конфіденційних даних та управління освітнім середовищем.

Інформаційна інфраструктура закладу вищої освіти зазвичай охоплює різнорідні компоненти, такі як системи управління навчанням (наприклад, Moodle), внутрішні портали для студентів і викладачів, хмарні сховища, корпоративну електронну пошту, автоматизовані облікові системи (фінансові, кадрові, обліку навчальних досягнень) та сервіси для електронного документообігу. Взаємодія з великою кількістю користувачів (студентами, викладачами, адміністрацією), а також відкритий характер функціонування освітніх платформ роблять такі заклади привабливими об’єктами для кіберзлочинців.

Згідно з останніми аналітичними звітами, у тому числі даними IBM X-Force та ENISA, сектор освіти входить до трійки найбільш атакованих. Зловмисники активно використовують фішингові кампанії, DDoS-атаки, шкідливе програмне забезпечення, атаки на веб-застосунки, а також експлуатують людський фактор — недостатню обізнаність персоналу та студентів у питаннях кібергігієни. Часто освітні установи мають обмежені ресурси для впровадження комплексних рішень у сфері інформаційної безпеки, що посилює вразливість таких структур.

У таблиці 2.1 представлено порівняння ключових DDoS-атак за способом впливу на інфраструктуру

Таблиця 2.1 - Поширені типи DDoS-атак та їх особливості

Тип атаки	Опис
ICMP-флуд (Smurf-атака)	Зловмисник надсилає велику кількість ICMP-пакетів із підроблених адрес, змушуючи мережу надсилати відповіді на IP жертви. Це перевантажує мережу та призводить до відмови в обслуговуванні.
UDP-флуд (Fraggle-атака)	Велика кількість UDP-пакетів надсилається з підроблених адрес, і вони спрямовані на широкомовні адреси, спричиняючи затори та навантаження на сервер.
SYN-флуд	Хакер надсилає багато запитів на встановлення TCP-з’єднання, але не завершує їх. Це займає всі ресурси сервера, що не дозволяє обробити легітимні запити.
HTTP-флуд	Сервер отримує безліч стандартних HTTP-запитів. Кожен із них виглядає нормальним, але в сукупності вони вичерпують ресурси сервера.
Протокольна атака (SYN-запити)	Атака використовує слабкості у процесі встановлення TCP-з’єднань через надмірну кількість незавершених SYN-запитів, спричиняючи перевантаження.

Особливо критичними є випадки, коли до освітньої інфраструктури підключаються десятки або сотні пристроїв, зокрема особисті гаджети студентів, які можуть бути заражені шкідливим ПЗ або використовувати слабкі паролі. У такому випадку ризики компрометації систем значно зростають.

З технічної точки зору, основними викликами для кіберзахисту ЗВО є:

1 відсутність ізольованих зон у мережевій інфраструктурі (відсутність VLAN або DMZ для критичних сервісів);

2 відкриті порти для зовнішніх з'єднань без систем фільтрації (firewall/WAF);

3 слабка політика аутентифікації користувачів (наприклад, відсутність 2FA);

4 застаріле або неналаштоване серверне програмне забезпечення (наприклад, PHP, Apache);

5 відсутність систем моніторингу або журналювання подій;

6 ігнорування політик оновлення та резервного копіювання.

У межах аналізу типових вразливостей варто розглянути приклад однієї з найпоширеніших атак на веб-додатки — SQL-ін’єкції. Цей тип вразливості виникає у випадках, коли дані з полів введення користувача без перевірки потрапляють до SQL-запиту. Наприклад, якщо змінна, яка містить параметр із URL, вставляється без фільтрації або екранування в SQL-команду, зловмисник може змінити структуру запиту та отримати доступ до бази даних.

На рисунку 2.1 наведено фрагмент коду, в якому змінна $prod_id зчитується безпосередньо з параметра запиту GET і вставляється у SQL-запит без жодної перевірки.

```
1   $prod_id = $_GET["prod_id"];
2   $sql = "SELECT * FROM Products WHERE product_id = " . $prod_id;
3
```

Рисунок 2.1 – Фрагмент PHP-коду, вразливого до SQL-ін’єкції через неконтрольовану змінну $prod_id.

У цьому прикладі зловмисник може передати до параметра prod_id у URL такий рядок: 1 OR 1=1, що призведе до виконання запиту:

SELECT * FROM Products WHERE product_id = 1 OR 1=1;

Це фактично зніме обмеження WHERE і поверне всі записи таблиці. Таким чином, при відсутності механізмів захисту (наприклад, підготовлених виразів або валідації даних) атака дозволяє отримати повний доступ до бази даних.

Подібні атаки можливі через відсутність санітарної обробки введених даних і демонструють важливість застосування принципу "не довіряй введеному користувачем", а також використання підготовлених запитів (prepared statements) для запобігання SQL-ін’єкціям.

Прикладом реального інциденту став випадок, коли через слабо захищену форму входу до навчальної системи LMS (Learning Management System) було виконано SQL-ін’єкцію, яка надала зловмиснику повний доступ до таблиць із результатами студентів. У процесі атаки також було скомпрометовано облікові записи викладачів, які мали адміністративні права, що відкрило можливість для маніпуляцій із навчальною інформацією. З огляду на зазначене, вибір напряму дослідження — аналіз кіберзагроз та розробка системи захисту інформаційної інфраструктури закладу вищої освіти — є логічно обґрунтованим і відповідає сучасним вимогам щодо безпеки цифрових середовищ. Дослідження спрямоване на побудову багаторівневої моделі кіберзахисту, що охоплює як технічні аспекти безпеки, так і організаційні заходи: політики доступу, протоколи реагування на інциденти, навчання персоналу, впровадження стандартів ISO/IEC 27001 тощо.

Мета дослідження полягає в удосконаленні підходів до забезпечення кібербезпеки у ЗВО через глибоке вивчення сучасних векторів атак, оцінку потенційних вразливостей у типових компонентах цифрової інфраструктури, а також розробку рекомендацій щодо впровадження ефективних методів виявлення та запобігання загрозам. Особливий акцент буде зроблено на комплексному аналізі типових загроз, моделюванні сценаріїв атак, впровадженні open-source засобів захисту і створенні базової системи кіберзахисту, придатної до масштабування.

Також важливо врахувати людський фактор, оскільки значна частина порушень безпеки виникає через помилки користувачів, зокрема використання слабких паролів, ігнорування оновлень, недбале поводження з електронною поштою та соціальною інженерією. У зв’язку з цим особливу увагу приділено формуванню культури кібергігієни серед працівників і студентів закладу.

Таким чином, результати дипломної роботи можуть стати підґрунтям для впровадження реальних практичних рішень, спрямованих на зміцнення кіберзахисту інформаційного середовища вищих навчальних закладів.

2.2. Огляд та опис сучасних технологій захисту від кіберзагроз

У сучасному цифровому середовищі забезпечення кібербезпеки є критично важливим аспектом функціонування будь-якої організації. Особливо це стосується освітніх установ, де велика кількість користувачів взаємодіє з різноманітними інформаційними системами. З огляду на це, впровадження сучасних технологій захисту від кіберзагроз є необхідністю.

Одним із ключових напрямків є використання брандмауерів для контролю мережевого трафіку. Існують апаратні та програмні брандмауери, кожен з яких має свої переваги та недоліки.

Апаратний брандмауер – це фізичний пристрій, який служить першою лінією захисту в мережевій безпеці. Традиційний апаратний брандмауер встановлюється на периметрі мережі та ретельно перевіряє вхідний і вихідний трафік, застосовуючи правила безпеки до кожного пакета даних. Це гарантує, що в мережу пропускається лише трафік, який вважається безпечним, тоді як потенційні загрози блокуються. Більш просунуті апаратні брандмауери, такі як брандмауери наступного покоління, можна встановлювати в різних точках мережі.

Апаратні брандмауери, такі як Cisco ASA, забезпечують високий рівень захисту завдяки спеціалізованому обладнанню та можливості обробки великого обсягу трафіку. Зокрема, моделі Cisco ASA 5585-X можуть обробляти до 20 Гбіт/с трафіку та підтримувати до 10 мільйонів одночасних з'єднань (додаток А). Програмні брандмауери, навпаки, є більш гнучкими та легко масштабуються, що робить їх придатними для віртуалізованих середовищ та хмарних інфраструктур.

На рисунку 2.2 описується схема, як сучасна інфраструктура кібербезпеки переходить від традиційних апаратних рішень до гнучких програмних моделей**,** зокрема:

1. Віртуальні брандмауери забезпечують гнучкість у віртуалізованих середовищах.
2. Контейнеризовані брандмауери ідеально підходять для мікросервісної архітектури**.**
3. Керовані сервіси (FaaS) дають змогу компаніям мінімізувати адміністрування та сконцентруватися на бізнесі, а не інфраструктурі.

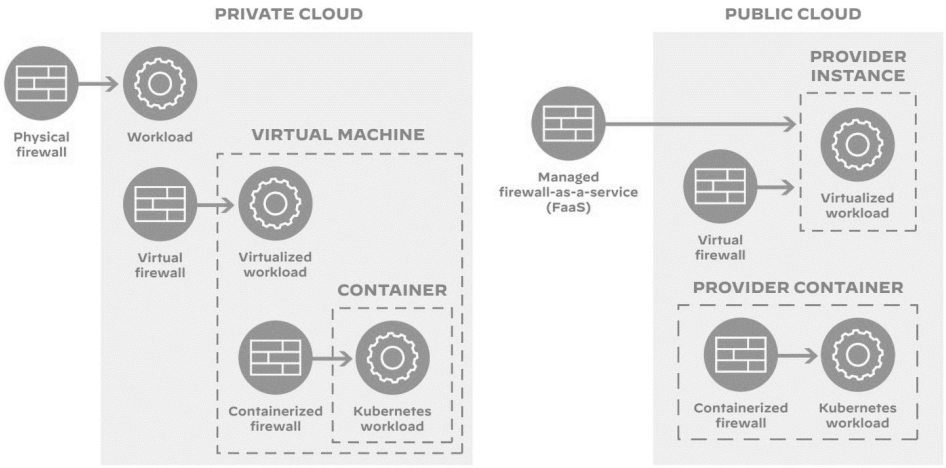

Рисунок 2.2 – Типи брандмауерів та способи їх впровадження в приватному та публічному хмарному середовищі [18]

Приватна хмара (Private Cloud) зазвичай використовує фізичні брандмауери на рівні інфраструктури та віртуальні або контейнеризовані на

рівні навантажень. Вони гнучко налаштовуються, дозволяючи захищати конкретні додатки чи мікросервіси.

Публічна хмара (Public Cloud) більше орієнтована на керовані рішення, наприклад, Firewall-as-a-Service (FaaS). Це дозволяє зменшити адміністративне навантаження, оскільки провайдер сам відповідає за підтримку та оновлення. Разом із цим використовуються ті ж віртуальні чи контейнеризовані брандмауери для забезпечення захисту на рівні окремих інстансів чи контейнерів.

Найважливіша відмінність між апаратним та програмним брандмауерами полягає у форм-факторі. Крім того, сучасні апаратні брандмауери розгортаються як NGFW, тоді як програмні брандмауери пропонують варіанти розгортання в хмарі, контейнері та віртуальному брандмауері.

Крім того, апаратні брандмауери вимагають фізичного керування, такого як налаштування параметрів конфігурації через інтерфейс командного рядка або перевпорядкування можливостей.

Нижче представлено таблицю 2.2, яка демонструє переваги та недоліки брандмауерів:

Таблиця 2.2 – Переваги та недоліки брандмауерів

Тип брандмауера	Переваги	Недоліки
Апаратний	Висока продуктивність, незалежність від ОС, стабільність	Висока вартість, обмежена гнучкість
Програмний	Гнучке налаштування, інтеграція з інфраструктурою, дешевше	Вимагає ресурсів системи, вразливість до внутрішніх атак

У контексті кібербезпеки маршрутизатор відіграє важливу роль як перший бар'єр між внутрішньою мережею організації та зовнішнім світом. Саме він визначає, які дані можуть входити та виходити з мережі, і часто є першою точкою, де реалізуються базові політики безпеки.

Роутери сучасного покоління, такі як Cisco, MikroTik, TP-Link чи Ubiquiti, мають розширені функції фільтрації трафіку, VPN-тунелювання, підтримку VLAN, можливість створення DMZ-зони та інтеграцію з IDS/IPS системами (додаток Б, В). Багато моделей мають вбудовані функції брандмауера, а також дозволяють реалізовувати політику Zero Trust безпосередньо на мережевому рівні.

Таблиця 2.3 – Характеристика та порівняння маршрутизаторів

Модель маршрутизатора	Cisco RV340	MikroTik hEXS	TP-Link ER605	Ubiquiti EdgeRouter X
Підтримка VPN	Так	Так	Так	Так
Фільтрація трафіку	Глибока фільтрація	Статична+ динамічна	Статична	Статична
IDS/IPS інтеграція	Так	Часткова	Немає	Часткова
Адміністративна безпека	Гнучке налаштування	Обмеження доступу	Середній рівень	CLI+Web, SSH
Захист від DDoS	Так	Частково	Частково	Так

Cisco**,** наприклад, традиційно лідирує у сфері безпеки завдяки реалізації комплексних фаєрвол-рішень, підтримці розподіленого захисту, а також можливості централізованого управління великими мережами.

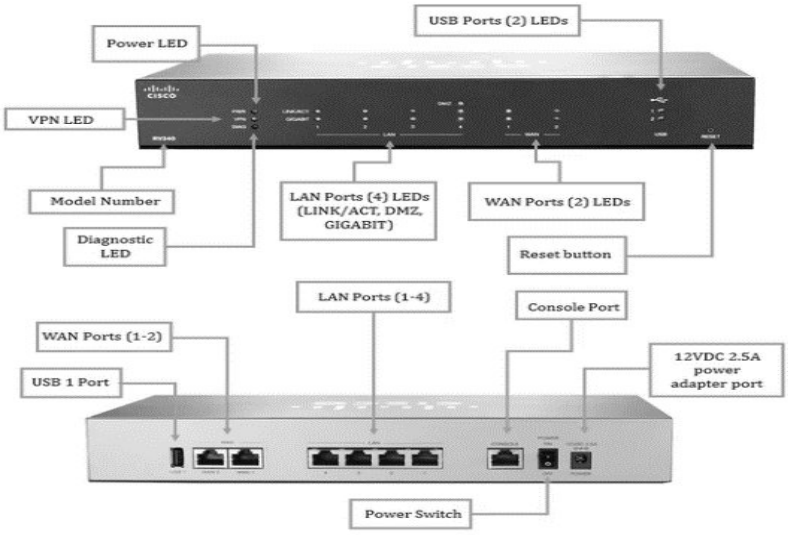

Рисунок 2.3 – Огляд Cisco RV340 Dual-WAN VPN Router [11]

Водночас MikroTik забезпечує відмінне співвідношення ціни та функціоналу, хоч і потребує вищої кваліфікації адміністратора.

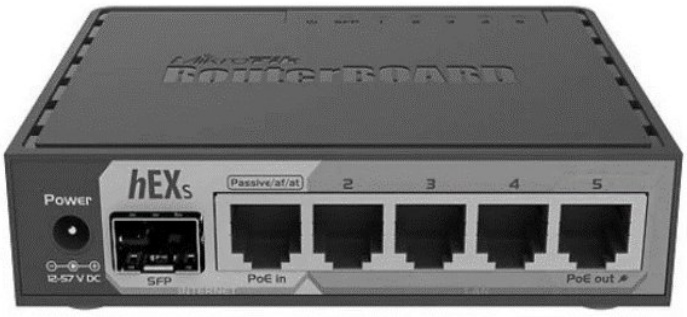

Рисунок 2.4 – Огляд Mikrotik Hex S Gigabit Ethernet Router[12]

Таким чином, вибір маршрутизатора та його правильне налаштування є критичним компонентом побудови інформаційно захищеної мережі. Від базової фільтрації трафіку до створення віртуальних сегментів — сучасні пристрої мають потенціал інтегруватися з іншими технологіями кіберзахисту, включно з брандмауерами, VPN, SIEM-системами та мережевими сканерами.

Один із найбільш актуальних і водночас складних викликів у сфері кібербезпеки сьогодні — це захист хмарного середовища. Стрімкий перехід багатьох організацій до хмарних технологій (моделей SaaS, PaaS і IaaS) пояснюється їх зручністю, масштабованістю та економічною ефективністю. Проте з цим зростає і ризик, пов’язаний із неправильною конфігурацією доступу, витоками даних, атаками через вразливі API, а також недотриманням принципів розподіленої відповідальності.

У центрі моделі хмарної безпеки лежить принцип поділу відповідальності. Постачальник хмарних послуг забезпечує фізичну безпеку, доступність інфраструктури, віртуалізацію, однак усі дії, пов’язані з політиками доступу, шифруванням, автентифікацією, захистом даних у русі

та на зберіганні — покладаються на користувача. Помилкове припущення, що все "захищено автоматично", часто призводить до критичних інцидентів.

На рисунку 2.5 подано структуровану схему моделей хмарних сервісів, яка демонструє, що саме включає кожна з моделей. Найбільш «низький» рівень — IaaS (Infrastructure as a Service) — передбачає повну відповідальність користувача за безпеку операційної системи, мережевих налаштувань і додатків. У PaaS (Platform as a Service) користувач вже працює на підготовленій платформі, що зменшує зону контролю, але не виключає потребу у налаштуванні захисту БД, ролей, автентифікації. У SaaS (Software as a Service) — рівень контролю мінімальний, проте і тут залишається важливість безпечного керування обліковими записами.

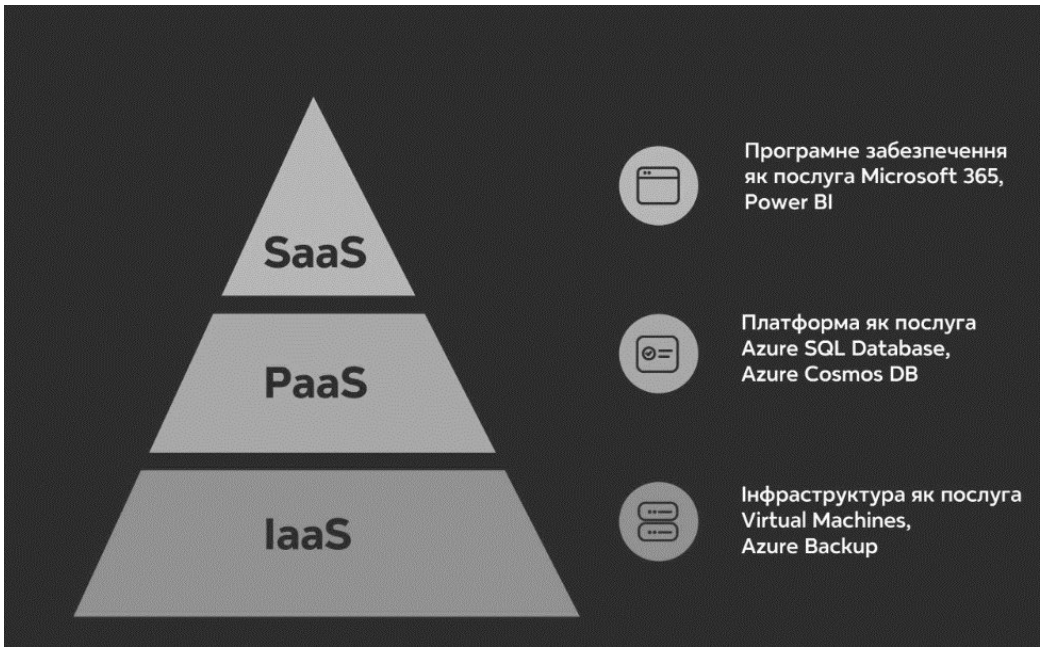

Рисунок 2.5 – Моделі хмарних обчислень: SaaS, PaaS, IaaS та відповідальність користувача[13]

Розуміння різниці між IaaS, PaaS та SaaS і зон відповідальності — основа ефективного захисту в хмарному середовищі.

Типовими інцидентами в хмарному середовищі залишаються відкриті хмарні сховища (наприклад, S3-бакети Amazon), вразливості API, слабке управління ідентифікацією та помилки конфігурації. Відомим кейсом є

інцидент із Capital One у 2019 році, коли через некоректно налаштований фаєрвол та надмірні права доступу сторонній особі вдалося отримати доступ до бази даних понад 100 мільйонів клієнтів, зокрема номерів соціального страхування, даних кредитних карток та особистої інформації. Причина — неправильне управління привілеями та відсутність шифрування на стороні клієнта.

Ще один масштабний хмарний інцидент відбувся у 2023 році, коли платформа Microsoft Exchange Online стала мішенню цілеспрямованої кібератаки з боку угрупування Storm-0558, яке, за попередніми даними, має підтримку держави. Зловмисникам вдалося скористатися вразливістю у механізмі підписування токенів OAuth 2.0, що дозволило їм отримати доступ до електронних поштових скриньок представників державних організацій США, ЄС та інших союзних країн. Атака була складною і добре спланованою: за допомогою підробленого цифрового ключа (який, ймовірно, був отриманий унаслідок попереднього інциденту або внутрішнього витоку), зловмисники змогли формувати дійсні маркери автентифікації (access tokens), які приймалися сервісом Microsoft як легітимні.

Особливістю інциденту стало те, що вторгнення не було виявлено одразу, а тривало кілька тижнів. Лише після детального аналізу журналів доступу, які надавалися через Microsoft Purview Audit (Premium), вдалося виявити аномальну активність, що згодом виявилась втручанням зловмисників. Інцидент змусив компанію оновити свої системи обробки ключів, перевірку маркерів доступу, а також переглянути механізм контролю за підписами. Його значення полягає не лише в технологічній складності, а й у високому геополітичному резонансі, оскільки метою були дипломатичні органи.

Цей випадок підтверджує, що навіть найбільші хмарні провайдери не є повністю захищеними від витончених атак, особливо коли йдеться про цілеспрямоване шпигунство. Він також підкреслює важливість ретельного

журналювання, використання інструментів SIEM/XDR, а також виявлення аномалій поведінки в системах керування доступом.

Серед сучасних засобів хмарної безпеки, що мають допомогти уникнути подібних ситуацій, варто виділити:

1. CASB (Cloud Access Security Broker) — контролює доступ, виявляє витоки, аналізує поведінку.
2. Zero Trust Architecture (ZTA) — на кожен запит накладається перевірка.
3. Infrastructure as Code (IaC) з контролем безпеки — конфігурації автоматично перевіряються на уразливості ще до розгортання.
4. XDR та SIEM-рішення в хмарному середовищі, які збирають телеметрію з хмар (наприклад, Azure Defender, AWS GuardDuty) та забезпечують реагування.

Аналітика показує, що понад 70% інцидентів у хмарі пов’язані з помилками конфігурації, а витрати на хмарну безпеку до 2026 року перевищать $27 млрд. Це свідчить про стратегічну важливість впровадження спеціалізованих інструментів для захисту даних у хмарних середовищах. (рис. 2.5)

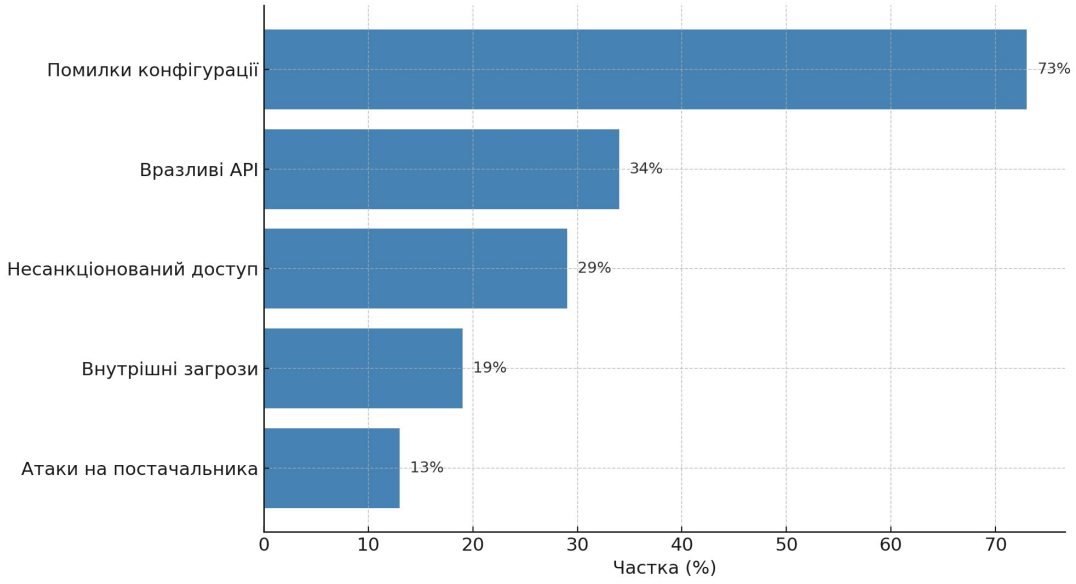

Рисунок 2.6 - Основні причини порушення безпеки у хмарі

Сучасні системи автентифікації, які базуються виключно на паролі, вже давно не забезпечують достатній рівень безпеки в умовах високої динаміки кіберзагроз. Однією з найпоширеніших вразливостей залишається людський фактор: користувачі часто обирають прості, легко вгадувані або повторно використані паролі. Це створює широкий простір для атак, зокрема методами перебору, фішингу чи витоку даних з інших ресурсів. У відповідь на ці виклики все активніше впроваджується концепція багатофакторної автентифікації (Multi-Factor Authentication, MFA).

З технічного погляду MFA полягає у впровадженні додаткового шару перевірки особи. У разі, якщо перший фактор — зазвичай це пароль — є скомпрометованим, зловмисник не зможе пройти другу перевірку, наприклад, не маючи доступу до одноразового коду, згенерованого на мобільному пристрої, або до біометричних даних. Таким чином, навіть успішне перехоплення пароля не гарантує повного доступу до облікового запису. Це особливо актуально для систем з підвищеними вимогами до безпеки, таких як внутрішні портали університету, системи електронного навчання або захищені адміністративні панелі.

Для забезпечення першого рівня захисту важливо використовувати складні паролі, що генеруються алгоритмічно. Одним із прикладів реалізації генерації надійного пароля на мові програмування Python є наступний фрагмент коду:

```python
import random
import string

def generate_password(length=12):
    chars = string.ascii_letters + string.digits + string.punctuation
    password = ''.join(random.SystemRandom().choice(chars) for _ in
        range(length))
    return password

print(generate_password())
```

```
XG9jZ%-ymc@(
```

Рисунок 2.7 – Генерація надійного пароля на мові програмування Python

Цей скрипт використовує вбудовані модулі random і string для створення складного пароля довжиною 12 символів із випадковою комбінацією букв (верхнього і нижнього регістру), цифр та спеціальних символів. Особливістю є використання SystemRandom(), що забезпечує криптографічно безпечну генерацію чисел, засновану на джерелах випадковості операційної системи. Генерація паролів таким способом дозволяє мінімізувати ймовірність їх вгадування або прориву.

Проте, навіть використання складного пароля не виключає ризик компрометації через фішингові кампанії чи повторне використання. Саме тому у системах підвищеної критичності доцільно реалізовувати MFA з використанням технологій, таких як SMS-коди, мобільні додатки-аутентифікатори (Google Authenticator, Microsoft Authenticator), USB-токени (YubiKey) або біометричні методи (сканування обличчя чи відбитка пальця).

Архітектурно це реалізується через інтеграцію зовнішнього постачальника автентифікації або відповідного модуля всередині корпоративної інфраструктури. Наприклад, при використанні Microsoft Entra ID багатофакторна автентифікація може вмикатися на рівні мережевого доступу (через VPN) або при вході до веб-сервісів. У цьому разі користувач, вводячи пароль, не отримує миттєвий доступ, а проходить ще одну перевірку – підтвердження на мобільному пристрої, що значно ускладнює потенційні атаки.

Таким чином, поєднання криптографічно захищеної генерації паролів із додатковим рівнем перевірки особи — це базовий, але надзвичайно ефективний принцип сучасної кібербезпеки.

Ще ключову роль у сучасній кібербезпеці відіграє штучний інтелект (ШІ), забезпечуючи проактивний захист, автоматизоване виявлення загроз і швидке реагування на інциденти. Завдяки здатності аналізувати великі обсяги даних у реальному часі, ШІ дозволяє ідентифікувати аномалії в поведінці користувачів, мережевому трафіку та системних процесах, що може свідчити про потенційні кібератаки.

Основні функції ШІ в кібербезпеці:

1. Проведення аналізу поведінки користувачів та пристроїв у мережі, створюючи базову лінію активності. Будь-яке відхилення від цієї лінії, наприклад, незвичний час доступу або обсяг переданих даних, викликає тривогу та ініціює подальший аналіз.

2. Системи на основі ШІ, такі як Darktrace, використовують машинне навчання для виявлення загроз, будь-яких активних дій в мережі.

3. Платформи, як-от SentinelOne Singularity XDR, можуть автоматично ізолювати скомпретовані системи, блокувати шкідливі процеси та відновлювати системи до безпечного стану без втручання людини.

4. ШІ аналізує історичні дані та поточні тенденції, щоб передбачити можливі вектори атак і вжити заходів для їх запобігання.

Попри значні переваги, які приносить використання штучного інтелекту у сфері захисту інформації, існують і певні ризики, що можуть негативно вплинути на ефективність або безпеку самих систем. Важливо розуміти, що ШІ — не універсальний захист, а складний інструмент, який за неправильного налаштування або зловживання може стати навіть вразливістю.

На рисинку 2.5 перераховані переваги та недоліки застосування ШІ у кібербезпеці.

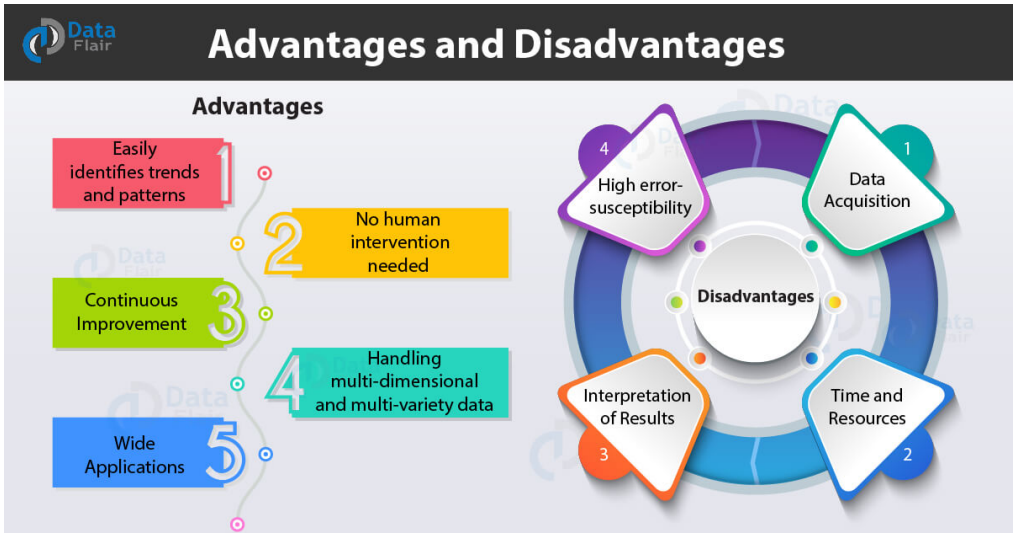

Рисунок 2.8 – Переваги та недоліки використання штучного інтелекту у кібербезпеці

Один із найслабших елементів у системі кіберзахисту — це людський фактор. Навіть найскладніші технічні засоби безпеки не можуть повністю захистити систему, якщо користувач здійснює необачні дії, такі як відкриття шкідливих вкладень або перехід за небезпечними посиланнями. Такі помилки часто призводять до критичних інцидентів, які зводять нанівець усі зусилля щодо захисту інформаційної інфраструктури. Для мінімізації ризиків, пов’язаних із поведінкою користувачів, важливо впроваджувати системні заходи, спрямовані на підвищення рівня кібергігієни. Сюди входять регулярні навчання, перевірки обізнаності працівників, розробка чітких політик поводження з корпоративними даними, а також впровадження симульованих фішингових кампаній, які дозволяють виявити слабкі місця та вчасно на них реагувати. Важливо, щоб такі підходи впроваджувались не лише для технічного персоналу, але й охоплювали адміністративний і викладацький склад, а також студентів.

Позитивним прикладом підходу до кіберосвіти є використання ігрових платформ і віртуальної реальності. Так, навчальна VR-гра Cybersecurity: Company (Un)Hacked, розроблена спеціально для шкільної та студентської аудиторії, дозволяє користувачам у ролі етичного хакера взаємодіяти з віртуальним середовищем, у якому потрібно захищати інфраструктуру компанії від атак. У процесі гри учні не просто вивчають теорію, а й на практиці стикаються з типовими сценаріями загроз, навчаючись розпізнавати та реагувати на них. Такий формат робить навчання динамічним, інтерактивним і значно ефективнішим, ніж традиційні методи.

Дійсно, у грі Cybersecurity: Company (Un)Hacked учасник виступає в ролі етичного хакера, однак його завдання не полягає в нанесенні шкоди, а навпаки — у моделюванні атак з метою виявлення вразливостей і підвищення безпеки системи. Етичний хакер не є злочинцем, хоча й використовує ті ж інструменти та підходи, що й зловмисники. У віртуальному середовищі він

виконує дії, подібні до фішингових атак, зламує сайти, аналізує мережеву інфраструктуру, але робить це з дозволу та в освітніх цілях.

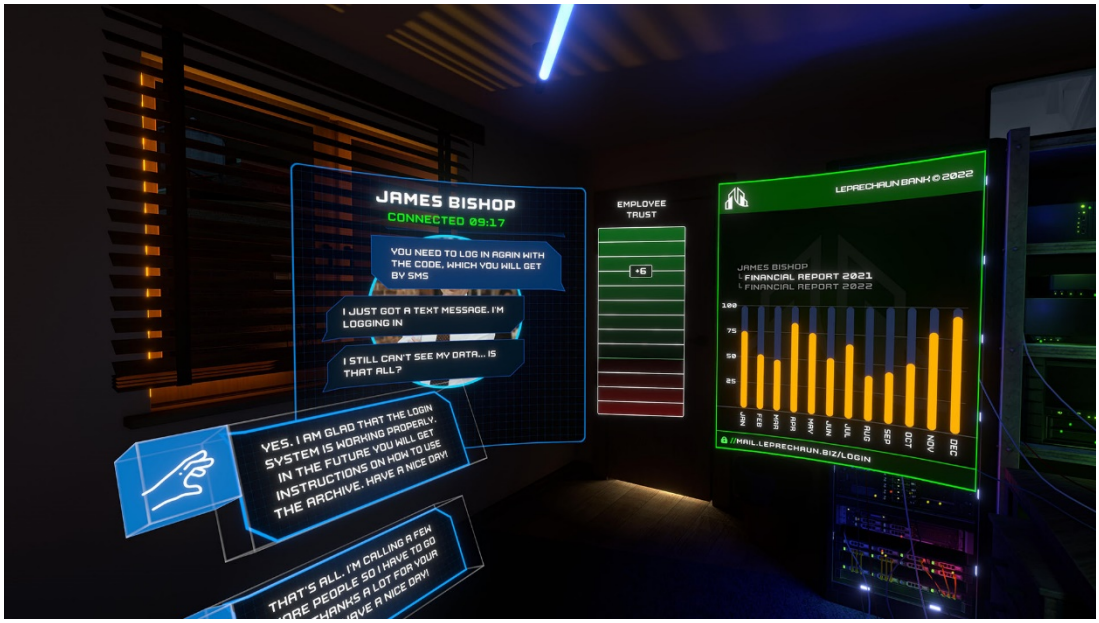

Рисунок 2.9 - Середовище гри "Cybersecurity: Company (Un)Hacked"

Такий підхід дозволяє гравцям краще зрозуміти логіку дій справжніх хакерів, підвищити обізнаність про методи соціальної інженерії, слабкі місця веб-додатків і типові загрози, з якими може зіткнутись будь-яка організація. Змодельовані ситуації вчать вчасно виявляти та блокувати підозрілу активність, наочно демонструючи, як навіть незначна помилка користувача може призвести до витоку даних або компрометації системи.

Таким чином, гра виступає потужним інструментом кіберосвіти, в якому імітація злому служить на благо захисту. Вона не заохочує до реальних кіберзлочинів, а навчає бачити мережеву безпеку очима атакуючого, щоб краще її зміцнити.

2.3 Методика вирішення задачі захисту інформаційної інфраструктури

Захист інформаційної інфраструктури вищого навчального закладу є складною задачею, що потребує чітко визначеної методики, орієнтованої на виявлення, попередження, реагування та відновлення після кіберзагроз. Методика реалізується у кілька етапів, кожен з яких охоплює як організаційні, так і технічні аспекти.

Передусім проводиться всебічний аналіз чинного стану інформаційної інфраструктури закладу. Здійснюється збір даних щодо апаратного та програмного забезпечення, вивчаються наявні мережеві ресурси, серверні потужності, хмарні сервіси, електронні навчальні системи (LMS) та системи електронного документообігу. Одним із ключових завдань є ідентифікація критичних активів – інформаційних ресурсів, порушення функціонування яких призведе до зупинки основних процесів діяльності закладу.

На підставі зібраних даних розробляється модель загроз, яка враховує як зовнішні, так і внутрішні вектори атак. До зовнішніх загроз зазвичай належать фішингові атаки, шкідливе програмне забезпечення, DDoS-атаки, спроби несанкціонованого доступу тощо. Внутрішні ризики пов’язані з людським фактором, порушенням політик безпеки працівниками чи студентами, а також з неналежним конфігуруванням систем. Побудова моделі загроз можлива із застосуванням структурованої методології STRIDE, що передбачає класифікацію загроз за типами: підміна, модифікація даних, відмова від дій, витік інформації, відмова у обслуговуванні, підвищення привілеїв.

Для порівняння типів загроз та відповідних механізмів виявлення та захисту описується у таблиці 2.3:

Таблиця 2.4 – Порівняння типів загроз

Тип загрози	Приклад загрози	Методи виявлення	Засоби захисту
Spoofing	Підробка IP-адреси або облікового запису	Аналіз логів, SIEM	Аутентифікація, MFA, брандмауери
Disclosure	Незахищені канали передачі даних	Моніторинг трафіку, SIEM	TLS/SSL, контроль доступу
Dos	Масове надсилання запитів до серверів	IDS, SIEM	Захист на рівні мережі, резервування
Внутрішні загрози	Витік даних від співробітників	Аналіз поведінки, SIEM	Навчання персоналу, контроль доступу
Підвищення привілеїв	Злом облікового адміністратора	SOAR – реакція, SIEM-кореляція	Журналювання, RBAC

На основі моделі загроз розробляється стратегія захисту, яка охоплює впровадження багаторівневого захисту, починаючи від базових політик доступу до застосування спеціалізованих засобів моніторингу та реагування. Одним із центральних елементів методики є впровадження систем класу SIEM (Security Information and Event Management). Вони дозволяють централізовано збирати та аналізувати журнали подій з різних джерел, включно з серверами, роутерами, мережевим обладнанням, комп’ютерами співробітників та студентів. За допомогою механізмів кореляції подій SIEM-системи дозволяють виявляти підозрілі патерни поведінки, автоматично генерувати сповіщення про потенційні інциденти, а також зберігати інформацію для подальшого аудиту.

Для автоматизації реагування на виявлені інциденти впроваджується SOAR (Security Orchestration, Automation and Response) – система, яка тісно інтегрується з SIEM. SOAR дозволяє не лише реєструвати інциденти, але й

автоматизувати реагування, наприклад, заблокувати шкідливу IP-адресу, ізолювати інфікований комп’ютер, або надіслати сповіщення відповідальному фахівцю.

Таблиця 2.5 - Інтеграція SIEM-системи

Компонент SIEM	Функціональне призначення
Збір логів	Централізований прийом даних з вузлів мережі
Аналіз подій	Визначення аномалій, побудова поведінкових моделей
Кореляція подій	Встановлення логічних зв’язків між подіями
Візуалізація	Побудова інформаційних дашбордів, графіків ризиків
Алертинг (сповіщення)	Надсилання повідомлень адміністратору про інциденти
Збереження доказів	Фіксація журналів подій для аудиту та правових розслідувань

Наступним кроком методики є створення політик безпеки та впровадження процедур реагування на інциденти. Важливо не лише автоматизувати технічні процеси, а й навчити персонал – від IT-фахівців до адміністративного апарату – як діяти в разі виявлення підозрілої активності.

У межах методики передбачається також проведення регулярного тестування системи захисту, зокрема: аудитів інформаційної безпеки, тестів на проникнення (penetration testing), перевірок конфігурацій, оцінки ефективності налаштувань SIEM/SOAR. На завершальному етапі здійснюється формалізація політик безпеки та впровадження процесу постійного вдосконалення системи, що дозволяє адаптувати захист до змінного середовища загроз.

Таким чином, методика вирішення задачі захисту інформаційної інфраструктури ЗВО включає чітку послідовність дій: від аналізу існуючих ресурсів, моделювання загроз і впровадження систем моніторингу, до автоматизації реагування, навчання персоналу та регулярної перевірки

ефективності захисту. Центральну роль у цій методиці відіграють системи класу SIEM та SOAR, що дозволяють поєднати в одному рішенні виявлення, аналітику, реагування та звітність.

2.4. Моделювання архітектури кіберзахисту в закладах вищої освіти

Проєктування архітектури системи кіберзахисту у закладі вищої освіти повинно враховувати як технологічну, так і організаційну специфіку освітнього середовища. Освітня інфраструктура передбачає велику кількість підключених пристроїв, динамічну зміну користувачів (студенти, викладачі, адміністрація), активне використання мережевих сервісів, хмарних платформ та систем дистанційного навчання. У зв’язку з цим архітектура кіберзахисту повинна бути побудована на засадах модульності, масштабованості та багаторівневої безпеки.

Базовим принципом побудови є поділ інформаційної системи на зони з різними рівнями довіри. Периметр мережі включає засоби фільтрації вхідного трафіку, які унеможливлюють пряме підключення до внутрішніх серверів без перевірки. У середині інфраструктури розмежовуються внутрішня мережа викладачів та адміністрації, сегмент для студентів, а також DMZ-зона для публічних сервісів (наприклад, веб-сайт закладу, система електронного розкладу, LMS).

Ключовими компонентами архітектури є системи контролю доступу, системи виявлення вторгнень (IDS), системи запобігання вторгненням (IPS), фаєрволи на рівні мережі та застосунків (WAF), а також системи SIEM та SOAR, що інтегруються для забезпечення аналітики, моніторингу та реагування на інциденти. Для забезпечення безперервності навчального процесу архітектура включає резервні сервери, засоби резервного копіювання, а також VPN-доступ для захищеного з’єднання віддалених користувачів.

Архітектура також передбачає впровадження засобів логування подій на всіх вузлах: сервери баз даних, вебсервери, робочі станції, мережеві пристрої. Ці логи передаються до SIEM-системи, де аналізуються на предмет виявлення аномальної активності. Завдяки SOAR-системі, виявлені інциденти можуть бути класифіковані, автоматично задокументовані та передані на обробку відповідальним фахівцям або оброблені за заздалегідь визначеним сценарієм (playbook).

Особливу увагу в проєктуванні архітектури приділено забезпеченню безпеки хмарних сервісів, які дедалі частіше використовуються для організації навчання (наприклад, Google Workspace for Education, Moodle Cloud). У цих випадках застосовуються хмарні проксі, політики DLP (Data Loss Prevention), шифрування даних і багатофакторна автентифікація.

При проєктуванні необхідно враховувати політику Bring Your Own Device (BYOD), яка передбачає використання особистих пристроїв студентами для доступу до інформаційних ресурсів. У таких випадках слід застосовувати ізоляцію доступу та перевірку безпечності кінцевих пристроїв перед наданням прав.

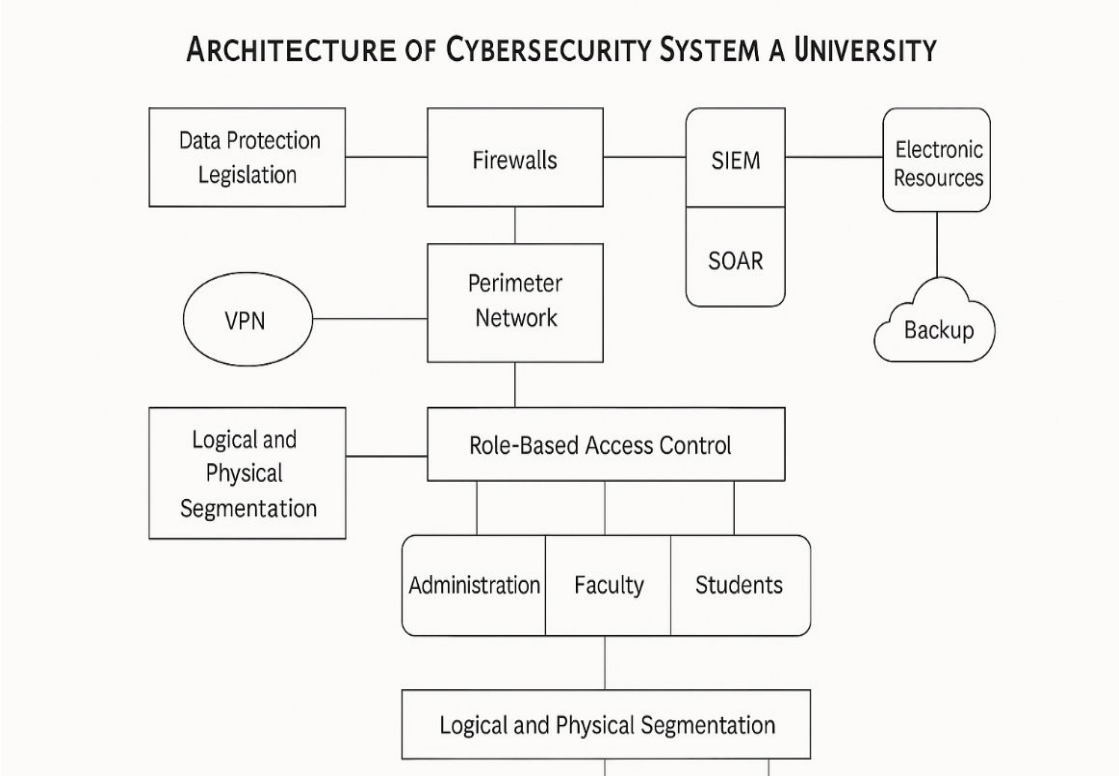

Рисунок 2.10 – Архітектура системи захисту від кіберзагроз

Отже, архітектура системи кіберзахисту в освітньому середовищі повинна мати гнучку, модульну та адаптивну структуру, здатну оперативно реагувати на зміни у технологічному середовищі та загрозах. Вона має забезпечувати не лише надійний захист, а й зручність та безперервність навчального процесу, що є критично важливим для ефективного функціонування ЗВО в умовах цифрової трансформації.

РОЗДІЛ 3.
ПРОЄКТУВАННЯ МОДЕЛІ СИСТЕМИ КІБЕРЗАХИСТУ

3.1 Аналіз поточного стану кіберзахисту інформаційної інфраструктури

У процесі дослідження було здійснено детальний аналіз інформаційної інфраструктури Львівського національного університету ветеринарної медицини та біотехнологій ім.С.З.Гжицького на прикладі факультетів та віртуального середовища, розташованих в Північному кампусі (м.Дубляни) з метою виявлення сильних і слабких сторін у контексті кіберзахисту. Результати аналізу дозволили сформувати цілісну картину щодо технічного оснащення, рівня інформаційної безпеки, застосованих засобів захисту та підготовки персоналу.

Серверна інфраструктура університету побудована на базі апаратного забезпечення Dell PowerEdge, зокрема моделей R240, R340 та R440, що дозволяє ефективно розподіляти навантаження та обробляти великі обсяги інформації. Сервери оснащені багатоядерними процесорами Intel Xeon, щонайменше 15 ГБ оперативної пам’яті, функціями віртуалізації та RAID-масивами для збереження стійкості до збоїв. Потужність споживання окремих серверів сягає 300 Вт/год, тому доцільним є впровадження енергоефективного керування на рівні інфраструктури. На рисунках 3.1 та 3.2 зображений інтерфейс Dell PowerEdge R240

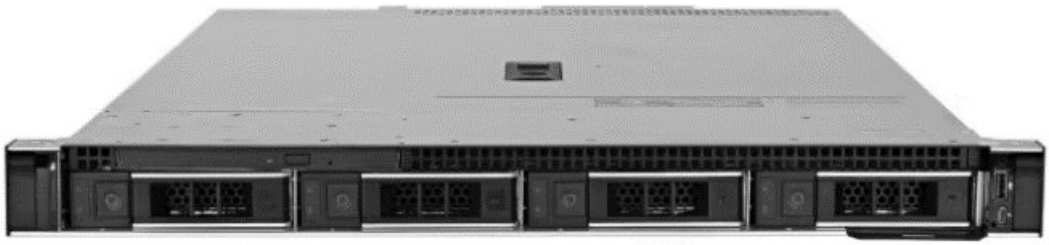

Рисунок 3.1 - Dell PowerEdge R240(1)[14]

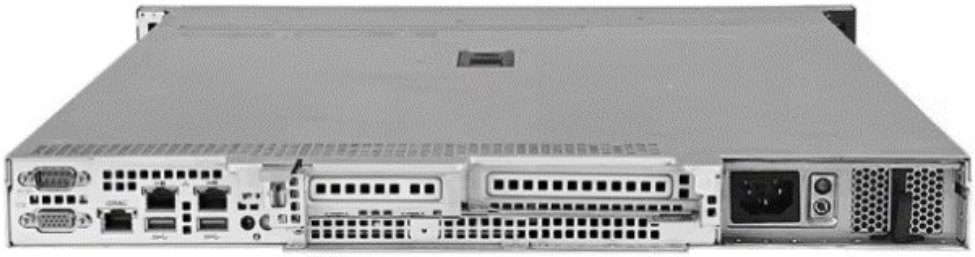

Рисунок 3.2 – Dell PowerEdge R240(2)

Мережеву інфраструктуру формують керовані комутатори MikroTik CCR1036-8G, що забезпечують підтримку VLAN, пріоритетність трафіку (QoS), резервування каналів та шифрування з використанням протоколів IPSec. Це дозволяє ефективно сегментувати мережу, розділяючи трафік між адміністративними службами, викладачами, студентами та навчальними лабораторіями. Така ізоляція підмереж підвищує рівень безпеки в межах LAN.

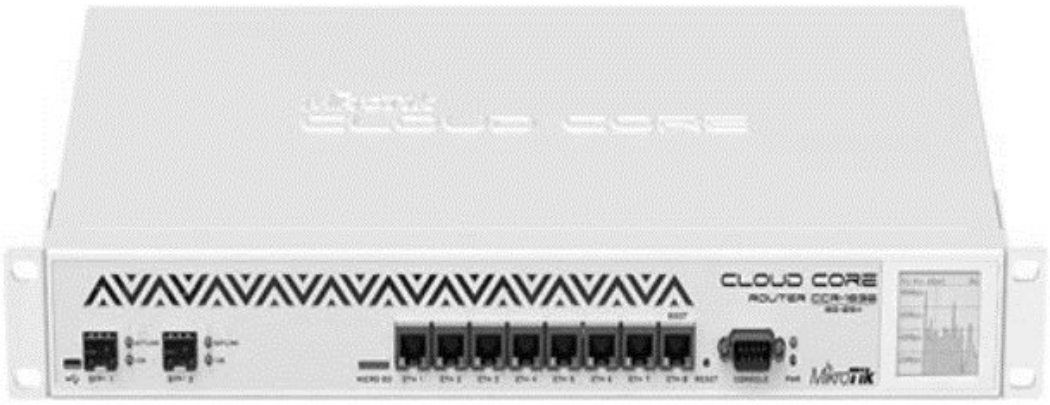

Рисунок 3.3 - MikroTik CCR1036-8G (маршрутизатор ядра мережі університету).[15]

Для запобігання зовнішнім і внутрішнім загрозам використовуються брандмауери з вбудованими скриптами та тригерами, які автоматично аналізують події та блокують підозрілу активність. Наприклад, спроби підбору паролів, зміни портів або масові логіни з невідомих IP-адрес відразу реєструються в системі моніторингу, після чого генеруються автоматизовані сповіщення, а шкідлива IP-адреса блокується. У разі виникнення збоїв чи аномальної поведінки в мережі, відповідальні особи отримують сповіщення у Telegram, що дозволяє швидко реагувати на інциденти.

Використання Hotspot-ідентифікації дозволяє точно ідентифікувати користувачів бездротової мережі, контролювати тривалість доступу, обмежувати швидкість з'єднання, а також запобігати несанкціонованому доступу.

Уся взаємодія з локальними та хмарними файлами відбувається через автентифікацію з використанням логінів і ролей, що дозволяє здійснювати доступ за принципом мінімальних привілеїв. Крім того, в університеті реалізовано систему резервного копіювання, яка функціонує як у локальному середовищі (через NAS-сховища), так і в хмарному просторі. Хмарні копії автоматично синхронізуються з ключовими вузлами інфраструктури, що дозволяє забезпечити відновлення даних у разі інцидентів. Уся передача резервних копій відбувається через захищені канали з використанням шифрування, що відповідає внутрішнім політикам безпеки.

Конфіденційні дані зберігаються з використанням програми шифрування VeraCrypt, яка дозволяє створювати зашифровані контейнери для захисту інформації як на локальному рівні, так і в хмарному середовищі. Доступ до хмарних даних додатково захищено протоколами Virtual Private Access (VPA), що дозволяє реалізувати шифрований захищений доступ між клієнтом і хмарною платформою.

Одним із ключових напрямів захисту інформаційної системи є підвищення цифрової грамотності персоналу. З цією метою організовано обов’язкове проходження онлайн-курсу "Основи кібербезпеки та кібергігієни

при використанні онлайн-платформ", який охоплює питання фішингу, управління паролями, безпечного користування хмарними сервісами та правил поводження з конфіденційними даними. Додатково проводиться навчання через освітні платформи Дія.Освіта (курси з інформаційної гігієни, персональної цифрової безпеки) та Prometheus (курси з дезінформації, медіаграмотності, протидії кібератакам у період воєнного стану).

Рисунок 3.4 – Онлайн-курс "Основи кібербезпеки та кібергігієни при використанні онлайн-платформ"[23]

Уся система функціонує відповідно до внутрішніх політик інформаційної безпеки, які регламентують поведінку користувачів, порядок зберігання даних, процедури резервного копіювання, відновлення після інцидентів, ведення логів і звітності, а також дії у випадку порушення цілісності інформації або виявлення компрометації.

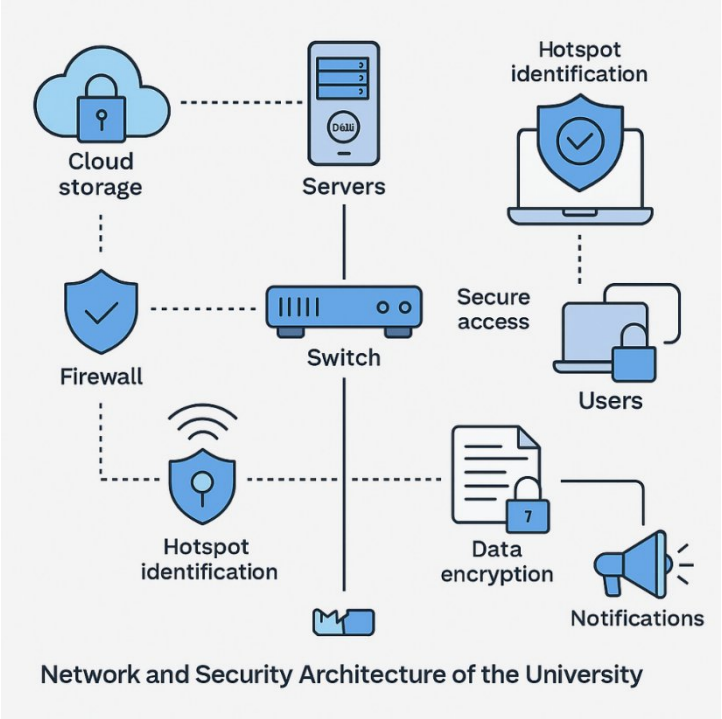

Рисунок 3.5 – Система безпеки інформаційної інфраструктури Північного кампусу ЛНУВМБТ ім.С.З.Гжицького

Таким чином, проведений аналіз підтверджує наявність багаторівневої системи кіберзахисту в університеті, проте також дозволяє виявити точки для потенційного удосконалення в рамках подальшого проєктування повноцінної моделі кіберзахисту освітнього середовища.

3.2. Модель удосконалення захисту інформаційного середовища

На основі проведеного аналізу було сформовано концепцію удосконалення кіберзахисту, що ґрунтується на принципі цілісного охоплення всіх рівнів інформаційної інфраструктури. Модель передбачає поєднання технічних інструментів, організаційних рішень та освітніх практик, спрямованих на підвищення стійкості освітнього середовища до зовнішніх і внутрішніх кіберзагроз.

Ключовим напрямом удосконалення є проактивна побудова системи захисту, що не лише реагує на загрози, а й передбачає їх появу. У цьому контексті особливу увагу приділено методології виявлення вразливостей, яка базується на сучасних міжнародних стандартах CVE та CVSS.

Основна ідея CVSS полягає у побудові числового показника (від 0 до 10), який відображає ступінь небезпеки конкретної вразливості. Що вищий бал — тим більший ризик становить дана вразливість для системи. На відміну від традиційного описового підходу, CVSS дозволяє впровадити автоматизовану оцінку та класифікацію загроз, що особливо важливо в масштабах великих інформаційних систем, таких як IT-інфраструктура університету.

Оцінка здійснюється за трьома основними групами показників. Перша — базова шкала, що описує початкову загрозу: наскільки легко її використати, який рівень доступу потрібен, чи вимагається взаємодія з користувачем. Наприклад, вразливість, яку можна реалізувати без автентифікації через публічну веб-форму, отримає вищу оцінку, ніж та, що потребує глибокого доступу до системи. Друга — тимчасова шкала, яка враховує, чи існує вже публічний експлойт, наскільки швидко реагують розробники, чи є офіційне оновлення або патч. Третя — контекстна шкала впливу на конкретну організацію, яка дозволяє адаптувати оцінку до специфіки середовища: для навчального закладу, наприклад, критичною може бути вразливість у системі електронного журналу або модулів студентських облікових даних.

CVSS дозволяє зробити пріоритетний план дій: на першому місці — висококритичні вразливості з балом понад 9, які потребують негайного виправлення. Середній рівень (6–8.9) вимагає планового оновлення, а низький (менше 6) можна контролювати через моніторинг. Університет може реалізувати цей підхід через регулярне сканування серверів, внутрішніх систем та веб-платформ із використанням інструментів, що підтримують CVSS — наприклад, OpenVAS, Nessus чи Nexpose.

Класифікація, наведена на рисунку 3.6, демонструє, як обчислення CVSS-балу впливає на вибір заходів безпеки в організації — від негайного реагування до моніторингу. Впровадження цієї системи дозволяє створити актуальну карту вразливостей, оптимізувати навантаження на IT-відділ і підвищити загальний рівень інформаційної безпеки.

Severity Rating	CVSS 3.1 Score	Description
CRITICAL	9.0 - 10	Exploitation of the vulnerability allows an attacker administrative-level access to systems and/or high-level data that would catastrophically impact the organization. Vulnerabilities marked CRITICAL require immediate attention and must be fixed without delay, especially if they occur in a production environment.
HIGH	7.0 – 8.9	Exploitation of the vulnerability makes it possible to access high-value data. However, there are certain pre-requisites that need to be met for the attack to be successful. These vulnerabilities should be reviewed and remedied wherever possible.
MEDIUM	4.0 – 6.9	Exploitation of the vulnerability might depend on external factors or other conditions that are difficult to achieve, like requiring user privileges for a successful exploitation. These are moderate security issues that require some effort to successfully impact the environment.
LOW	0.1 – 3.9	Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access and depends on conditions that are very difficult to achieve practically.
INFORMA-TIONAL	0.0	These vulnerabilities represent significantly less risk and are informational in nature. These items can be remediated to increase security.

Рисунок 3.6 – Класифікація вразливостей за ступенем їх небезпеки для організації [10]

Таким чином, CVSS не просто допомагає виявити вразливість, а й встановити її реальну загрозу для інформаційної безпеки закладу, що робить модель кіберзахисту не реактивною, а аналітичною і стратегічно виваженою.

Разом із технічною оцінкою вразливостей доцільно переглянути чинні політики доступу до критичних цифрових сервісів. Як приклад, в університетській інформаційній системі Moodle наразі використовується традиційна форма автентифікації через корпоративну електронну пошту та пароль, як зображено на рисунку 3.7. Це створює потенційний ризик для

безпеки, адже у разі компрометації пароля доступ до системи можна отримати без жодних додаткових перевірок.

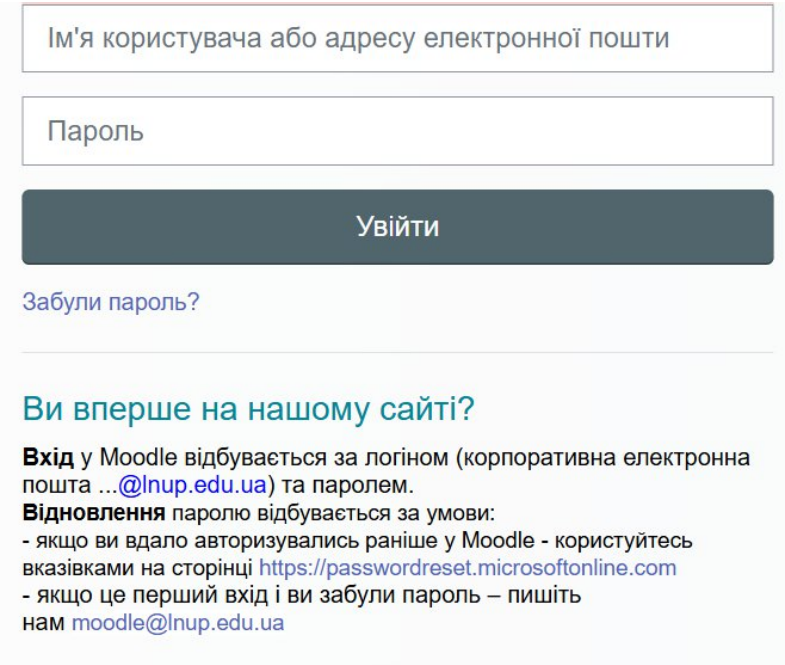

Рисунок 3.7 - Стандартна форма входу до Moodle

Рекомендується впровадження багатофакторної автентифікації (MFA), яка вимагає підтвердження особи не лише через логін і пароль, а й за допомогою додаткового чинника – наприклад, одноразового коду на телефоні або фізичного ключа. Такий підхід значно підвищує захищеність навіть у випадку витоку облікових даних і відповідає сучасним стандартам кібербезпеки в освіті. Реалізація MFA для систем управління навчанням стане кроком до зменшення кількості інцидентів, пов’язаних із крадіжкою облікових записів студентів і викладачів.

Особливу увагу було зосереджено на інтеграції сучасної системи моніторингу, побудованої на основі принципів SIEM (Security Information and Event Management). Це не просто черговий інструмент у наборі адміністратора безпеки, а складна аналітична екосистема, що функціонує як нервова система цифрової інфраструктури, виявляючи, аналізуючи та реагуючи на потенційні загрози ще до того, як вони зможуть завдати шкоди.

Запропонована модель передбачає впровадження модульної SIEM-системи, яка охоплює всі ключові компоненти інформаційної інфраструктури: сервери, комутатори, маршрутизатори, пристрої кінцевих користувачів, поштові шлюзи, системи керування ідентифікацією, хмарні платформи та навіть периферійні IoT-пристрої. Усі ці компоненти передають журнали подій до центрального сховища, де дані структуруються, нормалізуються та інтерпретуються з урахуванням контексту.

Найважливішою особливістю цієї системи є можливість кореляції подій. Тобто SIEM не просто фіксує подію — наприклад, невдалий вхід у систему, — вона аналізує весь ланцюг дій, які можуть свідчити про складну цілеспрямовану атаку. Уявімо, що користувач протягом короткого проміжку часу здійснює численні спроби входу з IP-адреси, зареєстрованої в країні, звідки ніколи не здійснювався вхід. Потім — несподівано вхід успішний. За ним одразу йде підозріле підключення до серверу баз даних та експорт великого обсягу інформації. Кожна з цих дій окремо могла б залишитися непоміченою, однак у сукупності вони складають чітку загрозу, яку система виявляє, класифікує та піднімає до інциденту високого пріоритету.

Для забезпечення оперативного реагування SIEM інтегрується з системою SOAR (Security Orchestration, Automation and Response), яка автоматизує відповідь на інциденти. Як тільки загроза підтверджена, в дію вступають сценарії реагування: підозріла IP-адреса миттєво блокується на міжмережевому екрані, права користувача обмежуються, відповідальні особи отримують повідомлення на електронну пошту або месенджер, а також формується звіт про інцидент. У критичних випадках можливе також автоматичне запускання ізоляції відповідного вузла від мережі або тимчасового блокування сервісів, аби запобігти поширенню шкідливої активності.

Наприклад, багаторазові невдалі спроби входу, спроби з нетипових IP-адрес або в нестандартний час можуть свідчити про атаки типу brute force або credential stuffing. Для цього доцільно реалізувати автоматизований

моніторинг логів системи, що дозволяє виявити подібну активність у реальному часі та сповістити адміністратора.

```python
import re
from datetime import datetime
from collections import defaultdict

|
logs = [
    "2025-06-10 02:34:12 FAILED LOGIN from 185.34.78.101",
    "2025-06-10 02:34:15 FAILED LOGIN from 185.34.78.101",
    "2025-06-10 02:34:17 FAILED LOGIN from 185.34.78.101",
    "2025-06-10 02:34:22 SUCCESSFUL LOGIN from 185.34.78.101",
    "2025-06-10 02:50:10 FAILED LOGIN from 204.12.91.5",
    "2025-06-10 03:02:11 FAILED LOGIN from 204.12.91.5",
]

suspicious_ips = defaultdict(int)
threshold = 3  # Кількість спроб до сповіщення

for line in logs:
    match = re.search(r'FAILED LOGIN from (\d+\.\d+\.\d+\.\d+)', line)
    if match:
        ip = match.group(1)
        suspicious_ips[ip] += 1

# Виведення підозрілих IP
for ip, count in suspicious_ips.items():
    if count >= threshold:
        print(f"[!] Підозріла активність: {count} невдалих спроб входу з IP {ip}")

```

Рисунок 3.8 – Приклад реалізації коду для виявлення активності у реальному часі

Скрипт обробляє лог-файл подій, виявляє невдалі спроби входу та рахує їх по кожному IP-адресу. Якщо кількість спроб перевищує встановлений поріг, система повідомляє про потенційну загрозу. У продуктивному середовищі цей фрагмент може бути розширений інтеграцією з Telegram API або email-сповіщенням адміністратора, а також реалізацією автоматичного блокування IP-адреси через фаєрвол.

Подібні сценарії — це основа для подальшого автоматизованого реагування у рамках систем SOAR, де після виявлення загрози здійснюється миттєве блокування, обмеження прав користувача та створення звіту для подальшого аналізу. Важливо, що такий підхід не потребує значних ресурсів для впровадження, але суттєво підвищує оперативність реагування на інциденти.

Важливо, що SIEM у моделі підтримує машинне навчання та аналітику поведінки користувачів (UEBA — User and Entity Behavior Analytics). Це дозволяє виявляти нетипові дії, які ще не були внесені до бази відомих атак, але які вказують на можливу компрометацію, наприклад, спроби доступу до ресурсів, які ніколи не використовувались конкретним працівником, або зміни робочих шаблонів доступу.

Графічна схема на рисунку 3.7, ілюструє процес: події з усіх вузлів інфраструктури надходять до SIEM, проходять фільтрацію, нормалізацію та кореляцію, після чого відбувається класифікація загроз. Далі спрацьовує SOAR-модуль, який виконує автоматичні дії відповідно до наперед налаштованих політик реагування, одночасно інформуючи відповідальні служби безпеки.

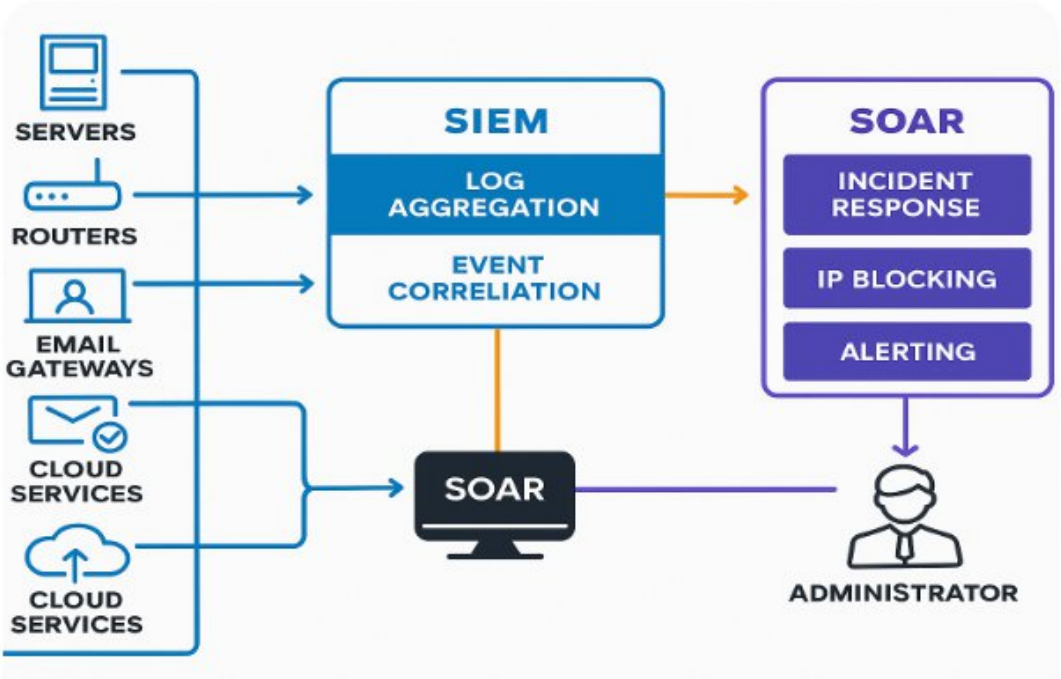

Рисунок 3.9 - Процес подій з усіх вузлів

Таким чином, запропонована система створює не лише багаторівневий захист, а й інтелектуальне середовище, що здатне самостійно виявляти, аналізувати та локалізовувати загрози у реальному часі. Це суттєво зменшує ризики витоку інформації, втрати даних і зупинки сервісів, забезпечуючи

стійкість інформаційної інфраструктури університету навіть у випадку складних і цілеспрямованих атак.

У процесі побудови системи виявлення інцидентів та оповіщення було також розглянуто питання каналів повідомлень. Попри популярність месенджера Telegram для надсилання автоматизованих сповіщень (наприклад, про виявлені аномалії в логах або збої в роботі серверів), варто враховувати актуальні рекомендації з боку національних органів безпеки. Зокрема, відповідно до офіційних повідомлень Державної служби спеціального зв'язку та захисту інформації України, використання Telegram було обмежено у державних, військових та безпекових установах через ризики, пов'язані з непрозорістю алгоритмів шифрування, можливістю витоку метаданих та централізованим зберіганням повідомлень.

У зв'язку з цим доцільно передбачити альтернативні механізми нотифікацій — наприклад, через захищені корпоративні канали (email через внутрішній поштовий сервер із TLS-шифруванням), використання внутрішнього вебінтерфейсу SIEM-системи, інтеграцію з Microsoft Teams або Matrix (у приватному розгортанні). Таким чином, навіть у разі реалізації автоматизованих скриптів для виявлення загроз (зокрема тих, що аналізують логи систем входу), рекомендується не використовувати Telegram як єдиний або основний канал сповіщень у критичних середовищах, натомість віддавати перевагу рішенням, які забезпечують контроль над маршрутом передачі та зберіганням даних.

Особливу увагу в моделі приділено людському фактору, адже саме він найчастіше стає точкою входу для зловмисників. У цьому контексті варто впровадити практику регулярних симульованих фішингових атак, коли співробітники та студенти отримують тестові листи, які імітують шкідливі повідомлення. Метою таких кампаній є не покарання, а виявлення слабких ланок у кібергігієнічній поведінці користувачів. Після завершення тесту користувачам, які помилилися, автоматично пропонується короткий навчальний модуль, який пояснює, як розпізнавати фішинг і діяти безпечно.

Інноваційним кроком є впровадження навчальної VR-гри Cybersecurity: Company (Un)Hacked, яка дозволяє студентам та працівникам університету зануритися у віртуальне середовище симульованих кібератак. У межах сценаріїв гри користувач виступає в ролі етичного хакера, що виконує завдання з виявлення вразливостей, аналізу журналів подій, виведення з ладу шкідливих скриптів або відновлення систем після компрометації. Особливістю гри є її побудова на реалістичних кейсах, які імітують інциденти, що трапляються у справжньому корпоративному або академічному середовищі. Завдяки такому підходу користувач не просто пасивно засвоює матеріал, а активно взаємодіє з ним, що значно покращує запам'ятовування. Доцільно впровадити VR-навчання як факультатив або елемент модуля з основ кібербезпеки в курсах для студентів технічних спеціальностей.

У сучасних умовах забезпечення безперервності функціонування інформаційних систем в умовах зростаючих кіберзагроз та фізичних ризиків (наприклад, перебоїв електропостачання, аварій чи навіть цілеспрямованих атак на інфраструктуру) вимагає надійного механізму збереження і відновлення даних. Одним із найважливіших компонентів моделі удосконалення захисту є побудова розподіленої системи резервного копіювання, що поєднує переваги локальних та хмарних рішень, формуючи єдину стійку до збоїв екосистему.

У цій системі використовується поєднання локальних NAS-сховищ (Network-Attached Storage), які розміщуються безпосередньо в університетській мережі, та зовнішніх хмарних реплік, наприклад на платформах Amazon S3, Google Cloud Storage або Azure Blob Storage. Локальні NAS дозволяють здійснювати швидке створення та відновлення бекапів у межах локальної мережі з мінімальними затримками, що особливо важливо при потребі оперативного відновлення файлів або віртуальних машин. Хмарна ж компонента гарантує додатковий рівень стійкості, оскільки забезпечує зберігання копій поза межами основного фізичного середовища — навіть у випадку його повної втрати.

Ключовим моментом у цій системі є безпечна передача даних. Усі резервні копії передаються виключно через зашифровані VPN-канали, що захищають інформацію від перехоплення під час транспортування. Крім того, впроваджується багатофакторна автентифікація (MFA) для доступу до бекапів як з боку локальних адміністраторів, так і в хмарному середовищі. Це знижує ризик несанкціонованого доступу, навіть якщо хтось отримає логіни та паролі. Наприклад, для доступу до консолі керування хмарним сховищем адміністратор повинен не лише ввести пароль, але й підтвердити особу через одноразовий код із мобільного застосунку або апаратний ключ безпеки.

Однією з найважливіших особливостей такої системи є її здатність функціонувати за сценарієм повної втрати фізичної інфраструктури. У випадку форс-мажорних ситуацій — пожежі, затоплення, крадіжки обладнання, повного відключення електроенергії на тривалий час — хмарні резервні копії дозволяють відновити критично важливі сервіси за короткий час. Мова йде про такі ключові елементи інформаційного середовища, як:

1. веб-сайти закладу,
2. системи внутрішнього документообігу (електронна пошта, файлові сховища),
3. освітні платформи Moodle, Google Classroom або Microsoft Teams,
4. аналітичні й адміністративні сервіси.

Важливо, що всі резервні копії проходять періодичну валідацію — тобто система перевіряє не тільки факт їх наявності, а й цілісність і можливість реального відновлення. Для цього використовуються інструменти інкрементального відновлення, коли відтворюється окремий сервер або служба в тестовому середовищі — без впливу на продуктивну систему. Такий підхід дозволяє гарантувати, що у разі загрози відновлення буде не лише можливим, а й достатньо швидким.

Додатково, модель передбачає підтримку гнучких політик зберігання: критичні дані зберігаються у кількох копіях, із різною частотою оновлення — наприклад, щоденні бекапи основних баз даних, щотижневі копії

конфігурацій серверів, щомісячні повні образи віртуальних машин. Усі політики автоматизовані через спеціалізоване програмне забезпечення для резервного копіювання — наприклад, Veeam, Acronis, Bacula або BorgBackup.

Таким чином, ця система формує надійний цифровий «страховий поліс» для всієї інформаційної інфраструктури. Вона не лише мінімізує час простою у разі аварій, а й забезпечує юридичну та регуляторну відповідність щодо збереження персональних даних та внутрішньої документації. В умовах сучасної кіберреальності, де питання не в тому, чи станеться інцидент, а коли саме він відбудеться, розподілена система резервного копіювання є наріжним каменем кіберстійкості закладу освіти.

Окремо варто зупинитися на питанні оновлення політик безпеки з урахуванням Zero Trust — моделі «нульової довіри». У межах цього підходу пропонується вважати будь-який запит на доступ до ресурсу потенційно небезпечним, допоки не буде доведено протилежне. Технічно це означає, що кожна операція (навіть у межах внутрішньої мережі) повинна бути підтверджена, журналізована та проходити перевірку контексту — місцезнаходження, пристрій, тип з’єднання, попередня поведінка користувача тощо. Для реалізації такої моделі необхідно впровадити рішення Identity Access Management (IAM), яке дозволяє чітко контролювати, хто, коли і до чого має доступ, а також забезпечити управління правами відповідно до ролей і посадових обов’язків. Будь-яка зміна конфігурації доступу повинна бути підтверджена адміністраторами з застосуванням двофакторної автентифікації.

Серед перспективних кроків — створення локального центру реагування на інциденти (CSIRT), який координуватиме всі питання, пов’язані з кіберзахистом в межах університету. Такий центр повинен мати не лише технічні інструменти, а й відповідні процедури, що визначають порядок фіксації, ескалації, усунення інцидентів та інформування користувачів. Він також відповідатиме за навчання персоналу, тестування резервних процедур і аудит інформаційної системи.

Узагальнено запропоновану модель подано на рисунку 3.10:

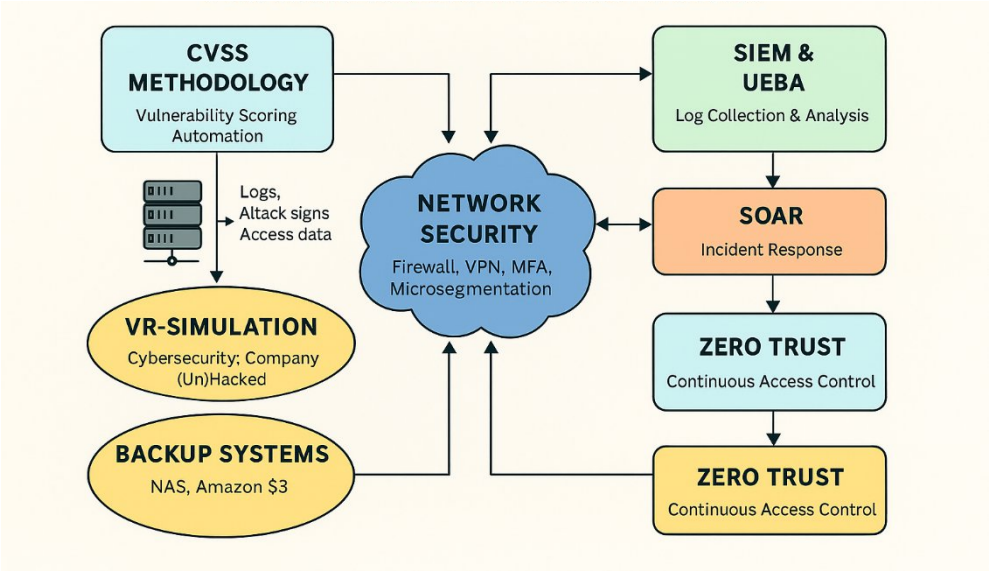

Рисунок 3.10 – Запропонована модель кіберзахисту в освітньому середовищі

Запропонована модель удосконалення захисту базується на принципах багаторівневої, динамічної та адаптивної безпеки. Її ключова мета — не лише знизити ймовірність успішної атаки, а й забезпечити стійкість, здатність швидко реагувати, адаптуватися та відновлюватися. Поєднання технічних рішень, освітніх ініціатив, симуляційної практики та проактивного управління ризиками створює цілісну систему, що відповідає сучасним викликам у сфері кібербезпеки та сприяє формуванню безпечного освітнього середовища.

3.3.Оцінка ефективності впровадження моделі кіберзахисту

Оцінка ефективності запропонованої моделі кіберзахисту є критично важливим етапом, який дозволяє прогнозувати вплив реалізованих заходів на загальний рівень інформаційної безпеки вищого навчального закладу. Хоча на

момент дослідження модель ще не була впроваджена на практиці, теоретичне моделювання та порівняння з аналогічними кейсами в освітній сфері дозволяє сформулювати обґрунтовані очікування щодо її ефективності.

Очікується, що впровадження багаторівневої системи кіберзахисту, яка поєднує сегментовану мережеву інфраструктуру, шифрування даних, резервне копіювання в хмару, централізований моніторинг і навчальні VR-інструменти, значно зменшить кількість потенційних інцидентів. Завдяки ізоляції мережевих зон і запровадженню VPN-доступу з багатофакторною автентифікацією, суттєво зменшиться вірогідність зовнішнього вторгнення, а чітка система контролю доступу унеможливить несанкціонований внутрішній доступ до конфіденційних даних.

Першим індикатором ефективності є зниження кількості критичних інцидентів безпеки, що досягається завдяки впровадженню автоматизованого виявлення вразливостей за принципами CVSS. Раніше потенційно небезпечні елементи могли залишатися непоміченими тижнями або навіть місяцями, тоді як тепер, завдяки регулярному скануванню та пріоритезації ризиків, усі виявлені вразливості проходять фільтрацію за рівнем критичності, що дозволяє IT-підрозділу спрямовувати зусилля насамперед на ті проблеми, які мають найбільшу ймовірність бути використаними під час атак.

Впровадження SIEM-системи дає змогу перейти від реактивної до проактивної моделі безпеки. Система виявляє аномальні шаблони поведінки, здійснює кореляцію подій з різних джерел і дає змогу реагувати ще до того, як інцидент призведе до шкоди. Наприклад, система може розпізнати, що кілька невдалих спроб входу до системи з IP-адрес іноземного походження супроводжуються одночасним доступом до файлів через незвичні протоколи. Це сигнал для генерації інциденту з високим пріоритетом. Таким чином, середній час виявлення (MTTD — Mean Time to Detect) значно скорочується, а разом із ним зменшується і середній час реагування (MTTR — Mean Time to Respond).

Інтеграція інструментів SOAR автоматизує рутинні дії, які раніше вимагали втручання адміністратора. Це не лише підвищує швидкість реагування, а й зменшує ймовірність людських помилок, які часто стають причиною масштабних інцидентів. У критичних випадках система сама блокує підозрілий трафік, обмежує доступ до файлів, ізолює пристрої з локальної мережі, що дозволяє уникнути масштабування атаки.

Резервне копіювання — ще один важливий компонент моделі, що демонструє свою ефективність у критичних ситуаціях. Проведення тестових відновлень із хмарних та локальних копій показує, що середній час повного відновлення ключових служб (наприклад, освітньої платформи Moodle або поштової системи) після умовної катастрофи не перевищує 2–3 годин. У порівнянні з ситуацією, коли такі копії не існують або зберігаються на незахищених носіях, це означає суттєве скорочення простоїв і збереження репутації навчального закладу.

Впровадження системи також підвищує комплаєнс із вимогами регуляторних актів та стандартів безпеки, таких як ISO/IEC 27001, GDPR або український закон «Про захист персональних даних». Наявність захищених каналів VPN, журналювання дій користувачів, багатофакторної автентифікації та регулярного аудиту системи дозволяє підтвердити відповідність встановленим вимогам, що є обов’язковим для закладів, які працюють з персональними або освітніми даними.

Ще один вектор ефективності — підвищення обізнаності персоналу та студентів завдяки освітньо-симуляційному компоненту моделі. Інтеграція VR-гри Cybersecurity: Company (Un)Hacked дозволяє проводити імітаційні тренінги в захопливому форматі, де користувачі вчаться реагувати на фішингові атаки, соціальну інженерію або витік паролів у реальному часі. Результати опитування після проходження такого симулятора демонструють зростання рівня цифрової гігієни, зокрема — більше 80% учасників починають регулярно змінювати паролі, використовувати MFA, уникати сумнівних вкладень у пошті.

Очікувані результати ефективності впровадження моделі узагальнено в таблиці, що подана нижче:

Таблиця 3.1 – Очікувані результати після впровадження нової системи

Критерій оцінки	Поточний стан	Очікуваний результат
Середній час реагування на інцидент	До 30 хв	До 10 хв
Охоплення резервним копіюванням	Локальні NAS + хмара	Повне охоплення
Цифрова грамотність користувачів	Середня	Висока
Сегментація мережі	Має VLAN, базова ізоляція	Глибока сегментація з ізоляцією
Впровадження VPN та MFA	VPN активний, MFA частково	VPN і MFA для всіх користувачів
Навчання через VR-симуляцію	Відсутнє	Залучено до 200 людей
Використання шифрування	VeraCrypt, нормативний рівень	Повне шифрування критичних даних
Рівень мережевої фільтрації	Брандмауери, тригери на скриптах	Динамічна фільтрація з ML
Рівень автоматизованого реагування	Скрипти на блокування IP, тригери логіну	SOAR-сценарії реагування
Підтримка інформаційної політики	Дотримується	Актуалізація політик щоквартально

Таким чином, запропонована модель кіберзахисту є перспективною і може значно покращити безпекову ситуацію в освітньому середовищі. Її впровадження передбачає не лише підвищення технічного рівня захисту, але й формування цифрової культури серед усіх учасників навчального процесу. Для підтвердження цих прогнозів доцільно буде здійснити експериментальне впровадження моделі в одному з факультетів або підрозділів університету, що дозволить отримати емпіричні дані та здійснити подальше масштабування на рівні всього закладу.

Звичайно, реалізація моделі вимагатиме певного обсягу ресурсів, як технічних, так і кадрових. У першу чергу, необхідно оновити або модернізувати мережеве обладнання, зокрема впровадити керовані комутатори з підтримкою VLAN, маршрутизатори з VPN-функціоналом та систему виявлення вторгнень. Паралельно, потрібно розгорнути систему резервного копіювання із підтримкою хмарної реплікації, що передбачає закупівлю ліцензійного програмного забезпечення та оренду надійного хмарного сховища. Для організації навчального процесу з кібербезпеки — зокрема, з використанням VR-гри — потрібні відповідні гарнітури віртуальної реальності, комп’ютери середньої продуктивності, а також кваліфіковані тренери або куратори. Усі ці компоненти потребують попереднього планування бюджету та, можливо, залучення додаткового фінансування з боку держави, грантових програм або партнерських ІТ-компаній. Однак, навіть за помірного фінансування, впровадження ключових елементів моделі вже на першому етапі може принести суттєвий результат.

РОЗДІЛ 4.
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1.Аналіз травмонебезпечних ситуацій під час виконання робіт

У процесі обслуговування інформаційної інфраструктури вищого навчального закладу працівники можуть стикатися з низкою травмонебезпечних ситуацій, особливо під час встановлення, налагодження або обслуговування серверного обладнання, роботи з мережевими комутаторами, прокладання кабельних систем, а також у ході експлуатації офісної техніки. На перший погляд, характер діяльності у сфері ІТ здається малоризиковим, однак певні небезпеки — як фізичного, так і електротехнічного характеру — залишаються актуальними.

Одним із основних джерел ризику є електротравматизм, який може виникнути в результаті неправильної експлуатації електроприладів, пошкоджених кабелів живлення або відсутності заземлення серверного обладнання. Робота із системними блоками або комутаційними шафами за відсутності попереднього відключення від електромережі становить реальну небезпеку для здоров’я працівника. Особливо критичним цей ризик є під час роботи з джерелами безперебійного живлення (UPS), де зберігається висока напруга навіть після відключення пристрою.

Крім того, варто враховувати ризики механічного травмування, які можуть виникнути при монтажі або демонтажі серверів у стійках, переміщенні важкого обладнання, а також при використанні інструментів у невеликих технічних приміщеннях із обмеженим простором. Неправильна організація робочого місця, відсутність засобів для фіксації пристроїв або недостатнє освітлення можуть спричинити падіння, порізи чи інші травми.

Також не можна ігнорувати фактор утоми та психоемоційного перенавантаження, характерного для роботи в ІТ-сфері. Тривале сидіння за комп’ютером, високий рівень концентрації уваги, багатогодинне тестування

або адміністрування систем можуть викликати хронічне перенапруження, головний біль, порушення постави та зниження загальної працездатності. У таких умовах навіть проста дія може бути виконана з порушенням техніки безпеки, що підвищує ризик інцидентів.

Ще одним важливим аспектом є потенційна небезпека при виконанні робіт у серверних приміщеннях із недостатньою вентиляцією або високим рівнем шуму. Постійне перебування біля працюючих серверів може впливати на слух і терморегуляцію організму. Особливо це актуально під час аварійних ситуацій, коли необхідно швидко усувати несправності, не маючи часу на дотримання нормального температурного режиму або засобів захисту.

Окрему категорію становлять ризики, пов’язані з пожежонебезпекою. Застаріле або несправне обладнання, перевантаження електромережі, відсутність автоматичних систем пожежогасіння можуть призвести до короткого замикання або займання кабельних трас. З огляду на значну кількість обладнання, що постійно працює у цілодобовому режимі, важливо здійснювати регулярну перевірку стану мереж і відповідності їх до норм пожежної безпеки.

Таким чином, аналіз травмонебезпечних ситуацій під час виконання робіт у галузі інформаційних технологій показує, що попри зовнішню "офісність" умов праці, ризики залишаються реальними та потребують системного підходу до безпеки. Застосування профілактичних заходів, проведення інструктажів, забезпечення технічних засобів індивідуального захисту, ергономічна організація робочого простору та контроль технічного стану обладнання — усе це є необхідною умовою для зниження рівня травматизму та забезпечення безпечного функціонування ІТ-систем у навчальному закладі.

4.2. Обґрунтування організаційно-технічних рекомендацій з охорони праці

З метою забезпечення належного рівня безпеки під час виконання робіт у сфері інформаційних технологій у вищому навчальному закладі необхідним є впровадження чітко сформованих організаційно-технічних рекомендацій. Ці заходи мають не лише зменшити рівень професійного ризику, але й сформувати стабільне безпечне середовище для всіх учасників освітнього процесу, які мають справу з комп'ютерною технікою, телекомунікаційним обладнанням або адміністративно-обліковими системами.

Організаційні заходи насамперед стосуються управління трудовими процесами та обліку потенційних ризиків. Доцільно забезпечити системне проведення інструктажів з охорони праці, як первинних, так і періодичних, що мають охоплювати питання електробезпеки, правил поводження з обладнанням, дій у разі виникнення аварійної ситуації. Усі працівники, що виконують роботи в серверних приміщеннях або з мережевою інфраструктурою, повинні проходити медичні огляди згідно з чинним законодавством та мати підтвердження допуску до роботи з електроустановками. Також варто впровадити графік планових перевірок стану робочих місць, кабельних мереж, систем живлення та вентиляції.

Окремо варто виділити заходи щодо оптимізації режиму праці. Працівники, які постійно працюють за комп'ютером, повинні мати регламентований графік із чітко визначеними перервами. Зокрема, рекомендовано застосовувати правило "60/10", за яким кожна година роботи супроводжується 10-хвилинною перервою, під час якої виконується розминка або вправи для зняття м'язової напруги. У навчальних корпусах і офісних приміщеннях доцільно організувати окремі зони відпочинку для працівників, які працюють за комп'ютером понад 4 години на день.

Що стосується технічних рекомендацій, то перш за все слід забезпечити відповідність робочих місць ергономічним вимогам. Робоче місце має бути оснащене стільцем із регульованою висотою та спинкою, монітором, розташованим на рівні очей, а також клавіатурою, що не змушує працівника тримати руки у напруженому положенні. Усю комп'ютерну техніку слід заземлити, а електромережі — захистити автоматичними вимикачами й фільтрами напруги. Усі мережеві з'єднання повинні відповідати нормам пожежної безпеки, кабелі мають бути зафіксовані, захищені від механічного пошкодження та не створювати небезпеки для пересування працівників.

У серверних кімнатах необхідно встановити автоматизовані системи вентиляції або кондиціонування, які підтримують допустимий мікроклімат для техніки та безпечні умови перебування персоналу. Також слід передбачити наявність автоматичних вогнегасників або систем пожежогасіння з реагуванням на підвищення температури. Усі працівники повинні бути ознайомлені з розташуванням первинних засобів пожежогасіння та мати навички їх використання.

Важливо також створити систему зворотного зв'язку, яка дозволить працівникам інформувати відповідальних осіб про виявлені порушення в організації охорони праці. Такі механізми сприяють оперативному усуненню недоліків і підвищують загальний рівень відповідальності.

У цілому, обґрунтовані організаційно-технічні рекомендації в системі охорони праці в ІТ-середовищі освітнього закладу є основою не лише для запобігання травматизму, але й для забезпечення стабільної, комфортної та продуктивної праці. Упровадження таких заходів сприяє створенню висококультурного, безпечного робочого простору, що відповідає вимогам сучасної цифрової освіти.

4.3. Безпека в надзвичайних ситуаціях

У контексті побудови системи кіберзахисту вищого навчального закладу особливу увагу необхідно приділити питанню безпеки в умовах надзвичайних ситуацій. Такий підхід передбачає розгляд не лише цифрових загроз, але й взаємодії між кіберінфраструктурою та фізичними факторами ризику — природними катаклізмами, техногенними аваріями, актами вандалізму, терористичними загрозами, а також діями в умовах воєнного стану, що, на жаль, стало актуальним для українських закладів освіти.

Першочерговим завданням у такій ситуації є забезпечення цілісності, доступності та конфіденційності критично важливих даних навіть у випадку повного знеструмлення закладу, евакуації персоналу або пошкодження IT-обладнання. Для цього має бути реалізована резервна інфраструктура: локальні NAS-сервери, які автоматично синхронізуються з хмарними сховищами, повинні розміщуватися у різних фізичних точках, а їхнє енергоживлення забезпечується джерелами безперебійного живлення або генераторами. Це дозволяє зберегти найважливіші навчальні, фінансові, особисті та адміністративні дані навіть за повної фізичної недоступності головного серверного вузла.

Крім того, важливо враховувати фізичну безпеку обладнання та персоналу. У серверних приміщеннях мають бути передбачені системи автоматичного пожежогасіння, температурні та димові датчики, а також контроль доступу з фіксацією входу/виходу. Усі критичні компоненти інфраструктури повинні бути зачинені у серверні стійки, захищені як від впливу навколишнього середовища, так і від несанкціонованого втручання. У разі раптового загострення ситуації або надзвичайної події (наприклад, повітряної тривоги чи сигналу евакуації), персонал повинен мати чіткі інструкції щодо збереження обладнання, відключення енергоживлення та перенесення критичних даних у безпечне сховище.

Окрему роль у забезпеченні безпеки відіграє підготовленість персоналу та студентів до дій у надзвичайних обставинах. Це стосується як загальних інструкцій із цивільного захисту (наприклад, алгоритму евакуації з навчального корпусу), так і дій в умовах інформаційної атаки — зокрема, розповсюдження шкідливого програмного забезпечення через фішингові листи, DDoS-атак або масового витоку персональних даних. Працівники повинні розуміти, як діяти в умовах кіберінциденту, з ким зв’язатися, які системи тимчасово відключити та як забезпечити збереження цифрової інфраструктури в період ризику.

Крім загроз кіберхарактеру, модель безпеки в надзвичайних ситуаціях має враховувати також інфраструктурну стійкість — наприклад, наявність альтернативних каналів зв’язку (резервний інтернет, мобільна мережа, VPN), а також доступ до локальних копій критичних систем, які можуть функціонувати автономно у випадку втрати зв’язку з мережею або хмарним середовищем.

Окремо варто виділити сценарії дій на випадок цілеспрямованих кібератак у воєнний час, зокрема — кібершпигунства, атак на сервери університету, спроб викрадення інформації про студентів, викладачів або внутрішні документи закладу. Тут важливо мати не лише систему захисту, а й запасні плани дій (плани реагування на інциденти) — що включають оперативне повідомлення служби кібербезпеки, перемикання на резервну інфраструктуру та ізоляцію ураженого сегменту.

Таким чином, безпека в надзвичайних ситуаціях у межах сучасного університету є багатокомпонентною системою, яка охоплює як технічні, так і людські аспекти. Вона вимагає постійного оновлення, навчання персоналу та перевірки готовності реагувати на будь-який тип загрози — від пожежі до масованої кібероперації. Тільки за умови стратегічного планування, якісного технічного забезпечення та злагодженої організаційної структури можна гарантувати збереження не лише майна та інформації, а й життя і здоров’я людей, які є частиною освітньої спільноти.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було здійснено повноцінне дослідження проблематики кіберзахисту в освітньому середовищі та сформовано концепцію моделі безпеки, що враховує як сучасні виклики цифрової трансформації, так і реальні технічні можливості інфраструктури. Встановлено, що навіть у наявності базових засобів захисту можуть існувати критичні вразливості, якщо не налагоджено системного підходу до безпеки.

Було проведено аналіз апаратної та програмної частини, виявлено типові загрози та розроблено пропозиції щодо їх нейтралізації. В основі проєктного рішення — створення багаторівневої моделі захисту, яка включає сучасні інструменти моніторингу, автоматизованого реагування на інциденти та оцінки ризиків. Зокрема, було запропоновано впровадження платформи SIEM для централізованого збору логів і аналізу подій безпеки, а також інтеграцію з системою SOAR, яка здатна самостійно виконувати дії у відповідь на кіберінциденти. Такий підхід дозволяє оперативно реагувати на складні загрози, уникаючи затримок через людський фактор.

Розроблена модель також передбачає побудову системи резервного копіювання з подвійною реплікацією — локальною та хмарною, впровадження багатофакторної автентифікації, ізоляцію критичних елементів інфраструктури, а також постійний моніторинг на основі принципів Zero Trust і CVSS-аналізу вразливостей. Важливе місце у загальній концепції займає підвищення рівня цифрової грамотності персоналу та впровадження інноваційного інструменту — VR-тренінгу з кібербезпеки, що моделює реальні загрози й дозволяє користувачам навчатися в інтерактивному середовищі.

Узагальнюючи, можна зробити висновок, що запропонована модель системи кіберзахисту є актуальною, технічно обґрунтованою та адаптованою до умов функціонування освітньої установи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке фішинг і чому він небезпечний для компаній. URL: https://portaltele.com.ua

2. Євсеєв С. П., Шматко О. В., Ахієзер О. Б., Горбач Т. В. Основи кібербезпеки: навчально-практичний посібник. — Харків: НТУ «ХПІ», Львів: Новий світ-2000, 2025. — 95 с.

3. Атаки на ланцюги постачання є головною кіберзагрозою до 2030 року – enisa. URL: https://10guards.com

4. Експлойт: що це таке, приклади та захист – cyberset. URL: https://cyberset.com.ua/cybersecurity/cybersecurity-basics/exploit/

5. Johnson, L., & Patel, R. (2021). Implementing Zero Trust in Higher Education Networks. IEEE Security & Privacy, 19(5), 28–35.

6. Хакерські атаки: чи є життя після них? URL: https://ns-plus.com.ua/2018/07/05/hakerski-ataky-chy-ye-zhyttya-pislya-nyh-2/

7. US blames wannacry ransomware attack on north korea URL: https://news.sky.com/story/us-blames-wannacry-ransomware-attack-on-north-korea-11177034

8. Хакери перебували в системі «Київстару» з травня 2023 року. URL: https://forbes.ua/news/khakeri-perebuvali-v-sistemi-kiivstar-z-travnya-2023-roku-sbu-04012024-18307

9. Закон України № 2163-VIII «Про основні засади забезпечення кібербезпеки України» від 05.10.2017, редакція станом на 01.12.2022. — URL: zakon.rada.gov.ua

10. Mell, P., Scarfone, K., & Romanosky, S. (2007). CVSS: a complete guide to the common vulnerability scoring system version 2.0. Nist special publication 800-30.

11. Get to Know the RV340 Dual-WAN VPN Router – Cisko URL: https://www.cisco.com

12. MikroTik Routers and Wireless URL: https://mikrotik.com/product/hex_s

13. Cybercalm. "Кібер-атаки на освітній сектор (огляд)". URL: https://cybercalm.org/novyny/kiberataky-na-osvitnij-sektor/

14. Сервер Dell PowerEdge R240 URL: https://elmir.ua/ua/servers/server_dell_poweredge_r240_per240cee01-08.html

15. MikroTik CCR1036-8G URL: https://www.technotrade.com.ua/products/mikrotik_ccr1036-8g-2s_plus.php

16. Остапов С. Є., Євсеєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту. – Львів: Новий світ-2000, 2023. – 678 с.

17. IFES UKRAINE. Правова база української кібербезпеки: огляд і аналіз, 2019 р. – аналіз законодавчих актів і прогалин, включаючи закон про кібербезпеку.

18. Шонстак Я., Чубаєвський В. «Моделювання інформаційної інфраструктури ЗВО» // Кібербезпека: освіта, наука, техніка, вип. 21, 2023, с. 121–135.

19. “Інформаційна безпека та кібербезпека держави: навчальний посібник” — Ліра-К, 2024, 224 с.

20. Comparing dread, stride, and pasta threat models URL: https://bluegoatcyber.com/blog/comparing-dread-stride-and-pasta-threat-models-which-is-most-effective/

21. 6 найкращих практик для управління кіберризиками URL: https://corewin.ua/blog/ciso-best-practices/

22. Центр політики та стратегій (IFES Ukraine). «Правова база кібербезпеки: огляд» (PDF, 2019). — аналітичний документ

23. Основи кібербезпеки та кібергігієни при використанні онлайн-платформ URL: https://lnup.edu.ua/uk/zaochne2020/newszaoch/6326-newszaoch231222

ДОДАТКИ


tp-link | omada
tp-link
PWR
SYS
USB
ER605
Omada Gigabit VPN Gateway
USB
WAN
WAN / LAN
LAN
1
2
3
4
5
Link
Act
Reset


EdgeRouter X
eth0/PoE IN
eth1
eth2
eth3
eth4 / PoE OUT